Copyright Information

© Copyright 2021 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

All third-party marks are property of their respective owners.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this document</td>
<td>3</td>
</tr>
<tr>
<td>- Applicable products</td>
<td>8</td>
</tr>
<tr>
<td>- Latest version available online</td>
<td>8</td>
</tr>
<tr>
<td>- Command syntax notation conventions</td>
<td>8</td>
</tr>
<tr>
<td>- About the examples</td>
<td>9</td>
</tr>
<tr>
<td>- Identifying switch ports and interfaces</td>
<td>9</td>
</tr>
<tr>
<td>- Identifying modular switch components</td>
<td>10</td>
</tr>
<tr>
<td>IRDP</td>
<td>11</td>
</tr>
<tr>
<td>- Configuring IRDP</td>
<td>12</td>
</tr>
<tr>
<td>- IRDP commands</td>
<td>13</td>
</tr>
<tr>
<td>- diag-dump irdp basic</td>
<td>13</td>
</tr>
<tr>
<td>- ip irdp</td>
<td>14</td>
</tr>
<tr>
<td>- ip irdp holdtime</td>
<td>14</td>
</tr>
<tr>
<td>- ip irdp maxadvertinterval</td>
<td>15</td>
</tr>
<tr>
<td>- ip irdp minadvertinterval</td>
<td>16</td>
</tr>
<tr>
<td>- ip irdp preference</td>
<td>17</td>
</tr>
<tr>
<td>- show ip irdp</td>
<td>18</td>
</tr>
<tr>
<td>IPv6 Router Advertisement</td>
<td>20</td>
</tr>
<tr>
<td>- Configuring IPv6 RA</td>
<td>20</td>
</tr>
<tr>
<td>- IPv6 RA scenario</td>
<td>22</td>
</tr>
<tr>
<td>- IPv6 RA commands</td>
<td>23</td>
</tr>
<tr>
<td>- ipv6 address &lt;global-unicast-address&gt;</td>
<td>23</td>
</tr>
<tr>
<td>- ipv6 address autoconfig</td>
<td>23</td>
</tr>
<tr>
<td>- ipv6 address link-local</td>
<td>24</td>
</tr>
<tr>
<td>- ipv6 nd cache-limit</td>
<td>25</td>
</tr>
<tr>
<td>- ipv6 nd dad attempts</td>
<td>26</td>
</tr>
<tr>
<td>- ipv6 nd hop-limit</td>
<td>27</td>
</tr>
<tr>
<td>- ipv6 nd mtu</td>
<td>27</td>
</tr>
<tr>
<td>- ipv6 nd ns-interval</td>
<td>28</td>
</tr>
<tr>
<td>- ipv6 nd prefix</td>
<td>29</td>
</tr>
<tr>
<td>- ipv6 nd ra dns search-list</td>
<td>30</td>
</tr>
<tr>
<td>- ipv6 nd ra dns server</td>
<td>31</td>
</tr>
<tr>
<td>- ipv6 nd ra lifetime</td>
<td>32</td>
</tr>
<tr>
<td>- ipv6 nd ra managed-config-flag</td>
<td>33</td>
</tr>
<tr>
<td>- ipv6 nd ra max-interval</td>
<td>34</td>
</tr>
<tr>
<td>- ipv6 nd ra min-interval</td>
<td>35</td>
</tr>
<tr>
<td>- ipv6 nd ra other-config-flag</td>
<td>36</td>
</tr>
<tr>
<td>- ipv6 nd ra reachable-time</td>
<td>37</td>
</tr>
<tr>
<td>- ipv6 nd ra retrans-timer</td>
<td>37</td>
</tr>
<tr>
<td>- ipv6 nd router-preference</td>
<td>38</td>
</tr>
<tr>
<td>- ipv6 nd suppress-ra</td>
<td>39</td>
</tr>
<tr>
<td>- show ipv6 nd global traffic</td>
<td>40</td>
</tr>
<tr>
<td>- show ipv6 nd interface</td>
<td>41</td>
</tr>
<tr>
<td>- show ipv6 nd interface prefix</td>
<td>43</td>
</tr>
</tbody>
</table>
show ipv6 nd ra dns search-list ........................................ 44
show ipv6 nd ra dns server ............................................. 45

sFlow ........................................................................ 47
sFlow agent .................................................................. 47
Configuring the sFlow agent ......................................... 48
sFlow scenario ................................................................ 49
sFlow scenario 2 ............................................................ 50
sFlow agent commands .................................................. 53
clear sflow statistics ......................................................... 53
sflow ........................................................................... 53
sflow agent-ip .................................................................. 55
sflow collector .................................................................. 56
sflow disable .................................................................. 57
sflow header-size .............................................................. 57
sflow max-datagram-size .................................................. 58
sflow mode ..................................................................... 59
sflow polling .................................................................... 59
sflow sampling .................................................................. 60
show sflow ................................................................. 61

DHCP .......................................................................... 63
DHCP client .................................................................. 63
DHCP client commands .................................................. 63
ip dhcp ........................................................................ 63
DHCP relay agent ........................................................... 64
DHCPv4 relay agent ........................................................ 64
Configuring the DHCPv4 relay agent ................................. 65
DHCPv4 relay scenario 1 .................................................... 66
DHCPv4 relay scenario 2 .................................................... 67
DHCPv4 relay scenario 3 .................................................... 68
DHCPv4 relay commands ............................................... 69
DHCPv6 relay agent ........................................................ 77
Configuring the DHCPv6 relay agent ................................ 77
DHCPv6 relay scenario 1 .................................................... 78
DHCPv6 relay scenario 2 .................................................... 79
DHCP relay (IPv6) commands ........................................ 80
DHCP server .................................................................. 84
Configuring a DHCPv4 server on a VRF ............................. 85
Configuring the DHCPv6 server on a VRF ......................... 86
DHCP server IPv4 commands ........................................... 87
authoritative ................................................................. 87
bootp .......................................................................... 88
clear dhcp-server leases .................................................. 89
default-router ............................................................... 90
dhcp-server external-storage ......................................... 91
dhcp-server vrf ............................................................... 92
disable ........................................................................ 93
dns-server ................................................................. 93
domain-name .............................................................. 94
enable ................................................................. 95
http-proxy ............................................................... 96
lease ................................................................. 97
netbios-name-server ..................................................... 98
netbios-node-type ........................................................ 99
option ......................................................................... 99
### DHCP snooping

#### DHCPv4 snooping commands
- clear dhcpv4-snooping binding
- clear dhcpv4-snooping statistics
- dhcpv4-snooping
- dhcpv4-snooping (in config-vlan context)
- dhcpv4-snooping allow-overwrite-binding
- dhcpv4-snooping authorized-server
- dhcpv4-snooping external-storage
- dhcpv4-snooping flash-storage
- dhcpv4-snooping max-bindings
- dhcpv4-snooping option 82
- dhcpv4-snooping trust
- dhcpv4-snooping verify mac
- show dhcpv4-snooping
- show dhcpv4-snooping binding
- show dhcpv4-snooping statistics

#### DHCPv6 snooping commands
- clear dhcpv6-snooping binding
- clear dhcpv6-snooping statistics
- dhcpv6-snooping
- dhcpv6-snooping (in config-vlan context)
- dhcpv6-snooping authorized-server
- dhcpv6-snooping external-storage
- dhcpv6-snooping flash-storage
- dhcpv6-snooping max-bindings
- dhcpv6-snooping trust
- dhcpv6-snooping verify mac
- show dhcpv6-snooping
- show dhcpv6-snooping binding
- show dhcpv6-snooping statistics

### ND snooping

#### Overview
- clear nd-snooping binding
- clear nd-snooping statistics
- nd-snooping
ip icmp throttle ................................................................. 201
ip icmp unreachable ....................................................... 202

DNS .................................................................................. 203
DNS client ......................................................................... 203
Configuring the DNS client ............................................. 203
DNS client commands ..................................................... 204
  ip dns domain-list ......................................................... 204
  ip dns domain-name ....................................................... 205
  ip dns host ....................................................................... 206
  ip dns server address .................................................... 207
  show ip dns ....................................................................... 208

ARP .................................................................................. 211
Configuring proxy ARP ................................................... 212
Configuring local proxy ARP .......................................... 212
Dynamic ARP Inspection ................................................ 213
ARP commands ............................................................... 214
  arp cache-limit ............................................................... 214
  arp inspection ............................................................... 214
  arp inspection trust ....................................................... 215
  arp ipv4 mac .................................................................. 216
  clear arp ......................................................................... 217
  ip local-proxy-arp ........................................................ 217
  ipv6 neighbor mac ........................................................ 218
  ip proxy-arp ................................................................. 219
  show arp ......................................................................... 220
  show arp inspection interface ....................................... 221
  show arp inspection statistics ........................................ 222
  show arp state ............................................................... 223
  show arp summary ........................................................ 224
  show arp timeout ........................................................ 225
  show arp vrf ................................................................. 226
  show ipv6 neighbors .................................................... 227
  show ipv6 neighbors state ............................................. 228

Network Load Balancing (NLB) ........................................ 231
NLB commands ............................................................... 231
  arp ipv4 mac ............................................................... 231
  show arp ......................................................................... 232
  show ip igmp snooping vlan group ................................. 232

Support and Other Resources ......................................... 234
Accessing Aruba Support ................................................. 234
Accessing Updates .......................................................... 234
  Aruba Support Portal .................................................... 234
  My Networking ............................................................ 235
Warranty Information ..................................................... 235
Regulatory Information ................................................... 235
Documentation Feedback ............................................... 235
Chapter 1
About this document

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing Aruba switches on a network.

Applicable products
This document applies to the following products:

- Aruba 6400 Switch Series (JL741A, R0X26A, R0X27A, R0X29A, R0X30A)

Latest version available online
Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in Support and Other Resources.

Command syntax notation conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
</table>
| example-text | Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets ([ ]).
<p>| example-text | In code and screen examples, indicates text entered by a user. |
| Any of the following: | Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: |
| &lt;example-text&gt; | For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (&lt; &gt;). Substitute the text—including the enclosing angle brackets—with an actual value. |
| &lt;example-text&gt; | For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value. |
| example-text | Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax. |
| { } | Braces. Indicates that at least one of the enclosed items is required. |</p>
<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Brackets. Indicates that the enclosed item or items are optional.</td>
</tr>
</tbody>
</table>
| ... or ... | Ellipsis:  
  ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information.  
  ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified. |

### About the examples

Examples in this document are representative and might not match your particular switch or environment. The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

### Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term switch, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
  Indicates the operator command context.
switch#
  Indicates the manager command context.
switch(CONTEXT-NAME)#
  Indicates the configuration context for a feature. For example:
switch(config-if)#
  Identifies the interface context.
```

### Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100)#
```

When referring to this context, this document uses the syntax:

```
switch(config-vlan-<VLAN-ID>)#
```

Where `<VLAN-ID>` is a variable representing the VLAN number.

### Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format:

```
member/slot/port
```

#### On the 6300 Switch Series

- **member**: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 10. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- **slot:** Always 1. This is not a modular switch, so there are no slots.
- **port:** Physical number of a port on the switch.

For example, the logical interface 1/1/4 in software is associated with physical port 4 on member 1.

**On the 6400 Switch Series**

- **member:** Always 1. VSF is not supported on this switch.
- **slot:** Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/1 and 1/2.
  - Line modules are on the front of the switch starting in slot 1/3.
- **port:** Physical number of a port on a line module.

For example, the logical interface 1/3/4 in software is associated with physical port 4 in slot 3 on member 1.

**Identifying modular switch components**

- Power supplies are on the front of the switch behind the bezel above the management modules. Power supplies are labeled in software in the format: **member/power supply**:
  - **member:** 1.
  - **power supply:** 1 to 4.
- Fans are on the rear of the switch and are labeled in software as: **member/tray/fan**:
  - **member:** 1.
  - **tray:** 1 to 4.
  - **fan:** 1 to 4.
- Fabric modules are not labeled on the switch but are labeled in software in the format: **member/module**:
  - **member:** 1.
  - **member:** 1 or 2.
- The display module on the rear of the switch is not labeled with a member or slot number.
ICMP Router Discovery Protocol (IRDP), an extension of the ICMP, is independent of any routing protocol. It allows hosts to discover the IP addresses of neighboring routers that can act as default gateways to reach devices on other IP networks.

**IRDP operation**

IRDP uses the following types of ICMP messages:

- **Router advertisement (RA):** Sent by a router to advertise IP addresses (including the primary and secondary IP addresses) and preference.
- **Router solicitation (RS):** Sent by a host to request the IP addresses of routers on the subnet.

An interface with IRDP enabled periodically broadcasts or multicasts an RA message to advertise its IP addresses. A receiving host adds the IP addresses to its routing table, and selects the IP address with the highest preference as the default gateway.

When a host attached to the subnet starts up, the host multicasts an RS message to request immediate advertisements. If the host does not receive any advertisements, it retransmits the RS several times. If the host does not discover the IP addresses of neighboring routers because of network problems, the host can still discover them from periodic RAs.

IRDP allows hosts to discover neighboring routers, but it does not suggest the best route to a destination. If a host sends a packet to a router that is not the best next hop, the host will receive an ICMP redirect message from the router.

**IP address preference**

Every IP address advertised in RAs has a preference value. A larger preference value represents a higher preference. The IP address with the highest preference is selected as the default gateway address.

You can specify the preference for IP addresses to be advertised on a router interface.

An address with the minimum preference value (-2147483648) will not be used as a default gateway address.

**Lifetime of an IP address**

An RA contains a lifetime field that specifies the lifetime of advertised IP addresses. If the host does not receive a new RA for an IP address within the address lifetime, the host removes the route entry.

All the IP addresses advertised by an interface have the same lifetime.

**Advertising interval**

A router interface with IRDP enabled sends out RAs randomly between the minimum and maximum advertising intervals. This mechanism prevents the local link from being overloaded by a large number of RAs sent simultaneously from routers.

As a best practice, shorten the advertising interval on a link that suffers high packet loss rates

**Destination address of RA**

An RA uses either of the following destination IP addresses:
- Broadcast address 255.255.255.255.
- Multicast address 224.0.0.1, which identifies all hosts on the local link.

By default, the destination IP address of an RA is the multicast address. If all listening hosts in a local area network support IP multicast, specify 224.0.0.1 as the destination IP address.

**Proxy-advertised IP addresses**

By default, an interface advertises its primary and secondary IP addresses. You can specify IP addresses of other gateways for an interface to proxy-advertise.

**VRF support**

In IP-based computer networks, virtual routing and forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

IRDP is VRF aware. As the router advertisements and solicit processing occurs on the interface, packet is through the interface and corresponding VRF.

**VSX synchronization**

IRDP supports VSX synchronization. For more information on using VSX, see the Virtual Switching Extension (VSX) Guide for your switch and software version

**Configuring IRDP**

**Prerequisites**

A layer 3 interface.

**Procedure**

1. Enable IRDP on an interface with the command `ip irdp`.
2. Set the maximum hold time with the command `ip irdp holdtime`.
3. Set the maximum router advertisement interval with the command `ip irdp maxadvertinterval`.
4. Set the minimum router advertisement interval with the command `ip irdp minadvertinterval`.
5. Set the IRDP preference level with the command `ip irdp preference`.
6. Review IRDP configuration settings with the command `show ip irdp`.

**Example**

This example creates the following configuration:

- Enables IRDP on the layer 3 interface 1/1/1 with packet type set to broadcast.
- Sets the hold time to 5000 seconds.
- Sets the advertisement interval to 30 seconds.
- Sets the minimum advertisement interval to 25 seconds.
- Sets the IRDP preference level to 25.

```bash
switch(config)# interface 1/1/1
switch(config-if)# ip irdp broadcast
```
IRDP commands

diag-dump irdp basic
diag-dump irdp basic

Description
Displays diagnostic information for IRDP.

Example
On the 6400 Switch Series, interface identification differs.

```
switch# diag-dump irdp basic
=========================================================================  
[Start] Feature irdp Time: Thu Jun 8 09:50:28 2017
=========================================================================  
[Start] Daemon hpe-rdiscd
-------------------------------------------------------------------------
Interface: 1/1/1 (state: Up)
rdisc ipv4 (enabled: 0, max:600, min:450, hold:1800, pref:0, isBcast:0)
Router IPs: 192.168.1.2,
Interface: 1/1/2 (state: Up)
rdisc ipv4 (enabled: 0, max:600, min:450, hold:1800, pref:0, isBcast:0)
Router IPs: 192.168.2.2,
-------------------------------------------------------------------------
[End] Daemon hpe-rdiscd
-------------------------------------------------------------------------
[End] Feature irdp
-------------------------------------------------------------------------
Diagnostic dump captured for feature irdp
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
**ip irdp**

Parameters:
- `broadcast`
- `multicast`

**Description**

Enables IRDP on an interface and specifies the packet type that is used to send advertisements. By default, the packet type is set to `multicast`. IRDP is only supported on layer 3 interfaces. The **no** form of this command disables IRDP on an interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Advertisements are sent as broadcast packets to IP address 255.255.255.255.</td>
</tr>
<tr>
<td>multicast</td>
<td>Advertisements are sent as multicast packets to the multicast group with IP address 240.0.0.1. Default.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Enabling IRDP on interface 1/1/1 with packet type set to the default value (multicast).

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp
```

Enabling IRDP on interface 1/1/1 with packet type set to broadcast.

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp broadcast
```

Disabling IRDP.

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip irdp holdtime**

Parameters:
- `<TIME>`
no ip irdp holdtime <TIME>

Description
Specifies the maximum amount of time the host will consider an advertisement to be valid until a newer advertisement arrives. When a new advertisement arrives, hold time is reset. Hold time must be greater than or equal to the maximum advertisement interval. Therefore, if the hold time for an advertisement expires, the host can reasonably conclude that the router interface that sent the advertisement is no longer available. The default hold time is three times the maximum advertisement interval.

The no form of this command removes the specified maximum amount of time the host will consider an advertisement to be valid until a newer advertisement arrives and update it to the default value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies the lifetime of router advertisements sent from this interface. Range: 4 to 9000 seconds. Default: 1800 seconds.</td>
</tr>
</tbody>
</table>

Example
On the 6400 Switch Series, interface identification differs.
Setting the hold time for interface 1/1/1 to 5000 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp holdtime 5000
```

Removing the the hold time for interface 1/1/1 to 5000 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp holdtime 5000
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

ip irdp maxadvertinterval

```
ip irdp maxadvertinterval <TIME>
no ip irdp maxadvertinterval <TIME>
```

Description
Specifies the maximum router advertisement interval.
The no form of this command removes the specified maximum router advertisement interval and reverts to the default value.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies the maximum time allowed between the sending of unsolicited router advertisements. Range: 4 to 1800 seconds. Default: 600 seconds.</td>
</tr>
</tbody>
</table>

**Example**

*On the 6400 Switch Series, interface identification differs.*

Setting the advertisement interval for interface 1/1/1 to 30 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp maxadvertinterval 30
```

Removing the advertisement interval for interface 1/1/1 to 30 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp maxadvertinterval 30
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip irdp minadvertinterval**

```
ip irdp minadvertinterval <TIME>
no ip irdp minadvertinterval <TIME>
```

**Description**

Specifies the minimum amount of time the switch waits between sending router advertisements. By default, this value is automatically set by the switch to be 75% of the value configured for maximum router advertisement interval. Use this command to override the automatically configured value.

The `no` form of this command removes the specified minimum amount of time the switch waits between sending router advertisements and reverts to the default value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies the minimum time allowed between the sending of unsolicited router advertisements. Range: 3 to 1800 seconds. Default: 450 seconds (75% of the default value for maximum router advertisement interval).</td>
</tr>
</tbody>
</table>
Example

On the 6400 Switch Series, interface identification differs.
Setting the minimum advertisement interval for interface 1/1/1 to 25 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp minadvertinterval 25
```

Removing the minimum advertisement interval for interface 1/1/1 to 25 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp minadvertinterval 25
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip irdp preference**

ip irdp preference <LEVEL>
no ip irdp preference <LEVEL>

Description

Specifies the IRDP preference level. If a host receives multiple router advertisement messages from different routers, the host selects the router that sent the message with the highest preference as the default gateway.

The no form of this command removes the specified IRDP preference level and reverts to the default value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;LEVEL&gt;</td>
<td>Specifies the IRDP preference level. Range: -2147483648 to 2147483647. Default: 0.</td>
</tr>
</tbody>
</table>

Example

On the 6400 Switch Series, interface identification differs.
Setting the IRDP preference level for interface 1/1/1 to 25.

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp preference 25
```

Removing the IRDP preference level for interface 1/1/1 to 25.
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp preference 25

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show ip irdp

show ip irdp [vsx-peer]

Description
Displays IRDP configuration settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| <location> | Specifies one of these values:  
  - <FQDN>: a fully qualified domain name.  
  - <IPV4>: an IPv4 address.  
  - <IPV6>: an IPv6 address.  |

vsx-peer
Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example
On the 6400 Switch Series, interface identification differs.

switch# show ip irdp

ICMP Router Discovery Protocol

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Advertising Address</th>
<th>Minimum Interval</th>
<th>Maximum Interval</th>
<th>Holdtime</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Enabled</td>
<td>multicast</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Disabled</td>
<td>multicast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>0</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Enabled</td>
<td>broadcast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>115</td>
</tr>
</tbody>
</table>

Command History
### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
IPv6 RA provides a method for local IPv6 hosts to automatically configure their own IP address (and other settings such as a preferred DNS server) based on information advertised by switches/routers operating on the network.

### IPv6 flags

Behavior of IPv6 hosts to IPv6 RA messages is controlled by the managed address configuration flag (M flag), and other stateful configuration flag (O flag).

<table>
<thead>
<tr>
<th>M flag</th>
<th>O flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Indicates that no information is available via DHCPv6.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Indicates that other configuration information is available via DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Indicates that addresses are available via Dynamic Host Configuration Protocol (DHCPv6).</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.</td>
</tr>
</tbody>
</table>

### Configuring IPv6 RA

#### Procedure

1. Enable transmission of IPv6 router advertisements with the command `no ipv6 nd suppress-ra`.
2. Optionally, configure IPv6 unicast address prefixes with the command `ipv6 nd prefix`.
3. Optionally, configure support for DNS name resolution with the commands `ipv6 nd ra dns server` and `ipv6 nd ra dns search-list`.
4. For most deployments, the default values for the following features do not need to be changed. If your deployment requires different settings, change the default values with the indicated command:

<table>
<thead>
<tr>
<th>IPv6 RA setting</th>
<th>Default value</th>
<th>Command to change it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of neighbor solicitations to be sent when performing DAD.</td>
<td>1</td>
<td><code>ipv6 nd dad attempts</code></td>
</tr>
<tr>
<td>Number of neighbor entries in the ND cache.</td>
<td>131072</td>
<td><code>ipv6 nd cache-limit</code></td>
</tr>
<tr>
<td>Hop limit to be sent in the RA messages.</td>
<td>64</td>
<td><code>ipv6 nd hop-limit</code></td>
</tr>
<tr>
<td>IPv6 RA setting</td>
<td>Default value</td>
<td>Command to change it</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>MTU value to be sent in the RA messages.</td>
<td>1500 bytes</td>
<td>ipv6 nd mtu</td>
</tr>
<tr>
<td>Neighbor solicitation interval</td>
<td>1000 milliseconds</td>
<td>ipv6 nd ns-interval</td>
</tr>
<tr>
<td>Lifetime of a default router.</td>
<td>1800 seconds</td>
<td>ipv6 nd ra lifetime</td>
</tr>
<tr>
<td>Retrieval of an IPv6 address by devices.</td>
<td>Disabled</td>
<td>ipv6 nd ra managed-config-flag</td>
</tr>
<tr>
<td>Maximum interval between transmissions of IPv6 RAs.</td>
<td>600 seconds</td>
<td>ipv6 nd ra max-interval</td>
</tr>
<tr>
<td>Minimum interval between transmissions of IPv6 RAs.</td>
<td>200 seconds</td>
<td>ipv6 nd ra min-interval</td>
</tr>
<tr>
<td>Time that an interface considers a device to be reachable.</td>
<td>0 milliseconds (no limit)</td>
<td>ipv6 nd ra reachable-time</td>
</tr>
<tr>
<td>Retry period between ND solicitations.</td>
<td>0 (Use locally configured NS-interval)</td>
<td>ipv6 nd ra retrans-timer</td>
</tr>
<tr>
<td>Default routing preference for an interface.</td>
<td>Medium</td>
<td>ipv6 nd router-preference</td>
</tr>
</tbody>
</table>

5. **Review IPv6 RA configuration settings with the commands** `show ipv6 nd interface`, `show ipv6 nd interface prefix`, `show ipv6 nd ra dns server`, and `show ipv6 nd ra dns search-list`.

**Example**

*On the 6400 Switch Series, interface identification differs.*

This example creates the following configuration:

- Enables IPv6 RA on interface 1/1/3.
- Sets the recursive DNS server address to 4001::1 with a lifetime of 400 seconds.
- Sets the minimum interval between transmissions to 3 seconds.
- Sets the maximum interval between transmissions to 13 seconds.
- Sets the lifetime of a default router to 1900 seconds.

```
switch(config)# interface 1/1/3
switch(config-if)# no ipv6 nd suppress-ra
switch(config-if)# ipv6 nd ra dns server 4001::1 lifetime 400
switch(config-if)# ipv6 nd ra min-interval 3
switch(config-if)# ipv6 nd ra max-interval 13
switch(config-if)# ipv6 nd ra lifetime 1900
switch(config-if)# end
switch# show ipv6 nd interface 1/1/3
```

Interface 1/1/3 is up
Admin state is up
IPv6 address: 2006::1/64 [VALID]
IPv6 link-local address: fe80::98f2:b321:368:6dc6/64 [VALID]
ICMPv6 active timers:
   Last Router-Advertisement sent: 0 Secs
Next Router-Advertisement sent in: 13 Secs

Router-Advertisement parameters:
- Periodic interval: 3 to 13 secs
- Router Preference: medium
- Send "Managed Address Configuration" flag: false
- Send "Other Stateful Configuration" flag: false
- Send "Current Hop Limit" field: 64
- Send "MTU" option value: 1500
- Send "Router Lifetime" field: 1900
- Send "Reachable Time" field: 0
- Send "Retrans Timer" field: 0
- Suppress RA: false
- Suppress MTU in RA: true

ICMPv6 error message parameters:
- Send redirects: false

ICMPv6 DAD parameters:
- Current DAD attempt: 1

switch# show ipv6 nd ra dns server
Recursive DNS Server List on: 1/1/3
Suppress DNS Server List: No
DNS Server 1: 2001::1 lifetime 400

**IPv6 RA scenario**

In this scenario, two host computers are auto-configured with IP addresses using IPv6 RA. In addition, the switch provides the hosts with an address of a recursive DNS server. The physical topology of the network looks like this:

![Network Topology Diagram]

On the 6400 Switch Series, interface identification differs.

**Procedure**

1. Configure the interfaces with IPv6 addresses.
   
   ```
   switch# config
   switch(config)# interface 1/1/1
   switch(config-if)# ipv6 address 2001::1/64
   switch(config)# interface 1/1/2
   switch(config-if)# ipv6 address 3001::1/64
   switch(config)# interface 1/1/3
   switch(config-if)# ipv6 address 4001::1/64
   ```

2. Enable transmission of all IPv6 RA messages.
   
   ```
   switch(config-if)# no ipv6 nd suppress-ra
   ```
**IPv6 RA commands**

**ipv6 address <global-unicast-address>**

`ipv6 address <global-unicast-address>`
`no ipv6 address <global-unicast-address>`

**Description**

Sets a global unicast address on the interface.
The `no` form of this command removes the global unicast address on the interface.

This command automatically creates an IPv6 link-local address on the interface. However, it does not add the `ipv6 address link-local` command to the running configuration. If you remove the IPv6 address, the link-local address is also removed. To maintain the link-local address, you must manually execute the `ipv6 address link-local` command.

**Example**

*On the 6400 Switch Series, interface identification differs.*

Enabling a global unicast address:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 address 3731:54:65fe:2::a7
```

Disabling a global unicast address:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 address 3731:54:65fe:2::a7
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**ipv6 address autoconfig**

`ipv6 address autoconfig`
`no ipv6 address autoconfig`

**Description**

Enables the interface to automatically obtain an IPv6 address using router advertisement information and the EUI-64 identifier.
The `no` form of this command disables address auto-configuration.

- A maximum of 15 autoconfigured addresses are supported.
- This command automatically creates an IPv6 link-local address on the interface. However, it does not add the `ipv6 address link-local` command to the running configuration. If you remove the IPv6 address, the link-local address is also removed. To maintain the link-local address, you must manually execute the `ipv6 address link-local` command.

**Usage**

The IPv6 SLAAC feature lets the router obtain the IPv6 address for the interface it is configured through the SLAAC method. This feature is not available on the `mgmt` VRF.

**Example**

*On the 6400 Switch Series, interface identification differs.*

Enabling unicast autoconfiguring:

```plaintext
switch(config)# interface 1/1/1
switch(config-if)# ipv6 address autoconfig
```

Disabling unicast autoconfiguring:

```plaintext
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 address autoconfig
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (<code>&gt;</code> only).</td>
</tr>
</tbody>
</table>

`ipv6 address link-local`

`ipv6 address link-local [IPv6-ADDR/MASK]`

**Description**

Enables IPv6 on the current interface. If no address is specified, an IPv6 link-local address is auto-generated for the interface. If an address is specified, auto-configuration is disabled and the specified address/mask is assigned to the interface.

To disable IPv6 link-local on the interface, remove `ipv6 address link-local`, `ipv6 address <global-ipv6-address>`, and `ipv6 address autoconfig` from the interface.
This feature is not available on the management VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6 ADDR&gt;</td>
<td>Specifies the IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. You can use two colons (:) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:4444:0055 becomes 2222:0:3333::4444:55.</td>
</tr>
<tr>
<td>&lt;MASK&gt;</td>
<td>Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.</td>
</tr>
</tbody>
</table>

**Example**

On the 6400 Switch Series, interface identification differs.

Enabling IPv6 link-local on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 address link-local
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**ipv6 nd cache-limit**

```
ipv6 nd cache-limit <CACHELIMIT>
no ipv6 nd cache-limit [ <CACHELIMIT> ]
```

**Description**

Configures the limit on the number of neighbor entries in the ND cache. The no form of this command sets the cache limit to the default value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
**Examples**

Setting the cache limit to 20.

```
switch(config)# ipv6 nd cache-limit 20
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd dad attempts**

```
ipv6 nd dad attempts <NUM-ATTEMPTS>
no ipv6 nd dad attempts [<NUM-ATTEMPTS>]
```

**Description**

Configures the number of neighbor solicitations to be sent when performing duplicate address detection (DAD) for a unicast address configured on an interface.

The `no` form of this command sets the number of attempts to the default value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd dad attempts 5
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
### ipv6 nd hop-limit

**ipv6 nd hop-limit** `<HOPLIMIT>`
no ipv6 nd hop-limit `[<HOPLIMIT>]`

**Description**

Configures the hop limit to be sent in RAs.

The `no` form of this command resets the hop limit to 0. This reset eliminates the hop limit from the RAs that originate on the interface, so the host determines the hop limit.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>hop-limit </code>&lt;HOPLIMIT&gt;`</td>
<td>Specifies the hop limit. Range: 0-255. Default: 64.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd hop-limit 64
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### ipv6 nd mtu

**ipv6 nd mtu** `<MTU-VALUE>`
nno ipv6 nd mtu `[<MTU-VALUE>]`

**Description**

Configures the MTU size to be sent in the RA messages.

The `no` form of this command sets hop limit to the default value.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

### Examples

*On the 6400 Switch Series, interface identification differs.*

switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd mtu 1300

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### ipv6 nd ns-interval

*ipv6 nd ns-interval <TIME>*

*no ipv6 nd ns-interval [<TIME>]*

### Description

Configures the ND time between DAD neighbor solicitations sent for an unresolved destination, or between duplicate address detection neighbor solicitation requests. Increase this setting when neighbor solicitation retries or failures are occurring, or in a slow (WAN) network.

The *no* form of this command sets the ns-interval to the default value.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

### Examples

*On the 6400 Switch Series, interface identification differs.*

switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ns-interval 1200
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd prefix**

ipv6 nd prefix `<IPV6-ADDR>/<PREFIX-LEN>`
```bash
[no-advertise | [valid <LIFETIME-VALUE> preferred <LIFETIME-VALUE>] | no-autoconfig | no-onlink]
```

no ipv6 nd prefix `<IPV6-ADDR>/<PREFIX-LEN>` [no-advertise | [valid <LIFETIME-VALUE> preferred <LIFETIME-VALUE>] | no-autoconfig | no-onlink]

ipv6 nd prefix default [no-advertise | [valid <LIFETIME-VALUE> preferred <LIFETIME-VALUE>] | no-autoconfig | no-onlink]

no ipv6 nd prefix default [no-advertise | [valid <LIFETIME-VALUE> preferred <LIFETIME-VALUE>] | no-autoconfig | no-onlink]

**Description**

Specifies prefixes for the routing switch to include in RAs transmitted on the interface. IPv6 hosts use the prefixes in RAs to autoconfigure themselves with global unicast addresses. The autoconfigured address of a host is composed of the advertised prefix and the interface identifier in the current link-local address of the host.

By default, advertise, autoconfig, and onlink are set.

The no form of this command removes the configuration on the interface.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV6-ADDR&gt;/&lt;PREFIX-LEN&gt;</code></td>
<td>Specifies the IPv6 prefix to advertise in RA. Format: XX:XX::X/M</td>
</tr>
<tr>
<td>default</td>
<td>Specifies apply configuration to all on-link prefixes that are not individually set by the ipv6 ra prefix <code>&lt;IPV6-ADDR&gt;/&lt;PREFIX-LEN&gt;</code> command. It applies the same valid and preferred lifetimes, link state, autoconfiguration state, and advertise options to the advertisements sent for all on-link prefixes that are not individually configured with a unique lifetime. This also applies to the prefixes for any global unicast addresses configured later on the same interface. Using default once, and then using it again with any new parameter values results in the new values replacing the former values in advertisements. If default is used without the no-advertise, no-autoconfig, or no-onlink parameter, the advertisement setting for the absent parameter is returned to its default setting.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-advertise</td>
<td>Specifies do not advertise prefix in RA.</td>
</tr>
<tr>
<td>valid &lt;LIFETIME-VALUE&gt;</td>
<td>Specifies the total time, in seconds, the prefix remains available before becoming unusable. After preferred-lifetime expiration, any autoconfigured address is deprecated and used only for transactions only before preferred-lifetime expires. If the valid lifetime expires, the address becomes invalid. You can enter a value in seconds or enter valid infinite which sets infinite lifetime. Default: 2,592,000 seconds which is 30 days. Range: 0–4294967294 seconds.</td>
</tr>
<tr>
<td>preferred &lt;LIFETIME-VALUE&gt;</td>
<td>Specifies the span of time during which the address can be freely used as a source and destination for traffic. This setting must be less than or equal to the corresponding valid-lifetime setting. You can enter a value in seconds or enter preferred infinite which sets infinite lifetime. Default: 604,800 seconds which is seven days. Range: 0–4294967294 seconds.</td>
</tr>
<tr>
<td>no-autoconfig</td>
<td>Specifies do not use prefix for autoconfiguration.</td>
</tr>
<tr>
<td>no-onlink</td>
<td>Specifies do not use prefix for onlink determination.</td>
</tr>
</tbody>
</table>

### Examples

**On the 6400 Switch Series, interface identification differs.**

```plaintext
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd prefix 4001::1/64 valid 30 preferred 10 no-autoconfig no-onlink
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd ra dns search-list**

*ipv6 nd ra dns search-list <DOMAIN-NAME>  [lifetime <TIME>]*

*no ipv6 nd ra dns search-list <DOMAIN-NAME>*

### Description

Configures the DNS Search List (DNSSL) to include in Router Advertisements (RAs) transmitted on the interface.

The no form of this command removes the DNS Search List from the RAs transmitted on the interface.
### IPv6 nd ra dns server

**Description**
Configures the IPv6 address of a preferred Recursive DNS Server (RDNSS) to be included in Router Advertisements (RAs) transmitted on the interface.

The **no** form of this command removes the configured DNS server from the RAs transmitted on the interface.

#### Parameter | Description
--- | ---
<IPV6-ADDR> | Specifies the RDNSS address in IPv6 format ([xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]), where x is a hexadecimal number from 0 to F. You can use two colons (:) to represent consecutive zeros (but only once), remove leading
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

**Usage**

- Including RDNSS information in RAs provides DNS server configuration for connected IPv6 hosts without requiring DHCPv6.
- Multiple servers can be configured on the interface by using the command repeatedly.
- A maximum of eight server addresses are allowed.

**Examples**

*On the 6400 Switch Series, interface identification differs.*

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns server 2001::1 lifetime 400
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd ra lifetime**

`ipv6 nd ra lifetime <TIME>`

no `ipv6 nd ra lifetime [<TIME>]`

**Description**

Configures the lifetime, in seconds, for the routing switch to be used as a default router by hosts on the current interface.

The `no` form of this command sets lifetime to the default of 1800 seconds.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

**Usage**

- A given host on an interface refreshes the default router lifetime for a specific router each time the host receives an RA from that router.
- A specific router ceases to be a default router candidate for a given host if the default router lifetime expires before the host is updated with a new RA from the router.

**Examples**

*On the 6400 Switch Series, interface identification differs.*

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra lifetime 1200
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`ipv6 nd ra managed-config-flag`

**Description**

Controls the M flag setting in RAs the router transmits on the current interface. Enable the M flag to indicate that hosts can obtain IP address through DHCPv6. The M flag is disabled by default.

The `no` form of this command turns off (disables) the M flag.

**Usage**

- Enabling the M flag directs hosts to acquire their IPv6 addressing for the current interface from a DHCPv6 server.
- When the M-bit is enabled, receiving hosts ignore the O flag setting, which is configured using the
command ipv6 nd ra other-config-flag.

- When the M-bit is disabled (the default), receiving hosts expect to receive their IPv6 addresses from RA.

<table>
<thead>
<tr>
<th>M flag</th>
<th>O flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Indicates that no information is available via DHCPv6.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Indicates that other configuration information is available via DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Indicates that addresses are available via Dynamic Host Configuration Protocol (DHCPv6).</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.</td>
</tr>
</tbody>
</table>

Examples

*On the 6400 Switch Series, interface identification differs.*

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra managed-config-flag
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd ra max-interval**

ipv6 nd ra max-interval <TIME>
no ipv6 nd ra max-interval [<TIME>]

Description

Configures the maximum interval between transmissions of IPv6 RAs on the interface. The interval between RA transmissions on an interface is a random value that changes every time an RA is sent. The interval is calculated to be a value between the current max-interval and min-interval settings.

The no form of this command returns the setting to its default, provided the default value is less than the default lifetime value.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies the maximum advertisement time in seconds. Range: 4-1800. Default: 600 seconds.</td>
</tr>
</tbody>
</table>

**Usage**

- This value has one setting per interface. The setting does not apply to RAs sent in response to a router solicitation received from another device.
- Attempting to set max-interval to a value that is not sufficiently larger than the current min-interval also results in an error message.

**Examples**

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra max-interval 30
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd ra min-interval**

ipv6 nd ra min-interval <TIME>
no ipv6 nd ra min-interval [<TIME>]

**Description**

Configures the minimum interval between transmissions of IPv6 RAs on the interface. The interval between RA transmissions on an interface is a random value that changes every time an RA is sent. The interval is calculated to be a value between the current max-interval and min-interval settings.

The no form of this command returns the setting to its default, provided the default value is less than the current max-interval setting.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies a minimum advertisement time in seconds. Range: 3-1350. Default: 200 seconds.</td>
</tr>
</tbody>
</table>

**Usage**
This value has one setting per interface and does not apply to RAs sent in response to a router solicitation received from another device.

The min-interval must be less than the max-interval. Attempting to set min-interval to a higher value results in an error message.

Examples

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra min-interval 25
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

```
ipv6 nd ra other-config-flag
```

```
no ipv6 nd ra other-config-flag
```

Description

Controls the O-bit in RAs the router transmits on the current interface; but is ignored unless the M-bit is disabled in RAs. Configure to set the O-bit in RA messages for host to obtain network parameters through DHCPv6. The other-config-flag is disabled by default.

For more information on configuring the M-bit, see `ipv6 nd ra managed-config-flag`.

The no form of this command turns off (disables) the setting for this command in RAs.

Usage

Enabling the O-bit while the M-bit is disabled directs hosts on the interface to acquire their other configuration information from DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.

Examples

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra other-config-flag
```

Command History
ipv6 nd ra reachable-time
ipv6 nd ra reachable-time <TIME>
no ipv6 nd ra reachable-time [<TIME>]

Description
Sets the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.
The no form of this command sets the reachable time to the default value of 0. (no limit).

Parameter | Description
--- | ---
<TIME> | Specifies the reachable time in milliseconds. Range: 1000-3600000. Default: 0 (no limit).

Examples
On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra reachable-time 2000
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

ipv6 nd ra retrans-timer
ipv6 nd ra retrans-timer <TIME>
no ipv6 nd ra retrans-timer [<TIME>]

Description
Configures the period (retransmit timer) between ND solicitations sent by a host for an unresolved destination, or between DAD neighbor solicitation requests. By default, hosts on the interface use their own locally configured NS-interval settings instead of using the value received in the RAs.

Increase this timer when neighbor solicitation retries or failures are occur, or in a "slow" (WAN) network. The no form of this command sets the value to the default of 0.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Specifies the retransmit timer value in milliseconds. Range: 0 - 4294967295 milliseconds. Default: 0 (Use locally configured NS-interval).</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra retrans-timer 400
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd router-preference**

```
ipv6 nd router-preference {high | medium | low}
no ipv6 nd router-preference [high | medium | low]
```

**Description**

Specifies the value that is set in the Default Router Preference (DRP) field of Router Advertisements (RAs) that the switch sends from an interface. An interface with a DRP value of high will be preferred by other devices on the network over interfaces with an RA value of medium or low.

The no form of this command set the value to the default of medium.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>high</td>
<td>Sets DRP to high.</td>
</tr>
<tr>
<td>medium</td>
<td>Sets DRP to medium. Default.</td>
</tr>
<tr>
<td>low</td>
<td>Sets DRP to low.</td>
</tr>
</tbody>
</table>

**Examples**
On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd router-preference high
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 nd suppress-ra**

ipv6 nd suppress-ra [SUPPRESS-OPTION]

no ipv6 nd ra suppress-ra [SUPPRESS-OPTION]

### Description

Configures suppression of IPv6 Router Advertisement transmissions on an interface. The `no` form of this command restores transmission of IPv6 Router Advertisement and options.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>suppress-ra [SUPPRESS-OPTION]</td>
<td>Specifies suppressing RA transmissions. Entering <code>suppress-ra</code> without any options, suppresses all RA messages (default). Or you can enter one of the following options.</td>
</tr>
<tr>
<td>dnsssl</td>
<td>Specifies suppressing DNSSSL options in RA messages.</td>
</tr>
<tr>
<td>mtu</td>
<td>Specifies suppressing MTU options in RA messages.</td>
</tr>
<tr>
<td>rdnss</td>
<td>Specifies suppressing RDNSS options in RA messages.</td>
</tr>
</tbody>
</table>

### Examples

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd suppress-ra mtu dnsssl rdnss
switch(config-if)# no ipv6 nd suppress-ra mtu dnsssl rdnss
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show ipv6 nd global traffic**

show ipv6 nd global traffic [vsx-peer]

**Description**

Displays IPv6 Neighbor Discovery traffic details on a device.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

```plaintext
switch# show ipv6 nd global traffic
ICMPv6 packet Statistics (sent/received)
  Total Messages : 18/0
  Error Messages : 0/0
  Destination Unreachables : 0/0
  Time Exceeded : 0/0
  Parameter Problems : 0/0
  Echo Request : 0/0
  Echo Replies : 0/0
  Redirects : 0/0
  Packet Too Big : 0/0
  Router Advertisements : 4/0
  Router Solicitations : 0/0
  Neighbor Advertisements : 0/0
  Neighbor Solicitations : 3/0
  Duplicate router RA received : 0/0
ICMPv6 MLD Statistics (sent/received)
  V1 Queries : 0/0
  V2 Queries : 0/0
  V1 Reports : 0/0
  V2 Reports : 11/0
  V1 Leaves : 0/0
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
### Platforms | Command context | Authority
--- | --- | ---
All platforms | Operator (>) or Manager(#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

**show ipv6 nd interface**

*show ipv6 nd interface [<IF-NAME> | all-vrfs | vrf <VRF-NAME>] [vsx-peer]*

**Description**
Displays neighbor discovery information for an interface. If no options are specified, displays information for the default VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IF-NAME&gt;</code></td>
<td>Displays information about the specified IPv6 enabled interface.</td>
</tr>
<tr>
<td>all-vrfs</td>
<td>Displays information about interfaces in all VRFs.</td>
</tr>
<tr>
<td>vrf <code>&lt;VRF-NAME&gt;</code></td>
<td>Displays information about interfaces in a particular VRF. Or, if <code>&lt;VRF-NAME&gt;</code> is not specified, information for the default VRF is displayed.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**
*On the 6400 Switch Series, interface identification differs.*
Showing information for all VRFs:

```
switch# show ipv6 nd interface all-vrfs
List of IPv6 Interfaces for VRF default
Interface 1/1/1 is up
  Admin state is up
  IPv6 address:
  IPv6 link-local address: fe80::7272:ffff:feef:a8b9/64 [VALID]
  ICMPv6 active timers:
    Last Router-Advertisement sent:
    Next Router-Advertisement sent in:
  Router-Advertisement parameters:
    Periodic interval: 200 to 600 secs
    Router Preference: medium
    Send "Managed Address Configuration" flag: false
    Send "Other Stateful Configuration" flag: false
    Send "Current Hop Limit" field: 64
    Send "MTU" option value: 1500
    Send "Router Lifetime" field: 1800
    Send "Reachable Time" field: 0
    Send "Retrans Timer" field: 0
    Suppress RA: true
```
Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1

List of IPv6 Interfaces for VRF red
Interface 1/1/2 is up
  Admin state is up
  IPv6 address:
    2001::1/64 [VALID]
  IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
ICMPv6 active timers:
  Last Router-Advertisement sent:
  Next Router-Advertisement sent in:
Router-Advertisement parameters:
  Periodic interval: 200 to 600 secs
  Router Preference: medium
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1800
  Send "Reachable Time" field: 0
  Send "Retrans Timer" field: 0
  Suppress RA: true
  Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1

Showing information for interface 1/1/1:

```
switch# show ipv6 nd interface 1/1/1
Interface 1/1/1 is up
  Admin state is up
  IPv6 address:
    IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
ICMPv6 active timers:
  Last Router-Advertisement sent:
  Next Router-Advertisement sent in:
Router-Advertisement parameters:
  Periodic interval: 200 to 600 secs
  Router Preference: high
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1800
  Send "Reachable Time" field: 0
  Send "Retrans Timer" field: 0
  Suppress RA: true
  Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1
```

Showing information for the default VRF:
switch# show ipv6 nd interface

List of IPv6 Interfaces for VRF default
Interface 1/1/1 is up
   Admin state is up
   IPv6 address:
      2001::1/64 [VALID]
   IPv6 link-local address: fe80::7272:ffff:fee7:a8b9/64 [VALID]
   ICMPv6 active timers:
      Last Router-Advertisement sent: 6 Secs
      Next Router-Advertisement sent in: 7 Secs
   Router-Advertisement parameters:
      Periodic interval: 3 to 13 secs
      Router Preference: medium
      Send "Managed Address Configuration" flag: false
      Send "Other Stateful Configuration" flag: false
      Send "Current Hop Limit" field: 64
      Send "MTU" option value: 1500
      Send "Router Lifetime" field: 1900
      Send "Reachable Time" field: 0
      Send "Retrans Timer" field: 0
      Suppress RA: true
      Suppress MTU in RA: true
   ICMPv6 error message parameters:
      Send redirects: false
   ICMPv6 DAD parameters:
      Current DAD attempt: 1

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show ipv6 nd interface prefix

show ipv6 nd interface prefix [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Shows IPv6 prefix information for all VRFs or a specific VRF. If no options are specified, shows information for the default VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-vrfs</td>
<td>Shows prefix information for all VRFs.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Name of a VRF.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

### Examples

*On the 6400 Switch Series, interface identification differs.*

Showing prefix information for the default VRF:

```
switch# show ipv6 nd interface prefix
```

List of IPv6 Interfaces for VRF default
List of IPv6 Prefix advertised on 1/1/1
  Prefix : 4545::/65
  Enabled : Yes
  Validlife time : 2592000
  Preferred lifetime : 604800
  On-link : Yes
  Autonomous : Yes

Showing information for VRF red:

```
switch# show ipv6 nd interface prefix vrf red
```

List of IPv6 Interfaces for VRF red
List of IPv6 Prefix advertised on 1/1/2
  Prefix : 2001::/64
  Enabled : Yes
  Validlife time : 2592000
  Preferred lifetime : 604800
  On-link : Yes
  Autonomous : Yes

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (+)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; ) only.</td>
</tr>
</tbody>
</table>

**show ipv6 nd ra dns search-list**

show ipv6 nd ra dns search-list [vsx-peer]
Description
Displays domain name information on all interfaces.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

Examples

*On the 6400 Switch Series, interface identification differs.*

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns search-list test.com
switch# show ipv6 nd ra dns search-list
Recursive DNS Search List on: 1
  Suppress DNS Search List: Yes
  DNS Search 1: test.com  lifetime 1800
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

`show ipv6 nd ra dns server`

*show ipv6 nd ra dns server [vsx-peer]*

Description
Displays DNS server information on all interfaces.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

Examples
On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns server 2001::1
switch# show ipv6 nd ra dns server
Recursive DNS Server List on: 1
  Suppress DNS Server List: Yes
  DNS Server 1: 2001::1  lifetime 1800
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
sFlow is a technology for monitoring traffic in switched or routed networks. The sFlow monitoring system is comprised of:

- An sFlow Agent that runs on a network device, such as a switch. The agent uses sampling techniques to capture information about the data traffic flowing through the device and forwards this information to an sFlow collector.
- An sFlow Collector that receives monitoring information from sFlow agents. The collector stores this information so that a network administrator can analyze it to understand network data flow patterns. One sFlow collector can receive the data from many sFlow agents.

The sFlow UDP datagrams sent to a collector are not encrypted, therefore any sensitive information contained in an sFlow sample is exposed.

**sFlow agent**

The sFlow agent on the switch provides ingress sampling of all forwarded layer 2 and layer 3 traffic on LAG and Ethernet ports. High-availability is supported (packet sampling continues to work after switch-over).

The sFlow agent can communicate with up to three sFlow collectors at the same time. The agent communicates with collectors only on the default VRF.

Although you can configure very high sampling rates, the switch may drop samples if it cannot handle the rate of sampled packets. High sampling rates may also cause high CPU usage resulting in control plane performance issues.

A single sFlow datagram sent to a collector contains multiple flow and counter samples. The total number of samples an sFlow datagram can contain varies depending on the settings for header size and maximum datagram size.

**Default settings**

- sFlow is disabled on all interfaces.
- Collector port: UDP port 6343.
- Sampling rate: 4096.
- Polling interval: 30 seconds.
- Header size: 128 bytes.
- Max datagram size: 1400 bytes.

**Supported features**

- Global sampling rate
- Interface counters polling
- Agent IP configuration for IPv4 and IPv6
- Header size configuration
- Max datagram size configuration
- Ingress sampling for all forwarded traffic (L2, L3)
- Enable/Disable sFlow per interface
- Support for three remote collectors
- An out-of-band collector can be defined on the management VRF
- A collector can be defined on the non-default VRF
- Sampling on Ethernet and LAG interfaces
- High availability support (sampling continues to work after switch-over)
- Source IP support (setting source IP for sFlow datagrams sent to a remote collector)

**Limitations**

- No sampling of egress traffic
- Sampling rate cannot be set per interface (global only)
- sFlow is not configurable via SNMP

**Configuring the sFlow agent**

**Procedure**

1. Configure one or more sFlow collectors with the command `sflow collector`. This determines where the sFlow agent sends sFlow information.
2. Enable the sFlow agent on all interfaces, or on a specific interface, with the command `sflow`.
3. Define the address of the sFlow agent with the command `sflow agent-ip`.
4. By default, the source IP address for sFlow datagrams is set to the IP address of the outgoing switch interface on which the sFlow client is communicating with a collector. Since the switch can have multiple routing interfaces, datagrams can potentially be sent on different paths at different times, resulting in different source IP addresses for the same client. To resolve this issue, define a single source IP address. For details, see *Single source IP address* in the *Fundamentals Guide*.
5. For most deployments, the default values for the following settings do not need to be changed. If your deployment requires different settings, change the default values with the indicated commands:

<table>
<thead>
<tr>
<th>sFlow setting</th>
<th>Default value</th>
<th>Command to change it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate at which packets are sampled.</td>
<td>1 in every 4096 packets</td>
<td><code>sflow sampling</code></td>
</tr>
<tr>
<td>Rate at which the switch sends data to an sFlow collector.</td>
<td>30 seconds</td>
<td><code>sflow polling</code></td>
</tr>
<tr>
<td>Size of the sFlow header.</td>
<td>128 bytes</td>
<td><code>sflow header-size</code></td>
</tr>
<tr>
<td>Maximum size of an sFlow datagram.</td>
<td>1400 bytes</td>
<td><code>sflow max-datagram-size</code></td>
</tr>
</tbody>
</table>

6. Review sFlow configuration settings with the command `show sflow`.

**Example**

This example creates the following configuration:
- Configures an sFlow collector with the IP address 10.10.20.209.
- Enables the sFlow agent on all interfaces.
- Defines the sFlow agent IP address to be 10.10.1.5.

```
switch(config)# sflow collector 10.10.20.209
switch(config)# sflow
switch(config)# sflow agent-ip 10.0.0.1
```

**sFlow scenario**

In this scenario, two hosts send sFlow traffic through a switch to an sFlow collector. The physical topology of the network looks like this:

![Physical topology diagram]

*On the 6400 Switch Series, interface identification differs.*

**Procedure**

1. Enable sFlow globally.
   ```
   switch# config
   switch(config)# sflow
   ```

2. Set the sFlow agent IP address to 10.10.12.1.
   ```
   switch(config)# sflow agent-ip 10.10.12.1
   ```

3. Set the sFlow collector IP address to 10.10.12.2.
   ```
   switch(config)# sflow collector 18.2.2.2
   ```

4. Configure sFlow sampling rate and polling interval.
   ```
   switch(config)# sflow sampling 5000
   switch(config)# sflow polling 20
   ```

5. Configure interface 1/1/1 with IP address 10.10.10.24.
   ```
   switch(config)# interface 1/1/1
   switch(config-if)# no shutdown
   switch(config-if)# ip address 10.10.10.1/24
   switch(config)# quit
   ```

6. Configure interface 1/1/2 with IP address 10.10.11.24.
   ```
   switch(config)# interface 1/1/2
   switch(config-if)# no shutdown
   switch(config-if)# ip address 10.10.11.1/24
   switch(config)# quit
   ```

switch(config)# interface 1/1/3
switch(config-if)# no shutdown
switch(config-if)# ip address 10.10.12.1/24
switch(config)# quit

8. Verify sFlow configuration

switch# show sflow
sFlow Global Configuration
---------------------------------------------
sFlow enabled
Collector IP/Port/Vrf 10.10.10.2/6343/default
Agent Address 10.0.0.1
Sampling Rate 1024
Polling Interval 30
Header Size 128
Max Datagram Size 1400
Sampling Mode both

sFlow Status
---------------------------------------------
Running - Yes

sFlow enabled on Interfaces:
---------------------------------------------
lag100

sFlow Statistics
---------------------------------------------
Number of Ingress Samples 200
Number of Egress Samples 0

sFlow scenario 2

In this scenario, two hosts connected to different switches send sFlow traffic to a collector. A LAG is used to connect the two switches. The physical topology of the network looks like this:
On the 6400 Switch Series, interface identification differs.

**Procedure**

1. Configure switch 1.
   a. Enable sFlow globally.
      ```
      switch# config
      switch(config)# sflow
      ```
   b. Set the sFlow agent IP address to 10.10.12.1.
      ```
      switch(config)# sflow agent-ip 10.10.12.1
      ```
   c. Set the sFlow collector IP address to 10.10.12.2.
      ```
      switch(config)# sflow collector 10.10.12.2
      ```
   d. Configure sFlow sampling rate and polling interval.
      ```
      switch(config)# sflow sampling 5000
      switch(config)# sflow polling 10
      ```
   e. Create VLAN 8.
      ```
      switch(config)# vlan 8
      switch(config-vlan-8)# no shutdown
      switch(config)# exit
      ```
   f. Define LAG 100 and assign VLAN vlan 8 to it.
      ```
      switch(config)# interface lag 100
      switch(config-lag-if)# no shutdown
      switch(config-lag-if)# vlan access 8
      switch(config-lag-if)# lacp mode active
      ```
g. Configure interface 1/1/1.
   switch(config)# interface 1/1/1
   switch(config-if)# no shutdown
   switch(config-lag-if)# no routing
   switch(config-if)# vlan access 8

h. Configure interface 1/1/2 and 1/1/3 as members of LAG 100.
   switch# (config)#interface 1/1/2
   switch(config-if)# no shutdown
   switch(config-if)# lag 100
   switch(config-if)# exit
   switch# (config)#interface 1/1/3
   switch(config-if)# no shutdown
   switch(config-if)# lag 100
   switch(config-if)# exit

i. Configure interface 1/1/4 with IP address 10.10.12.1/24.
   switch# (config)#interface 1/1/4
   switch(config-if)# no shutdown
   switch(config-if)# ip address 10.10.12.1/24
   switch(config-if)# quit

j. Verify sFlow configuration.

switch# show sflow
sFlow Global Configuration
---------------------------------------------
sFlow enabled
Collector IP/Port/Vrf 10.10.10.2/6343/default
Agent Address 10.0.0.1
Sampling Rate 1024
Polling Interval 30
Header Size 128
Max Datagram Size 1400
Sampling Mode both

sFlow Status
---------------------------------------------
Running - Yes

sFlow enabled on Interfaces:
---------------------------------------------
lag100

sFlow Statistics
---------------------------------------------
Number of Ingress Samples 200
Number of Egress Samples 0

2. Configure switch 2.
   a. Create VLAN 8.
      switch(config)# vlan 8
      switch(config-vlan-8)# no shutdown
      switch(config)# exit
   b. Define LAG 100 and assign VLAN vlan 8 to it.
      switch(config)# interface lag 100
      switch(config-lag-if)# no shutdown
      switch(config-lag-if)# vlan access 8
      switch(config-lag-if)# lacp mode active
   c. Configure interface 1/1/1.
      switch(config)# interface 1/1/1
sFlow agent commands

**clear sflow statistics**

clear sflow statistics {global | interface <INTERFACE-NAME>}

**Description**
This command clears the sFlow sample statistics counter to 0 either globally or for a specific interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>global</td>
<td>Specifies all interfaces on the switch.</td>
</tr>
<tr>
<td>interface &lt;INTERFACE-NAME&gt;</td>
<td>Specifies the name of an interface on the switch.</td>
</tr>
</tbody>
</table>

**Examples**

Clearing the global sFlow sample statistics counter to 0 globally:

```
switch(config)# clear sflow statistics global
```

Clearing the global sFlow sample statistics counter to 0 for interface 1/1/1:

```
switch(config)# clear sflow statistics interface 1/1/1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
sFlow
no sFlow

Description
Enables the sFlow agent.
- In the config context, this command enables the sFlow agent globally on all interfaces.
- In an config-if context, this command enables the sFlow agent on a specific interface. sFlow cannot be enabled on a member of a LAG, only on the LAG.

The sFlow agent is disabled by default.
The no form of this command disables the sFlow agent and deletes all sFlow configuration settings, either globally, or for a specific interface.

Examples
*On the 6400 Switch Series, interface identification differs.*

Enabling sFlow globally on all interfaces:

```
switch(config)# sflow
```

Disabling sFlow globally on all interfaces:

```
switch(config)# no sflow
```

Enabling sFlow on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# sflow
```

Disabling sFlow on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no sflow
```

Enabling sFlow on interface lag100:

```
switch(config)# interface lag100
switch(config-if)# sflow
```

Disabling sFlow on interface lag100:

```
switch(config)# interface lag100
switch(config-if)# no sflow
```

Command History
### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td></td>
<td>config-if</td>
<td></td>
</tr>
</tbody>
</table>

### sflow agent-ip

```
sflow agent-ip <IP-ADDR>
sno sflow agent-ip [<IP-ADDR>]
```

#### Description
Defines the IP address of the sFlow agent to use in sFlow datagrams. This address must be defined for sFlow to function. HPE recommends that the address:

- can uniquely identify the switch
- is reachable by the sFlow collector
- does not change with time

The `no` form of this command deletes the IP address of the sFlow agent. This causes sFlow to stop working and no datagrams will be sent to the sFlow collector.

#### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP-ADDR&gt;</td>
<td>Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. The agent address is used to identify the switch in all sFlow datagrams sent to sFlow collectors. It is usually set to an IP address on the switch that is reachable from a sFlow collector.</td>
</tr>
</tbody>
</table>

#### Examples

Setting the agent address to **10.10.10.100**:

```
switch(config)# sflow agent-ip 10.0.0.100
```

Setting the agent address to **2001:0db8:85a3:0000:0000:8a2e:0370:7334**:

```
switch(config)# sflow agent-ip 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Removing the address configuration from the switch, which results in sFlow being disabled:

```
switch(config)# no sflow agent-ip
```
sFlow

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

sflow collector

sflow collector <IP-ADDR> [port <PORT>] [vrf <VRF>]
no sflow collector <IP-ADDR> [port <PORT>] [vrf <VRF>]

Description

Defines a collector to which the sFlow agent sends data. Up to three collectors can be defined. At least one collector should be defined, and it must be reachable from the switch for sFlow to work.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collector &lt;IP-ADDR&gt;</td>
<td>Specifies the IP address of a collector in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td>port &lt;PORT&gt;</td>
<td>Specifies the UDP port on which to send information to the sFlow collector. Range: 0 to 65536. Default: 6343.</td>
</tr>
<tr>
<td>vrf &lt;VRF&gt;</td>
<td>Specifies the VRF on which to send information to the sFlow collector. The VRF must be defined on the switch. If no VRF is specified, the default VRF (default) is used.</td>
</tr>
</tbody>
</table>

Example

Defining a collector with IP address **10.10.10.100** on UDP port **6400**:

```
switch(config)# sflow collector 10.0.0.1 port 6400
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
sflow disable
sflow disable

Description
Disables the sFlow agent, but retains any existing sFlow configuration settings. The settings become active if the sFlow agent is re-enabled.

Example
Disabling sFlow support:

```
switch(config)# sflow disable
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

sflow header-size
sflow header-size <SIZE>
no sflow header-size [<SIZE>]

Description
Sets the sFlow header size in bytes.
The no form of this command sets the header size to the default value of 128.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

Examples
Setting the header size to 64 bytes:

```
switch(config)# sflow header-size 64
```
Setting the header size to the default value of 128 bytes:

```
switch(config)# no sflow header-size
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**sflow max-datagram-size**

sflow max-datagram-size <SIZE>
no sflow max-datagram-size [<SIZE>]

**Description**

Sets the maximum number of bytes that are sent in one sFlow datagram.

The `no` form of this command sets maximum number of bytes to the default value of 1400.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

**Examples**

Setting the datagram size to 1000 bytes:

```
switch(config)# sflow max-datagram-size 1000
```

Setting the header size to the default value of 1400 bytes:

```
switch(config)# no sflow max-datagram-size
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
**Platforms** | **Command context** | **Authority**  
---|---|---  
All platforms | config | Administrators or local user group members with execution rights for this command.  

**sflow mode**  
sflow mode {ingress | egress | both}  
no sflow mode {ingress | egress | both}  

**Description**  
Sets the sFlow sampling mode. The default mode is ingress.  
The no form of the command sets the sampling mode to ingress. Executing the no form of the command with the ingress option will have no impact as ingress is the default mode.  

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ingress</td>
<td>Samples only ingress traffic.</td>
</tr>
<tr>
<td>egress</td>
<td>Samples only egress traffic.</td>
</tr>
<tr>
<td>both</td>
<td>Samples both ingress and egress traffic.</td>
</tr>
</tbody>
</table>

**Examples**  
Setting the sFlow mode to only sample egress traffic:  
```
switch# configure terminal  
switch(config)# sflow mode egress
```

Resetting the sFlow sampling mode to the default of ingress from previously configured mode of egress:  
```
switch# configure terminal  
switch(config)# no sflow mode egress
```

**Command History**  

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**  

<table>
<thead>
<tr>
<th><strong>Platforms</strong></th>
<th><strong>Command context</strong></th>
<th><strong>Authority</strong></th>
</tr>
</thead>
</table>
| 6300  
6400 | config | Administrators or local user group members with execution rights for this command. |

**sflow polling**  
sflow polling <INTERVAL>  
no sflow polling [<INTERVAL>]

---

AOS-CX 10.08 IP Services Guide | (6300 and 6400 Switch Series) 59
Description
Defines the global polling interval for sFlow in seconds.
The no form of this command sets the polling interval to the default value of 30 seconds.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;INTERVAL&gt;</td>
<td>Specifies the polling interval in seconds. Range: 10 to 3600. Default: 30.</td>
</tr>
</tbody>
</table>

Examples
Setting the polling interval to 10:

```
switch(config)# sflow polling 10
```

Setting the polling interval to the default value.

```
switch(config)# no sflow polling
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

sflow sampling

```
sflow sampling <RATE>
no sflow sampling [<RATE>]
```

Description
Defines the global sampling rate for sFlow in number of packets. The default sampling rate is 4096, which means that one in every 4096 packets is sampled. A warning message is displayed when the sampling rate is set to less than 4096 and proceeds only after user confirmation.
The no form of this command sets the sampling rate to the default value of 4096.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sampling &lt;RATE&gt;</td>
<td>Specifies the sampling rate. Range: 1 to 1000000000. Default: 4096.</td>
</tr>
</tbody>
</table>

Examples
Setting the sampling rate to 5000:
Setting the sampling rate to the default:

```
switch(config)# no sflow sampling
```

Setting the sampling rate to 1000:

```
switch(config)# sflow sampling 1000
Setting the sFlow sampling rate lower than 4096 is not recommended and might affect system performance.
Do you want to continue [y/n]? y
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**show sflow**

```
show sflow [interface <INTERFACE-NAME>] [vsx-peer]
```

**Description**

Shows sFlow configuration settings and statistics for all interfaces, or for a specific interface

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface &lt;INTERFACE-NAME&gt;</td>
<td>Specifies the name of an interface on the switch.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

```
switch# show sflow
```
sFlow Global Configuration
-------------------------------------
sFlow enabled
Collector IP/Port/Vrf 10.10.10.2/6343/default
Agent Address 10.0.0.1
Sampling Rate 1024
Polling Interval 30
Header Size 128
Max Datagram Size 1400
Sampling Mode both

sFlow Status
-------------------------------------
Running - Yes

sFlow enabled on Interfaces:
-------------------------------------
lag100

sFlow Statistics
-------------------------------------
Number of Ingress Samples 200
Number of Egress Samples 0

Showing sFlow information for interface 1/1/1:

switch# show sflow interface 1/1/1
sFlow configuration - Interface 1/1/1
-------------------------------------
sFlow enabled
Sampling Rate 1024
Sampling Mode both
Number of Ingress Samples 81
Number of Egress Samples 20
sFlow Sampling Status success

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
The Dynamic Host Configuration Protocol (DHCP) enables the automatic assignment of IP addresses and other configuration settings to network devices. DHCP is composed of three components: DHCP server, DHCP client, and DHCP relay agent. The DHCP server contains the IP addresses and configuration settings for a network as defined by a network administrator. It responds to DHCP requests issued by DHCP clients, returning the requested network configuration settings. The DHCP client runs on a network device. It issues a request to a DHCP server to obtain an IP address for the network device, and other network settings. The DHCP relay agent acts an intermediary, forwarding DHCP requests/response between DHCP clients/servers on different networks. This enables DHCP clients to use the services of DHCP servers that are not on the same subnet on which they are located.

**DHCP client**
By default, the switch operates as a DHCP client on VLAN 1 or the management interface allowing it to automatically obtain an IP address from a DHCP server on the network to which it is connected.

**DHCP client commands**

**ip dhcp**

ip dhcp

**Description**
Enables the DHCP client on the management interface enabling the interface to automatically obtain an IP address from a DHCP server on the network. By default, the DHCP client is enabled.

**Examples**
This example enables the DHCP client on the management interface.

```
switch(config)# interface mgmt
switch(config-if-mgmt)# ip dhcp
switch(config-if-mgmt)# no shutdown
```

If the interface is not enabled, you can enable it by entering the `no shutdown` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
DHCP relay agent

The function of the DHCP relay agent is to forward the DHCP messages to other subnets so that the DHCP server does not have to be on the same subnet as the DHCP clients. The DHCP relay agent transfers DHCP messages from the DHCP clients located on a subnet without a DHCP server, to other subnets. It also relays answers from DHCP servers to DHCP clients.

Supported interfaces

The DHCP relay agent is supported on layer 3 interfaces, layer 3 VLAN interfaces, and LAG interfaces. DHCP relay is not supported on the management interface.

VRF support

The DHCP relay agent is VRF aware and behaves as follows when VRFs are defined on the switch:

- DHCP client requests received on an interface are forwarded to the configured servers via the VRF that the interface is part of.
- DHCP server responses received on an interface are forwarded to the client that is reachable via the VRF that the interface is part of.

DHCP server interoperation

Both DHCP relay and DHCP server can be configured on the same VRF.

DHCPv4 relay agent

Hop count in DHCP requests

When a DHCP client broadcasts request, the DHCP relay agent in the switch receives the packets and forwards them to the DHCP server as unicast requests. During this process, the DHCP relay agent increments the hop count before forwarding DHCP packets to the server. The DHCP server, in turn, includes the hop count in the DHCP header in the response sent back to a DHCP client.

DHCP relay option 82

Option 82 is called the relay agent information option. When a DHCP relay agent forwards client-originated DHCP packets to a DHCP server, the option 82 field is inserted/replaced, or the packet with this option is dropped. Servers recognizing the relay agent information option may use the information to implement policies for the assignment of IP addresses and other parameters. The relay agent relays the server-to-client replies to the client.

If a second relay agent is configured to add its own option 82 information, it can encapsulate option 82 information in messages from a first relay agent. The DHCP server uses the option 82 information from both relay agents to decide the IP address for the client.

Inter-VRF DHCP relay

The DHCP relay agent supports anycast gateway using option 82 sub-option 5 (RFC 3527). The DHCP relay discovery packet is filled with the client's gateway IP address in sub-option 5 (discovery packet). The DHCP server uses this information to offer an IP address from the right pool. Pool selection occurs by matching

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if-mgmt</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
the default gateway configuration settings on the DHCP server with the requested gateway IP address in sub-option 5 in the discovery packet.

The switch uses DHCP relay sub-option 151 to enable DHCP relay to forward discovery and reply packets between VXLAN DHCP clients and DHCP servers even when they are on different overlay or underlay VRFs and the DHCP-server is reachable on the default VRF or one of the overlay VRFs.

In general deployments, a renewal of a DHCP client's IP occurs when the client sends a request to the DHCP server directly. In the case of EVPN VXLAN clients, the DHCP server is not directly reachable. Instead, the renewal request is sent to the DHCP relay. DHCP relay agent fills the option 82 sub-option 11 field in the DHCP discovery packet with the client's gateway IP on the VTEP (which is the relay interface IP address of the VTEP) and the DHCP server returns a DHCP offer reply packet with option 54 set to the DHCP server Identifier. When the reply packet is received by the client, the client uses the IP in option 54 to send subsequent renewal requests to this IP (VTEP's Relay Interface IP) using sub-option 11 (also known as the Server ID Override Sub-option). Refer to RFC 5107 for more details.

Sub-options 5,11,151,152 are filled in the discover packet, only if a source IP address is defined (using the command ip source-address) for the given DHCP server's source VRF. If the server does not understand sub-option 151, then the server will add sub-option 152 in offer packet.

In an inter-VRF situation, when both DHCP relay and DHCP snooping are enabled on the switch with option 82, DHCPv4 clients will not receive an IP address.

**Configuring a BOOTP/DHCP relay gateway**

The DHCP relay agent selects the lowest-numbered IP address on the interface to use for DHCP messages. The DHCP server then uses this IP address when it assigns client addresses. However, this IP address may not be the same subnet as the one on which the client needs the DHCP service. This feature provides a way to configure a gateway address for the DHCP relay agent to use for relayed DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address.

**Configuring the DHCPv4 relay agent**

**Prerequisites**

- An enabled layer 3 interface.

**Procedure**

1. The DHCPv4 relay agent is enabled by default. If it was previously disabled, enable it with the command `dhcp-relay`.
2. Configure one or more IP helper addresses with the command `ip helper-address`. This determines where the DHCPv4 agent forwards DHCP requests. IP helper addresses can be configured on layer 3 interfaces, layer 3 VLAN interfaces, and LAG interfaces.
3. If you want to modify the content of forwarded DHCP packets or drop DHCP packets, configure option 82 support with the command `dhcp-relay option 82`.
4. Define the gateway address that the DHCPv4 agent will use with the command `ip bootp-gateway`.
5. If required, enable the hop count increment feature with the command `dhcp-relay hop-count-increment`.
6. Review DHCPv4 relay agent configuration settings with the commands `show dhcp-relay`, `show ip helper-address`, and `show dhcp-relay bootp-gateway`.

**Example**

This example creates the following configuration:
- Enables the DHCPv4 relay agent.
- Enables interface 1/1/1 and assigns an IPv4 address to it. (By default, all interfaces are layer 3 and disabled.)
- Defines an IP helper address of **10.10.20.209** on the interface.
- Enables DHCP option 82 support and replaces all option 82 information with the values from the switch with the switch MAC address as the remote ID.

```
switch(config)# dhcp-relay
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ip address 198.51.100.1/24
switch(config-if)# ip helper-address 10.10.20.209
switch(config-if)# exit
switch(config)# dhcp-relay option 82 replace mac
```

**DHCPv4 relay scenario 1**

In this scenario, DHCP relay on the server enables two hosts to obtain their IP addresses from a DHCP server on a different subnet. The physical topology of the network looks like this:

![DHCPv4 relay scenario 1](image)

**Procedure**
1. DHCP relay is enabled by default. If it was previously disabled, enable it.
   
   ```
   switch# config
   switch(config)# dhcp-relay
   ```

2. Define an IPv4 helper address on interfaces 1/1/1 and 1/1/2.
   
   ```
   switch(config)# interface 1/1/1
   switch(config-if)# ip address 192.168.2.11/24
   switch(config-if)# ip helper-address 192.168.1.1
   switch(config-if)# interface 1/1/2
   switch(config-if)# ip address 192.168.2.12/24
   switch(config-if)# ip helper-address 192.168.1.1
   ```

3. Verify DHCP relay configuration.
   
   ```
   switch# show dhcp-relay
   DHCP Relay Agent : Enabled
   DHCP Request Hop Count Increment : Enabled
   L2VPN Clients : Disabled
   Option 82 : Disabled
   Source-Interface : Disabled
   Response Validation : Disabled
   Option 82 Handle Policy : replace
   Remote ID : mac
   
   DHCP Relay Statistics:
   Valid Requests Dropped Requests Valid Responses Dropped Responses
   ------------------- ------------------- ------------------- -------------------
   60                  10                  60                  10
   
   DHCP Relay Option 82 Statistics:
   Valid Requests Dropped Requests Valid Responses Dropped Responses
   ------------------- ------------------- ------------------- -------------------
   50                  8                   50                  8
   ```

   ```
   switch# show ip helper-address
   IP Helper Addresses
   
   Interface: 1/1/1  
   IP Helper Address     VRF
   -------------------     ---------
   192.168.1.1            default
   
   Interface: 1/1/2  
   IP Helper Address     VRF
   -------------------     ---------
   192.168.1.1            default
   ```

**DHCPv4 relay scenario 2**

In this scenario, the two host computers communicate with two different DHCP servers. Each server is reached on a different VRF. The physical topology of the network looks like this:
Procedure

1. Create the two VRFs.
   switch# configure terminal
   switch(config)# vrf vrf1
   switch(config)# vrf vrf2

2. Configure interface 1/1/1. Set its IP address, associate it with VRF 1, and define the helper IP address to reach DHCP server 1.
   switch(config-if)# interface 1/1/1
   switch(config-if)# vrf attach vrf1
   switch(config-if)# ip address 20.0.0.1/8
   switch(config-if)# ip helper-address 10.0.10.2

3. Configure interface 1/1/2. Set its IP address and associate it with VRF 1.
   switch(config-if)# interface 1/1/2
   switch(config-if)# vrf attach vrf1
   switch(config-if)# ip address 10.0.10.2/24

   switch(config-if)# interface 1/1/3
   switch(config-if)# vrf attach vrf2
   switch(config-if)# ip address 9.0.0.1/24

5. Configure interface 1/1/4. Set its IP address, associate it with VRF 2, and define the helper IP address to reach DHCP server 2.
   switch(config-if)# interface 1/1/4
   switch(config-if)# vrf attach vrf2
   switch(config-if)# ip address 30.0.0.1/8
   switch(config-if)# ip helper-address 9.0.0.2

DHCPv4 relay scenario 3
In this scenario, host on switch 1 reaches the DHCP server on switch two via a LAG. The physical topology of the network looks like this:
Procedure

1. On switch 1:
   a. Create LAG 100 and assign an IP address to it.
      ```
      switch# config
      switch(config)# interface lag 100
      switch(config-lag-if)# ip address 10.0.10.1/24
      switch(config-lag-if)# lACP mode active
      switch(config-lag-if)# exit
      ```
   
   b. Assign an IP address to interface 1/1/1 and a helper address to reach the DHCP server.
      ```
      switch(config)# interface 1/1/1
      switch(config-if)# ip address 20.0.0.1/8
      switch(config-if)# ip helper-address 9.0.0.2
      ```
   
   c. Assign interfaces 1/1/2 and 1/1/3 to LAG 100
      ```
      switch(config-if)# interface 1/1/2
      switch(config-if)# lag 100
      switch(config-if)# interface 1/1/3
      ```
   
   d. Create a route between 10.0.10.2 and 9.0.0.0.
      ```
      switch(config)# ip route 9.0.0.0.24 10.0.10.2
      ```

2. On switch 2:
   a. Create LAG 100 and assign an IP address to it.
      ```
      switch# config
      switch(config)# interface lag 100
      switch(config-lag-if)# ip address 10.0.10.2/24
      switch(config-lag-if)# lACP mode active
      switch(config-lag-if)# exit
      ```
   
   b. Assign interfaces 1/1/1 and 1/1/2 to LAG 100
      ```
      switch(config-if)# interface 1/1/2
      switch(config-if)# lag 100
      switch(config-if)# interface 1/1/3
      ```
   
   c. Assign an IP address to interface 1/1/3.
      ```
      switch(config)# interface 1/1/3
      switch(config-if)# ip address 9.0.0.1/24
      ```
   
   d. Create a route between 20.0.0.0 and 10.0.10.1.
      ```
      switch(config)# ip route 20.0.0.0/8 10.0.10.1
      ```

DHCPv4 relay commands
**dhcp-relay**

`dhcp-relay`

no dhcp-relay

**Description**

Enables DHCP relay support. DHCP relay is enabled by default. DHCP relay is not supported on the management interface. The no form of this command disables DHCP relay support.

**Examples**

This example enables DHCP relay support.

```
switch(config)# dhcp-relay
```

This example removes DHCP relay support.

```
switch(config)# no dhcp-relay
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dhcp-relay hop-count-increment**

`dhcp-relay hop-count-increment`

no dhcp-relay hop-count-increment

**Description**

Enables the DHCP relay hop count increment feature, which causes the DHCP relay agent to increment the hop count in all relayed DHCP packets. Hop count is enabled by default. The no form of this command disables the hop count increment feature.

**Examples**

Enabling the hop count increment feature.

```
switch(config)# dhcp-relay hop-count-increment
```

Disabling the hop count increment feature.
switch(config)# no dhcp-relay hop-count-increment

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>


dhcp-relay l2vpn-clients

dhcp-relay l2vpn-clients
no dhcp-relay l2vpn-clients

Description

Enables forwarding of packets from L2 VPN clients. Forwarding is enabled by default.
The no form of this command disables forwarding of packets from L2 VPN clients.

Example

Enabling forwarding of packets from L2 VPN clients.

switch(config)# dhcp-relay l2vpn-clients
switch(config)# no dhcp-relay l2vpn-clients

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>


dhcp-relay option 82

dhcp-relay option 82 {replace [validate] | drop [validate] | keep | source-interface | validate [replace | drop]} [ip | mac]
no dhcp-relay option 82 {replace [validate] | drop [validate] | keep | source-interface | validate [replace | drop]} [ip | mac]

Description
Configures the behavior of DHCP relay option 82. A DHCP relay agent can receive a message from another DHCP relay agent having option 82. The relay information from the previous relay agent is replaced by default.

The no form of this command disables the DHCP relay option 82 configurations.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replace</td>
<td>Replace the existing option 82 field in an inbound client DHCP packet with the information from the switch. The remote ID and circuit ID information from the first relay agent is lost. Default.</td>
</tr>
<tr>
<td>validate</td>
<td>Validate option 82 information in DHCP server responses and drop invalid responses.</td>
</tr>
<tr>
<td>drop</td>
<td>Drop any inbound client DHCP packet that contains option 82 information.</td>
</tr>
<tr>
<td>keep</td>
<td>Keep the existing option 82 field in an inbound client DHCP packet. The remote ID and circuit ID information from the first relay agent is preserved.</td>
</tr>
<tr>
<td>source-interface</td>
<td>Configures the DHCP relay to use a configured source IP address for inter-VRF server reachability. Set the source IP address with the command ip source-interface.</td>
</tr>
<tr>
<td>ip</td>
<td>Use the IP address of the interface on which the client DHCP packet entered the switch as the option 82 remote ID.</td>
</tr>
<tr>
<td>mac</td>
<td>Use the MAC address of the switch as the option 82 remote ID. Default.</td>
</tr>
</tbody>
</table>

**Example**

This example enables DHCP option 82 support and replaces all option 82 information with the values from the switch, with the switch MAC address as the remote ID.

```
switch(config)# dhcp-relay option 82 replace mac
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ip bootp-gateway**

```
ip bootp-gateway <IPV4-ADDR>
no ip bootp-gateway <IPV4-ADDR>
```
Description
Configures a gateway address for the DHCP relay agent to use for DHCP requests. By default DHCP relay agent picks the lowest-numbered IP address on the interface.
The no form of this command removes the gateway address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV4-ADDR&gt;</td>
<td>Specifies the IP address of the gateway in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
</tbody>
</table>

Examples
On the 6400 Switch Series, interface identification differs.
Sets the IP address of the gateway for interface 1/1/1 to 10.10.10.10.

```
switch(config)# interface 1/1/1
switch(config-if)# ip bootp-gateway 10.10.10.10
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ip helper-address

```
ip helper-address <IPV4-ADDR> [vrf <VRF-NAME>]
no ip helper-address <IPV4-ADDR> [vrf <VRF-NAME>]
```

Description
Defines the address of a remote DHCP server or DHCP relay agent. Up to eight addresses can be defined. The DHCP agent forwards DHCP client requests to all defined servers.
This command requires that you define a source IP address for DHCP relay with the command ip source-interface. The configured source IP on the VRF is used to forward DHCP packets to the server.
A helper address cannot be defined on the OOBM interface.
The no form of this command removes an IP helper address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>helper-address &lt;IPV4-ADDR&gt;</td>
<td>Specifies the helper IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF. Default: default.</td>
</tr>
</tbody>
</table>
Examples

*On the 6400 Switch Series, interface identification differs.*

Defining the IP helper address `10.10.10.209` on interface `1/1/1`.

```
switch(config)# interface 1/1/1
switch(config-if)# ip helper-address 10.10.10.209
```

Removing the IP helper address `10.10.10.209` on interface `1/1/1`.

```
switch(config-if)# no ip helper-address 10.10.10.209
```

Defining the IP helper address `10.10.10.209` on interface `1/1/2` on VRF `myvrf`.

```
switch(config)# interface 1/1/2
switch(config-if)# ip helper-address 10.10.10.209 vrf myvrf
```

Removing the IP helper address `10.10.10.209` on interface `1/1/2` on VRF `myvrf`.

```
switch(config-if)# no ip helper-address 10.10.10.209 vrf myvrf
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

`show dhcp-relay`  
`show dhcp-relay [vsx-peer]`

Description

Shows DHCP relay configuration settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>
switch# show dhcp-relay

DHCP Relay Agent : Enabled
DHCP Request Hop Count Increment : Enabled
L2VPN Clients : Disabled
Option 82 : Disabled
Source-Interface : Disabled
Response Validation : Disabled
Option 82 Handle Policy : replace
Remote ID : mac

DHCP Relay Statistics:

<table>
<thead>
<tr>
<th>Valid Requests</th>
<th>Dropped Requests</th>
<th>Valid Responses</th>
<th>Dropped Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>10</td>
<td>60</td>
<td>10</td>
</tr>
</tbody>
</table>

DHCP Relay Option 82 Statistics:

<table>
<thead>
<tr>
<th>Valid Requests</th>
<th>Dropped Requests</th>
<th>Valid Responses</th>
<th>Dropped Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>8</td>
<td>50</td>
<td>8</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; ) only.</td>
</tr>
<tr>
<td>6400</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; ) only.</td>
</tr>
</tbody>
</table>

show dhcp-relay bootp-gateway

show dhcp-relay bootp-gateway [interface <INTERFACE-NAME>] [vsx-peer]

Description

Shows the bootp gateway defined for all interfaces or a specific interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

Examples
On the 6400 Switch Series, interface identification differs.

```
switch# show dhcp-relay bootp-gateway
BOOTP Gateway Entries
   Interface  Source IP
           ----------  -----------
   1/1/1      1.1.1.1
   1/1/2      1.1.1.2
```

```
switch# show ip helper-address interface 1/1/1
BOOTP Gateway Entries
   Interface  Source IP
           ----------  -----------
   1/1/1      1.1.1.1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show ip helper-address**

```
show ip helper-address [interface <INTERFACE-ID>] [vsx-peer]
```

**Description**

Shows the helper IP addresses defined for all interfaces or a specific interface.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Example**

On the 6400 Switch Series, interface identification differs.
show ip helper-address

IP Helper Addresses

Interface: 1/1/1
IP Helper Address VRF
---------------------
192.168.20.1 default
192.168.10.1 default

Interface: 1/1/2
IP Helper Address VRF
---------------------
192.168.30.1 RED

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

DHCPv6 relay agent

Supporting VXLAN topologies or inter-VRF deployment

When deploying EVPN VXLAN or inter-VRF topologies where the source VRFs for the DHCP and DHCP client are different, it is recommended that you install the DHCPv6 server in the underlay so that there is only one instance of the DHCPv6 server serving overlay clients.

Configuring the DHCPv6 relay agent

Prerequisites

- An enabled layer 3 interface.

Procedure
1. Enable the DHCPv6 agent with the command `dhcpv6-relay`.
2. Configure one or more IP helper addresses with the command `ipv6 helper-address`. This determines where the DHCPv6 agent forward DHCP requests.
3. If you want to enable DHCP option 79 support to forward client link-layer addresses, use the command `dhcpv6-relay option 79`.
4. Review DHCPv6 relay agent configuration settings with the commands `show dhcpv6-relay` and `show ipv6 helper-address`.

**Example**

This example creates the following configuration:

- Enables the DHCPv6 relay agent.
- Enables interface 1/1/2 and assigns an IPv6 address to it. (By default, all interfaces are layer 3 and disabled.)
- Defines an IP helper address of FF01::1:1000 on interface 1/1/2.
- Enables DHCP option 79.

```bash
switch(config)# dhcpv6-relay
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
switch(config-if)# ip helper-address FF01::1:1000
switch(config-if)# exit
switch(config)# dhcpv6-relay option 79
```

**DHCPv6 relay scenario 1**

In this scenario, DHCP relay on the server enables two hosts to obtain their IP addresses from a DHCP server on a different subnet. The physical topology of the network looks like this:

[Diagram of DHCPv6 relay scenario 1]

**Procedure**
1. Enable DHCP relay.
   switch# config
   switch(config)# dhcpv6-relay

2. Define an IPv6 helper address on interfaces 1/1/1 and 1/1/2.
   switch(config)# interface 1/1/1
   switch(config-if)# ipv6 address 2002::22/64
   switch(config-if)# ipv6 helper-address 2001::1
   switch(config-if)# interface 1/1/2
   switch(config-if)# ipv6 address 2002::21/64
   switch(config-if)# ipv6 helper-address 2001::1
   switch(config-if)# quit

3. Verify DHCP relay configuration.
   switch# show dhcpv6-relay
   DHCPv6 Relay Agent : Enabled
   Option 79 : Disabled
   switch# show ipv6 helper-address

   Interface: 1/1/1
   IPv6 Helper Address  Egress Port
   ----------------------  --------
   2001::1               1/1/3

   Interface: 1/1/2
   IPv6 Helper Address  Egress Port
   ----------------------  --------
   2001::1               1/1/3

**DHCPv6 relay scenario 2**

In this scenario, the two host computers communicate with two different DHCP servers. Each server is reached on a different VRF. The physical topology of the network looks like this:
1. Create the two VRFs.
   switch# config
   switch(config)# vrf vrf 1
   switch(config)# vrf vrf 2

2. Configure interface 1/1/1. Set its IP address, associate it with VRF 1, and define the helper IP address to reach DHCP server 1.
   switch(config-if)# interface 1/1/1
   switch(config-if)# vrf attach vrf1
   switch(config-if)# ipv6 address 2001:0:0:1/8
   switch(config-if)# ipv6 helper-address unicast 1040::2

3. Configure interface 1/1/2. Set its IP address and associate it with VRF 1.
   switch(config-if)# interface 1/1/2
   switch(config-if)# vrf attach vrf1
   switch(config-if)# ipv6 address 1040::1/120

   switch(config-if)# interface 1/1/3
   switch(config-if)# vrf attach vrf2
   switch(config-if)# ipv6 address 3030::1/120

5. Configure interface 1/1/4. Set its IP address, associate it with VRF 2, and define the helper IP address to reach DHCP server 2.
   switch(config-if)# interface 1/1/4
   switch(config-if)# vrf attach vrf2
   switch(config-if)# ipv6 address 4040::1/120
   switch(config-if)# ipv6 helper-address unicast 3030::2

DHCP relay (IPv6) commands

dhcpv6-relay
   dhcpv6-relay
   no dhcpv6-relay

Description
Enables DHCPv6 relay support. DHCPv6 relay is disabled by default.
DHCP relay is not supported on the management interface
The no form of this command disables DHCP relay support.

Examples
Enables DHCPv6 relay support.

   switch(config)# dhcpv6-relay

Removes DHCPv6 relay support.

   switch(config)# no dhcpv6-relay

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dhcpv6-relay option 79**

dhcpv6-relay option 79
no dhcpv6-relay option 79

**Description**

Enables support for DHCP relay option 79. When enabled, the DHCPv6 relay agent forwards the link-layer address of the client. This option is disabled by default.

The no form of this command disables support for DHCP relay option 79.

**Examples**

Enables DHCP option 79 support.

switch(config)# dhcpv6-relay option 79

Disables DHCP option 79 support.

switch(config)# no dhcpv6-relay option 79

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 helper-address**

ipv6 helper-address unicast <UNICAST-IPV6-ADDR>
no ipv6 helper-address unicast <UNICAST-IPV6-ADDR>
ipv6 helper-address multicast {all-dhcp-servers | <MULTICAST-IPV6-ADDR>} egress <PORT-NUM>
no ipv6 helper-address multicast {all-dhcp-servers | <MULTICAST-IPV6-ADDR>} egress <PORT-NUM>

**Description**

Defines the address of a remote DHCPv6 server or DHCPv6 relay agent. Up to eight addresses can be defined. The DHCPv6 agent forwards DHCPv6 client requests to all defined servers.

Not supported on the OOBM interface.
The no form of this command removes an IP helper address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;UNICAST-IPV6-ADDR&gt;</code></td>
<td>Specifies the unicast helper IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td><code>&lt;MULTICAST-IPV6-ADDR&gt;</code></td>
<td>Specifies the multicast helper IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td>all-dhcp-servers</td>
<td>Specifies all the DHCP server IPv6 addresses for the interface.</td>
</tr>
<tr>
<td>egress <code>&lt;PORT-NUM&gt;</code></td>
<td>Specifies the port number on which DHCPv6 service requests are relayed to a multicast destination. The egress port must be different than the one on which the multicast helper address is configured. Format: member/slot/port.</td>
</tr>
<tr>
<td>vrf <code>&lt;VRF-NAME&gt;</code></td>
<td>Specifies the name of the VRF from which the specified protocol sets its source IP address.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Defining a multicast IPv6 helper address of `2001:DB8::1` on port `1/1/2`:

```
switch(config-if)# ipv6 helper-address multicast 2001:DB8:0:0:0:0:1 egress 1/1/2
```

Removing the IP helper address of `2001:DB8::1` on port `1/1/2`:

```
switch(config-if)# no ipv6 helper-address multicast 2001:DB8:0:0:0:0:1 egress 1/1/2
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
</table>
| 6300  
6400 | config-if | Administrators or local user group members with execution rights for this command. |

`show dhcpv6-relay`

`show dhcpv6-relay [vsx-peer]`

**Description**

Shows DHCP relay configuration settings.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Example**

```
switch# show dhcpv6-relay
DHCPv6 Relay Agent : Enabled
Option 79 : Enabled
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;only).</td>
</tr>
</tbody>
</table>

**show ipv6 helper-address**

```
show ipv6 helper-address [interface <INTERFACE-ID>] [vsx-peer]
```

**Description**

Shows the helper IP addresses defined for all interfaces or a specific interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

```
switch# show ipv6 helper-address
```
The dynamic host configuration protocol (DHCP) enables a server to automate the assignment of IP addresses, and other networking settings, to host computers. The DHCP server on the switch provides both IPv4 and IPv6 support and is independently configurable on each VRF.

**Key features**

- Supports multiple address pools and static address bindings.
- Supports DHCP options, enabling the server to provide additional information about the network when DHCP clients request an address.
- Supports BOOTP to distribute boot image files using an external TFTP server.
- VRF aware, meaning that DHCP client requests received on an interface are processed by the DHCP server instance configured for a VRF. DHCP server responses are forwarded to clients on the VRF.
- Supports external storage of lease information on a remote host. This enables the DHCP server to restore lease information after a reboot or a failure. Lease information is stored in a flat file on the configured external device. It is important that the external device provide persistent external storage to allow restoration of lease information. If external storage is not configured, then after a failure or reboot, all existing lease information is lost.
- Supports VSX. In a VSX setup, one switch acts as primary and the other switch acts as secondary. The DHCP server is active only on the primary switch. After a failover, the DHCP server is enabled based on the state and role of the switch. The state of the DHCP server indicates the operational state of the server. VSX synchronization supports DHCPv4 and DHCPv6 server, including external storage configurations. For more information on VSX support, see the Virtual Switching Extension (VSX) Guide.

**DHCP relay interoperation**

Both DHCP relay and DHCP server can be configured on the same VRF.

**DHCP snooping interoperation**

DHCP snooping may not be configured with DHCP server.

### Configuring a DHCPv4 server on a VRF

**Prerequisites**

- An enabled layer 3 interface.
- A VRF.
- An external TFTP server to host BOOTP image files (optional).
- An external storage device installed and configured (optional).

**Procedure**

1. Assign the DHCPv4 server to a VRF with the command `dhcp-server vrf`. This switches to the DHCPv4 server configuration context.
2. If you want the DHCPv4 server to be the sole authority for IP addresses on the VRF, enable authoritative mode with the command `authoritative`.
3. Define an address pool for the VRF with the command `pool`. This switches to the DHCPv4 server pool context. Customize pool settings as follows:
   a. Define the range of addresses in the pool with the command `range`.
   b. Set the lease time for addresses in the pool with the command `lease`.
   c. Set the domain name for the pool with the command `domain-name`.
   d. Define up to four default routers with the command `default-router`.
   e. Define up to four DNS servers with the command `dns-server`.
   f. Create static bindings for specific addresses in the pool with the command `static-bind`.
   g. Configure custom DHCPv4 options for the pool with the command `option`.
   h. Configure NetBIOS support with the commands `netbios-name-server` and `netbios-node-type`.
   i. Configure BOOTP support with the command `bootp`.
   j. Exit the DHCPv4 server pool context with the command `exit`.
4. Enable the DHCP server on the VRF with the command `enable`.
5. Configure support for persistent external storage of DHCP settings with the command `dhcp-server external-storage`.
6. View DHCPv4 server configuration settings with the command `show dhcp-server all-vrfs`.

**Example**

This example creates the following configuration:

- Configures the DHCPv4 server on VRF `primary-vrf`.
- Enables authoritative mode.
- Defines the pool `primary-pool` with the following settings:
  - Address range: `10.0.0.1` to `10.0.0.100`.
  - Lease time: 12 hours.
  - Domain name: `example.org.in`.
  - Default routers: `10.30.30.1` and `10.30.30.2`.
  - DNS servers: `125.0.0.1` and `125.0.0.2`.
  - Static binding of `10.0.0.11` for MAC address `24:be:05:24:75:73`.
  - DHCP custom option 3 with IP address `10.30.30.3`.
- Enables the DHCPv4 server.

```plaintext
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# range 10.0.0.1 10.0.0.100
switch(config-dhcp-server-pool)# lease 12:00:00
switch(config-dhcp-server-pool)# domain-name example.org.in
switch(config-dhcp-server-pool)# default-router ip 10.30.30.1 10.30.30.2
switch(config-dhcp-server-pool)# dns-server 125.0.0.1 125.0.0.2
switch(config-dhcp-server-pool)# static-bind ip 10.0.0.11 mac 24:be:05:24:75:73
switch(config-dhcp-server-pool)# option 3 ip 10.30.30.3
switch(config-dhcp-server-pool)# exit
switch(config-dhcp-server)# enable
```

**Configuring the DHCPv6 server on a VRF**

**Prerequisites**

- An enabled layer 3 interface.
- A VRF.
- An external storage device installed and configured (optional).

**Procedure**

1. Assign the DHCPv6 server to a VRF with the command `dhcv6-server vrf`. This switches to the DHCPv6 server configuration context.
2. If you want the DHCP server to be the sole authority for IP addresses on the VRF, enable authoritative mode with the command `authoritative`.
3. Define an address pool for the VRF with the command `pool`. This switches to the DHCPv6 server pool context. Customize pool settings as follows:
a. Define the range of addresses in the pool with the command `range`.
b. Set the DHCP lease time for addresses in the pool with the command `lease`.
c. Define up to four DNS servers with the command `dns-server`.
d. Create static bindings for specific addresses in the pool with the command `static-bind`.
e. Configure custom DHCP options for the pool with the command `option`.
f. Exit the DHCP server pool context with the command `exit`.

4. Enable the DHCPv6 server on the VRF with the command `enable`.
5. Configure support for persistent external storage of DHCP settings with the command `dhcv6p-server external-storage`.
6. View DHCPv6 server configuration settings with the command `show dhcpv6-server all-vrfs`.

**Example**

This example creates the following configuration:

- Configures a DHCPv6 server on VRF `primary-vrf`.
- Enables authoritative mode.
- Defines the pool `primary-pool` with the following settings:
  - Address range: `2001::1` to `2001::100`.
  - Lease time: 12 hours.
  - DNS servers: `2101::13` and `2101::14`.
  - Static binding of `2001::101` for client ID `1:0:a0:24:ab:fb:9c`.
  - DHCP custom option: `22` with IP address `2101::15`.

- Enables the DHCPv6 server.

```
switch(config)# dhcv6-server vrf primary
switch(config-dhcv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# range 2001::1 2001::100 prefix-len 64
switch(config-dhcpv6-server-pool)# lease 12:00:00
switch(config-dhcpv6-server-pool)# dns-server 2101::13 2101::14
switch(config-dhcpv6-server-pool)# static-bind ipv6 2001::10 client-id 1:0:a0:24:ab:fb:9c
switch(config-dhcpv6-server-pool)# option 22 ipv6 2101::15
switch(config-dhcpv6-server-pool)# exit
switch(config-dhcpv6-server)# enable
```

**DHCP server IPv4 commands**

**authoritative**

`authoritative`
`no authoritative`

**Description**

Configures the DHCPv4 server as `authoritative` on the current VRF. This means that the server is the sole authority for the network on the VRF. Therefore, if a client requests an IP address lease for which the server has no record, the server responds with DHCPNAK, indicating that the client must no longer use that IP address. If the server is not authoritative, then it will ignore DHCPv4 requests received for unknown leases from unknown hosts.

The `no` form of this command disables authoritative mode on the current VRF.
Example
Configures DHCPv4 server authoritative mode on VRF primary.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# authoritative
```

Removes the DHCPv4 server authoritative mode on VRF primary.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# no authoritative
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcp-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

bootp

```
bootp <REMOTE-URL>
no bootp <REMOTE-URL>
```

Description

Sets the BOOTP options that are returned by the DHCPv4 server for the current pool. BOOTP provides a way to distribute an IP address and boot image file to client stations. The DHCPv4 server returns the IP address and the location of the boot image file, which must be stored on an external TFTP server. The no form of this command disables support for BOOTP.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| `<REMOTE-URL>` | Specifies the name and location of a BOOTP file on a TFTP server in the format:
  tftp://{<IP> | <HOST>)/<FILE>
  - `<IP>`: Specifies the IP address of the TFTP server hosting the file in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100.
  - `<HOST>`: Specifies the fully-qualified domain name of the TFTP server hosting the file. Range: 1 to 64 printable ASCII characters.
  - `<FILE>`: Specifies the name of the BOOTP file. Range: 1 to 64 printable ASCII characters. |

Example
Defines BOOTP support on the DHCPv4 server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# bootp tftp://10.0.0.1/mybootfile
```

Deletes BOOTP support on the DHCPv4 server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no bootp tftp://10.0.0.1/mybootfile
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**clear dhcp-server leases**

`clear dhcp-server leases [all-vrfs | <IPV4-ADDR> vrf <VRF-NAME>] | vrf <VRF-NAME>]`

**Description**

Clears DHCPv4 server lease information. The DHCPv4 server must be disabled before clearing lease information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-vrfs</td>
<td>Clears leases for all VRFs.</td>
</tr>
<tr>
<td><code>&lt;IPV4-ADDR&gt; vrf &lt;VRF-NAME&gt;</code></td>
<td>Clears the lease for a specific client on a specific VRF. Specify the client address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100.</td>
</tr>
<tr>
<td>vrf <code>&lt;VRF-NAME&gt;</code></td>
<td>Clears leases for a specific VRF.</td>
</tr>
</tbody>
</table>

**Examples**

Clearing all DHCPv4 server leases.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# disable
switch(config-dhcp-server)# exit
```
DHCP

Clearing all DHCPv4 server leases for VRF `primary-vrf`.

```
switch(config)# exit
switch# clear dhcp-server leases
```

Clear the DHCPv4 server lease for IP address 10.10.10.1 on VRF `primary-vrf`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# disable
switch(config-dhcp-server)# exit
switch(config)# exit
switch# clear dhcp-server leases 10.10.10.1 vrf primary-vrf
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

`default-router`

default-router `<IPV4-ADDR-LIST>`
no default-router `<IPV4-ADDR-LIST>`

Description

Defines up to four default routers for the current DHCPv4 server pool.
The `no` form of this command removes the specified default routers from the pool.

```
<IPV4-ADDR-LIST>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV4-ADDR-LIST&gt;</code></td>
<td>Specifies the IP addresses of the default routers in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100. Separate addresses with a space. A maximum of four IP addresses can be defined.</td>
</tr>
</tbody>
</table>

Example
Defines two default routers, 10.0.0.1 and 10.0.0.10, for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# default-router ip 10.0.0.1 10.0.0.10
```

Deletes the default router 10.0.0.1 from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no default-router ip 10.0.0.1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dhcp-server external-storage**

dhcp-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
nodhcp-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]

**Description**

Configures the external storage file location for DHCPv4 server lease information. This file provides persistent storage, enabling DHCPv4 server settings to be restored when the switch is restarted. Lease information is stored in a flat file on the configured external device.

If external storage is not configured, then after a failure or reboot, all existing lease information is lost.

Lease information is saved to external storage each time the delay timer expires, which by default is every 300 seconds.

Lease information is not restored when issuing the command `dhcp-server enable`.

The `no` form of this command removes external storage support for the DHCPv4 server.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VOLUME-NAME&gt;</td>
<td>Specifies the external storage volume name. Range: 1 to 64 printable ASCII characters.</td>
</tr>
<tr>
<td>file &lt;LEASE-FILENAME&gt;</td>
<td>Specifies the external storage filename. Range: 1 to 255 printable ASCII characters.</td>
</tr>
<tr>
<td>delay &lt;DELAY&gt;</td>
<td>Specifies the interval in seconds between updates to the external storage file. Range: 15 to 86400. Default: 300.</td>
</tr>
</tbody>
</table>

**Example**
Stores the lease file on external storage volume **Storage1** in file **LeaseFile** at an interval of 600 seconds.

```
switch(config)# dhcp-server external-storage Storage1 file LeaseFile delay 600
```

Disables storage of the lease file on external storage volume **Storage1** in file **LeaseFile**.

```
switch(config)# no dhcp-server external-storage Storage1 file LeaseFile delay 600
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

#### dhcp-server vrf

dhcp-server vrf VRF-NAME  
no dhcp-server vrf VRF-NAME

description

Configures the DHCPv4 server to support a VRF and changes to the **config-dhcp-server** context for that VRF.

The `no` form of this command removes DHCPv4 server support on a VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>Name of a VRF.</td>
</tr>
</tbody>
</table>

### Example

Configures DHCPv4 server support on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
```

Removes DHCPv4 server support on VRF **primary**.

```
switch(config)# no dhcp-server vrf primary
```

### Command History
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**disable**

disable

**Description**

Disables the DHCPv4 server on the current VRF. The DHCPv4 server is disabled by default when configured on a VRF.

**Example**

Disables the DHCPv4 server on VRF primary.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# disable
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcp-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dns-server**

dns-server <IPV4-ADDR-LIST>
no dns-server <IPV4-ADDR-LIST>

**Description**

Defines up to four DNS servers for the current DHCPv4 server pool.

The no form of this command removes the specified DNS servers from the pool.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV4-ADDR-LIST&gt;</td>
<td>Specifies the IP addresses of the DNS servers in IPv4 format</td>
</tr>
</tbody>
</table>
### Parameter | Description
--- | ---
(x.x.x.x), where x is a decimal number from 0 to 255. Separate addresses with a space.

### Example
Defines two DNS servers for the server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# dns-server 10.0.20.1
```

Deletes a DNS server from the server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no dns-server 10.0.20.1
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### domain-name

domain-name `<DOMAIN-NAME>`

no domain-name `<DOMAIN-NAME>`

### Description
Defines a domain name for the current DHCPv4 server pool.
The `no` form of this command removes the specified domain name from the pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DOMAIN-NAME&gt;</code></td>
<td>Specifies a domain name. Range: 1 to 255 printable ASCII characters.</td>
</tr>
</tbody>
</table>

### Example
Defines a domain name for the server pool `primary-pool` on VRF `primary`.
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# domain-name example.org.in

Deletes a domain name from the server pool `primary-pool` on VRF `primary`.

switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no domain-name example.org.in

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**enable**

<table>
<thead>
<tr>
<th>enable</th>
</tr>
</thead>
</table>

**Description**

Enables the DHCPv4 server on the current VRF. The DHCPv4 server is disabled by default when configured on a VRF.

**Example**

Enables the DHCPv4 server on VRF `primary`.

switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# enable

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcp-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
**http-proxy**

`http-proxy <FQDN | IPV4-ADDR> [vrf <VRF-NAME>]`

`no http-proxy <FQDN | IPV4-ADDR> [vrf <VRF-NAME>]`

**Description**

 Specifies HTTP proxy location and VRF.

 The `no` form of this command removes a specified HTTP proxy location.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;FQDN&gt;</code></td>
<td>Specifies FQDN for HTTP proxy location.</td>
</tr>
<tr>
<td><code>&lt;IPV4-ADDR&gt;</code></td>
<td>Specifies IPV4 address for HTTP proxy location.</td>
</tr>
<tr>
<td><code>&lt;VRF-NAME&gt;</code></td>
<td>Specifies VRF for HTTP proxy.</td>
</tr>
</tbody>
</table>

A FQDN or IPV4 address are optional in the `no` form of the command.

**Usage**

- HTTP proxy location can be configured using the CLI/REST interface or auto-configured through the DHCP server connected to the switch.
- There are three sources for HTTP proxy location:
  - User configured HTTP proxy via CLI or REST interface.
  - DHCP options received via management/OOBM port.
  - DHCP options received via VLAN 1 on supported switch platforms.
- Operational configuration for HTTP proxy location is determined by the source with the highest priority.
  - Source priority:
    1. User configured.
    2. DHCP options received via management/OOBM port.
    3. DHCP options received via VLAN 1.

- HTTP proxy location can only be a FQDN or an IPV4 address.
- When HTTP proxy location and VRF are configured, they override any existing HTTP proxy location and VRF.
- If this command is executed without the VRF parameter, the default VRF will be used.
- Port number may need to be specified at the end of the IP address for FQDN to connect via HTTP proxy.
  - For example, 8088 is the TCP port number: `http-proxy 192.168.248.248:8088`

**Examples**

Specifying a FQDN for HTTP proxy location and MGMT VRF:

```bash
switch(config)# http-proxy http-proxy.aruba.com vrf mgmt
```

Removing HTTP proxy location
switch(config)# no http-proxy

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

lease

lease {<TIME> | infinite}
no lease

Description

Sets the length of the DHCPv4 lease time for the current pool. The lease time determines how long an IP address is valid before a DHCPv4 client must request that it be renewed.

The no form of this command returns the DHCPv4 lease time to its default value 1 hour.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TIME&gt;</td>
<td>Sets the DHCPv4 lease time. Format: DD:HH:MM. Default: 01:00:00.</td>
</tr>
<tr>
<td>infinite</td>
<td>Sets the DHCPv4 lease time to infinite. This means that addresses do not need to be renewed.</td>
</tr>
</tbody>
</table>

Example

Sets the lease time for DHCPv4 server pool primary-pool on VRF primary to 12 hours.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# lease 00:12:00
```

Deletes the lease time for DHCPv4 server pool primary-pool on VRF primary.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no lease 00:12:00
```
netbios-name-server

netbios-name-server <IPV4-ADDR-LIST>
no netbios-name-server <IPV4-ADDR-LIST>

Description
Defines up to four NetBIOS WINS servers for the current DHCPv4 server pool. WINS is used by Microsoft DHCP clients to match host names with IP addresses.
The no form of this command removes the specified WINS servers from the pool.

Parameter | Description
--- | ---
<IPV4-ADDR-LIST> | Specifies the IP addresses of NetBIOS (WINS) servers in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Separate addresses with a space. A maximum of four IP addresses can be defined.

Example
Defines two WINS servers for the server pool primary-pool on VRF primary.

```bash
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# netbios-name-server ip 10.0.20.1 10.0.30.10
```

Deletes a WINS server from the server pool primary-pool on VRF primary.

```bash
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no netbios-name-server ip 10.0.20.1
```
### Platforms
<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### netbios-node-type

**Syntax**

- `netbios-node-type <TYPE>`
- `no netbios-node-type <TYPE>`

**Description**

Defines the NetBIOS node type for the current DHCPv4 server pool.

The `no` form of this command removes the NetBIOS node type for the current pool.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;TYPE&gt;</code></td>
<td>Specifies the NetBIOS node type: broadcast, hybrid, mixed, or peer-to-peer.</td>
</tr>
</tbody>
</table>

**Examples**

Defines the NetBIOS node type **broadcast** for the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# netbios-node-type broadcast
```

Deletes the NetBIOS node type **broadcast** from the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no netbios-node-type broadcast
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### option

**Syntax**

- `option <OPTION-NUM> {ascii <ASCII-STR> | hex <HEX-STR> | ip <IPV4-ADDR-LIST>}`
- `no option <OPTION-NUM> {ascii <ASCII-STR> | hex <HEX-STR> | ip <IPV4-ADDR-LIST>}`

**Description**
Defines custom DHCPv4 options for the current DHCPv4 server pool. DHCPv4 options enable the DHCPv4 server to provide additional information about the network when DHCPv4 clients request an address. The no form of this command removes custom DHCPv4 options from the pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;OPTION-NUM&gt;</td>
<td>Specifies a DHCPv4 option number. For a list of DHCPv4 option numbers, see <a href="https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml">https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml</a>. Range: 2 to 254.</td>
</tr>
<tr>
<td>ascii &lt;ASCII-STR&gt;</td>
<td>Specifies a value for the selected option as an ASCII string. Range: 1 to 255 ASCII characters.</td>
</tr>
<tr>
<td>hex &lt;HEX-STR&gt;</td>
<td>Specifies a value for the selected option as a hexadecimal string. Range: 1 to 255 hexadecimal characters.</td>
</tr>
<tr>
<td>ip &lt;IPV4-ADDR-LIST&gt;</td>
<td>Specifies a list of IP addresses in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Separate addresses with a space. A maximum of four IP addresses can be defined.</td>
</tr>
</tbody>
</table>

**Example**

Defines DHCPv4 option 3 for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# option 3 ip 192.168.1.1
```

Deletes DHCPv4 option 3 for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no option 3 ip 192.168.1.1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-dhcp-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**pool**

pool <POOL-NAME>
no pool <POOL-NAME>

**Description**
Creates a DHCPv4 server pool for the current VRF and switches to the `config-dhcp-server-pool` context for it. Multiple pools, each with a distinct range, can be assigned to a VRF. A maximum of 64 pools (IPv4 and IPv6), 64 address ranges, and 8182 clients are supported on the switch across all VRFs.

The `no` form of this command deletes the specified DHCPv4 server pool.

### Parameter | Description
--- | ---
`<POOL-NAME>` Specifies the DHCPv4 pool name. A maximum of 64 pools (IPv4 and IPv6) are supported across VRFs on the switch. Range: 1 to 32 printable ASCII characters. First character must be a letter or number.

### Example

**Creates the DHCPv4 server pool** `primary-pool` **on VRF** `primary`

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)#
```

**Deletes the DHCPv4 server pool** `primary-pool` **on VRF** `primary`

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# no pool primary-pool
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcp-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-dhcp-server</td>
<td></td>
</tr>
</tbody>
</table>

### range

```
range <LOW-IPV4-ADDR> <HIGH-IPV4-ADDR> [prefix-len <MASK>]
no range <LOW-IPV4-ADDR> <HIGH-IPV4-ADDR> [prefix-len <MASK>]
```

### Description

 Defines the range of IP addresses supported by the current DHCPv4 server pool. A maximum of 64 ranges are supported per switch across all VRFs.

The `no` form of this command deletes the address range for the current pool.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;LOW-IPV4-ADDR&gt;</code></td>
<td>Specifies the lowest IP address in the pool in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
<tr>
<td><code>&lt;HIGH-IPV4-ADDR&gt;</code></td>
<td>Specifies the highest IP address in the pool in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
<tr>
<td>prefix-len <code>&lt;MASK&gt;</code></td>
<td>Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.</td>
</tr>
</tbody>
</table>

**NOTE:** When active gateway is configured on the interface serviced by the pool, you must specify a prefix length that matches the mask on the IP address assigned to the interface. Otherwise, client stations will get a prefix length from active gateway that may not be consistent with the configured range, and a DHCP error will occur. In the following example, the DHCP range prefix is set to 16 to match the mask on the IP address assigned to interface VLAN 2.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip address 200.1.1.1/16
switch(config-if-vlan)# active-gateway ip 200.1.1.3
    mac 00:aa:aa:aa:aa:aa
switch(config-if-vlan)# exit
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# range 192.168.1.1 192.168.1.100
```

**Examples**

Defines the address range **192.168.1.1** to **192.168.1.100** with a mask of **24** bits for the DHCPv4 server pool primary-pool on VRF primary.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# 192.168.1.1 192.168.1.100 prefix-len 24
```

Deletes the address range **192.168.1.1** to **192.168.1.100** with a mask of **24** bits from the DHCPv4 server pool primary-pool on VRF primary.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no 192.168.1.1 192.168.1.100 prefix-len 24
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
Platforms | Command context | Authority
---|---|---
6300 6400 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command.

**show dhcp-server**

show dhcp-server [all-vrfs]
show dhcp-server leases [all-vrfs | vrf <VRF-NAME>]
show dhcp-server pool <POOL-NAME> [vrf <VRF-NAME>]

**Description**

Shows configuration settings for the DHCPv4 server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-vrfs</td>
<td>Shows DHCPv4 server configuration settings for all VRFs.</td>
</tr>
<tr>
<td>leases [all-vrfs</td>
<td>vrf &lt;VRF-NAME&gt;]</td>
</tr>
<tr>
<td>pool &lt;POOL-NAME&gt; [vrf &lt;VRF-NAME&gt;]</td>
<td>Shows DHCPv4 server pool configuration settings for all VRFs or a specific VRF.</td>
</tr>
</tbody>
</table>

**Examples**

Showing all DHCPv4 server configuration settings.

```
switch# show dhcp-server
VRF Name : default
DHCP Server : enabled
Operational State : operational
Authoritative Mode : false
Pool Name : test
Lease Duration : 00:01:00

DHCP dynamic IP allocation
---------------------------
Start-IP-Address End-IP-Address Prefix-Length
-------- -------- ---------
192.168.1.1 192.168.1.20 24

DHCP Server options
---------------------
Option-Number Option-Type Option-Value
------------- -------- ------------
6      ip          10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.6

DHCP Server static IP allocation
---------------------------------
IP-Address Client-Hostname State MAC-Address
------- -------- -------- ---------
10.0.0.3 * OPERATIONAL aa:aa:aa:aa:aa:aa
```
DHCP

BOOTP Options
-----------------
Boot-File-Name  TFTP-Server-Name  TFTP-Server-Address
-----------------  -----------------  -----------------
boot.txt        *                  10.0.0.10

Showing DHCP server configuration settings for VRF primary-vrf.

switch# `show dhcp-server vrf primary-vrf`

VRF Name : primary-vrf
DHCP Server : disabled
Operational State : disabled
Authoritative Mode : false

Pool Name : test
Lease Duration : 00:01:00

DHCP dynamic IP allocation
--------------------------
Start-IP-Address  End-IP-Address  Prefix-Length
--------------------------  --------------------------  ---------------
10.0.0.1          10.0.0.30       *
192.168.1.1      192.168.1.20     24
192.168.10.30   192.168.10.60     16

DHCP Server options
---------------------
Option-Number  Option-Type  Option-Value
---------------------  ---------------------  ---------------------
6                   ip          10.0.0.3  10.0.0.4  10.0.0.5  10.0.0.6
18                  ascii        aswed

DHCP Server static IP allocation
-------------------------------
IP-Address  Client-Hostname  MAC-Address
------------  -----------------  -------------------
10.0.0.1     *                aa:bb:cc:11:12:4a

BOOTP Options
-------------
Boot-File-Name  TFTP-Server-Name  State  TFTP-Server-Address
-------------  -----------------  ---------  -----------------
boot.txt       *                  OPERATIONAL  10.0.0.10

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
**Platforms**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**static-bind**

`static-bind ip <IPV4-ADDR> mac <MAC-ADDR> [hostname <HOST>]

no static-bind <IPV4-ADDR-LIST>`

**Description**

Creates a static binding that associates an IP address in the current pool with a specific MAC address. This causes the DHCPv4 server to only assign the specified IP address to a client station with the specified MAC address.

The `no` form of this command removes the specified binding.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV4-ADDR&gt;</code></td>
<td>Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. The IP address must be within the address range defined for the current pool.</td>
</tr>
<tr>
<td><code>mac &lt;MAC-ADDR&gt;</code></td>
<td>Specifies a client station MAC address (xx:xx:xx:xx:xx:xx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td><code>hostname &lt;HOST&gt;</code></td>
<td>Specifies the host name of the client station. Range: 1 to 255 printable ASCII characters</td>
</tr>
</tbody>
</table>

**Examples**

Defines a static address for the server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# static-bind ip 10.0.0.1 mac 24:be:05:24:75:73
```

Deletes a static address from the server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no static-bind ip 10.0.0.1 mac 24:be:05:24:75:73
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
DHCP server IPv6 commands

**authoritative**

*authoritative*

*no authoritative*

**Description**

Configures the DHCPv6 server as *authoritative* on the current VRF. This means that the server is the sole authority for the network on the VRF. It responds to client solicit messages with advertise messages having a priority/preference value set to 255 (the maximum), instead of 0 (the minimum). Clients always choose the DHCPv6 server with the highest priority/preference value. If two DHCPv6 servers send an advertise message with the same priority/preference value, then the client picks one and discards the other. The *no* form of this command disables authoritative mode on the current VRF.

**Example**

Configures DHCPv6 server authoritative mode on VRF *primary*.

```bash
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# authoritative
```

Removes DHCPv6 server authoritative mode on VRF *primary*.

```bash
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# no authoritative
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcpv6-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-dhcpv6-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**clear dhcpv6-server leases**

*clear dhcpv6-server leases [all-vrfs | <IPV6-ADDR> vrf <VRF-NAME>] | vrf <VRF-NAME>]*

**Description**

Clears DHCPv6 server lease information. The DHCPv6 server must be disabled before clearing lease information.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-vrfs</td>
<td>Clears leases for all VRFs.</td>
</tr>
<tr>
<td>&lt;IPV6-ADDR&gt; vrf &lt;VRF-NAME&gt;</td>
<td>Clears the lease for a specific client on a specific VRF. Specify the</td>
</tr>
<tr>
<td></td>
<td>where x is a hexadecimal number from 0 to F. You can use two colons (:) to</td>
</tr>
<tr>
<td></td>
<td>represent consecutive zeros (but only once), remove leading zeros, and</td>
</tr>
<tr>
<td></td>
<td>collapse a hextet of four zeros to a single 0. For example, this address</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Clears leases for a specific VRF.</td>
</tr>
</tbody>
</table>

**Examples**

Clearing all DHCPv6 server leases.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
switch(config-dhcpv6-server)# exit
switch(config)# exit
switch# clear dhcpv6-server leases
```

Clearing all DHCPv6 server leases for VRF `primary-vrf`.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
switch(config-dhcpv6-server)# exit
switch(config)# exit
switch# clear dhcpv6-server leases vrf primary-vrf
```

Clear the DHCPv6 server lease for IP address `2001::1` on VRF `primary-vrf`.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
switch(config-dhcpv6-server)# exit
switch(config)# exit
switch# clear dhcpv6-server leases 2001::1 vrf primary-vrf
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with</td>
</tr>
<tr>
<td>Platforms</td>
<td>Command context</td>
<td>Authority</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>6400</td>
<td>execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
<td></td>
</tr>
</tbody>
</table>

**dhcv6p-server external-storage**

dhcv6-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
no dhcv6-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]

**Description**

Configures the external storage file location for DHCPv6 server lease information. This file provides persistent storage, enabling DHCPv6 server settings to be restored when the switch is restarted. Lease information is stored in a flat file on the configured external device.

If external storage is not configured, then after a failure or reboot, all existing lease information is lost.

Lease information is saved to external storage each time the delay timer expires, which by default is every 300 seconds.

Lease information is not restored when issuing the command dhcp-server enable.

The no form of this command removes external storage support for the DHCPv6 server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VOLUME-NAME&gt;</td>
<td>Specifies the external storage volume name. Range: 1 to 64 printable ASCII characters.</td>
</tr>
<tr>
<td>file &lt;LEASE-FILENAME&gt;</td>
<td>Specifies the external storage filename. Range: 1 to 255 printable ASCII characters.</td>
</tr>
<tr>
<td>delay &lt;DELAY&gt;</td>
<td>Specifies the interval in seconds between updates to the external storage file. Range: 15 to 86400. Default: 300.</td>
</tr>
</tbody>
</table>

**Example**

Stores the lease file on external storage volume **Storage1** in file **LeaseFile** at an interval of 600 seconds.

```
switch(config)# dhcv6-server external-storage Storage1 file LeaseFile delay 600
```

Disables storage of the lease file on external storage volume **Storage1** in file **LeaseFile**.

```
switch(config)# no dhcv6-server external-storage Storage1 file LeaseFile delay 600
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
**dhcpv6-server vrf**

dhcpv6-server vrf VRF-NAME  
no dhcpv6-server vrf VRF-NAME

**Description**

Configures the DHCPv6 server to support a VRF and changes to the config-dhcpv6-server context for that VRF.

The `no` form of this command removes DHCPv6 server support on a VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF-NAME</td>
<td>Name of a VRF.</td>
</tr>
</tbody>
</table>

**Example**

Configures DHCPv6 server support on VRF `primary`.

```
switch(config)# dhcpv6-server vrf primary
```

Removes the DHCPv6 server support on VRF `primary`.

```
switch(config)# no dhcpv6-server vrf primary
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Disables the DHCPv6 server on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcpv6-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dns-server**

dns-server `<IPV6-ADDR-LIST>`
no dns-server `<IPV6-ADDR-LIST>`

### Description

Defines up to four DNS servers for the current DHCPv6 server pool.

The `no` form of this command removes the specified DNS servers from the pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV6-ADDR-LIST&gt;</code></td>
<td>Specifies the IP addresses of the DNS servers in IPv6 format (xxxx::xxxx::xxxx::xxxx::xxxx::xxxx::xxxx), where x is a hexadecimal number from 0 to F. Separate addresses with a space. A maximum of four IP addresses can be defined.</td>
</tr>
</tbody>
</table>

### Example

Defines DNS server `2001::13` for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# dns-server 2001::13
```

Deletes DNS server `2001::13` from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no dns-server 2001::13
```

### Command History
**enable**

**Description**
Enables the DHCPv6 server on the current VRF. The DHCPv6 server is disabled by default when configured on a VRF.

**Example**
Enables the DHCPv6 server on VRF `primary`.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcpv6-server)# enable
```

**lease**

**Description**
Sets the length of the DHCPv6 lease time for the current pool. The lease time determines how long an IP address is valid before a DHCPv6 client must request that it be renewed.

The `no` form of this command returns the DHCPv6 lease time to the default value 1 hour.
Parameter | Description
--- | ---
<TIME> | Sets the DHCPv6 lease time. Format: DD:HH:MM. Default: 01:00:00.
infinite | Sets the DHCPv6 lease time to infinite. This means that addresses do not need to be renewed.

**Example**

Sets the lease time for DHCPv6 server pool **primary-pool** on VRF **primary** to 12 hours.

```plaintext
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# lease 00:12:00
```

Sets the lease time for DHCP server pool **primary-pool** on VRF **primary** to the default value.

```plaintext
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no lease 00:12:00
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcpv6-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**option**

```plaintext
option <OPTION-NUM> {ascii <ASCII-STR> | hex <HEX-STR> | ip <IPV6-ADDR-LIST>}
no option <OPTION-NUM> {ascii <ASCII-STR> | hex <HEX-STR> | ip <IPV6-ADDR-LIST>}
```

**Description**

Defines custom DHCPv6 options for the current DHCPv6 server pool.

The **no** form of this command removes custom DHCPv6 options from the pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;OPTION-NUM&gt;</td>
<td>Specifies a DHCPv6 option number. Range: 2 to 254.</td>
</tr>
<tr>
<td>ascii &lt;ASCII-STR&gt;</td>
<td>Specifies a value for the selected option as an ASCII string. Range: 1 to 255 ASCII characters.</td>
</tr>
<tr>
<td>hex &lt;HEX-STR&gt;</td>
<td>Specifies a value for the selected option as a hexadecimal string.</td>
</tr>
</tbody>
</table>
### Parameter | Description
--- | ---
| | Range: 1 to 255 hexadecimal characters.
| ip <IPV6-ADDR-LIST> | Specifies a list of IP addresses for the option in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

### Example

**Defines DHCPv6 option 22 for the server pool primary-pool on VRF primary.**

```plaintext
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# option 22 ipv6 2001::12
```

**Deletes DHCPv6 option 22 for the server pool primary-pool on VRF primary.**

```plaintext
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no option 22 ipv6 2001::12
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-dhcpv6-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### pool

### Description

Creates a DHCPv6 server pool for the current VRF and switches to the `config-dhcpv6-server-pool` context for it. Multiple pools, each with a distinct range, can be assigned to a VRF. A maximum of 64 pools (IPv4 and IPv6), 64 address ranges, and 8182 clients are supported on the switch across all VRFs.

The `no` form of this command deletes the specified DHCPv6 server pool.

### Parameter | Description
--- | ---
| <POOL-NAME> | Specifies the DHCPv6 pool name. A maximum of 64 pools (IPv4 and IPv6) are supported across VRFs on the switch. Range: 1 to 32 printable ASCII characters. First character must be a letter or number. |
Example

Creates the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)#
```

Deletes the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# no pool primary-pool
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcpv6-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-dhcpv6-server</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**range**

range **<LOW-IPV6-ADDR> <HIGH-IPV6-ADDR> [prefix-len <MASK>]**
no range **<LOW-IPV6-ADDR> <HIGH-IPV6-ADDR> [prefix-len <MASK>]**

**Description**

Defines the range of IP addresses supported by the current DHCPv6 server pool. A maximum of 64 ranges are supported per switch across all VRFs.

The **no** form of this command deletes the address range for the current pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;LOW-IPV6-ADDR&gt;</strong></td>
<td>Specifies the lowest IP address in the pool in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where × is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td><strong>&lt;HIGH-IPV6-ADDR&gt;</strong></td>
<td>Specifies the highest IP address in the pool in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where × is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td><strong>prefix-len &lt;MASK&gt;</strong></td>
<td>Specifies the number of bits in the address mask in CIDR format (×), where × is a decimal number from 64 to 128.</td>
</tr>
</tbody>
</table>

**Example**

Defines an address range for the DHCPv6 server pool **primary-pool** on VRF **primary**.
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# range 2001::1 2001::10 prefix-len 64

Deletes an address range for the DHCPv6 server pool primary-pool on VRF primary.

switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no range 2001::1 2001::10 prefix-len 64

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcpv6-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-dhcpv6-server-pool</td>
<td></td>
</tr>
</tbody>
</table>

**show dhcpv6-server**

show dhcpv6-server [all-vrfs]
show dhcpv6-server leases {all-vrfs | vrf <VRF-NAME>}
show dhcpv6-server pool <POOL-NAME> [vrf <VRF-NAME>]

**Description**

Shows configuration settings for the DHCPv6 server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-vrfs</td>
<td>Shows DHCPv6 server configuration settings for all VRFs.</td>
</tr>
<tr>
<td>leases {all-vrfs</td>
<td>vrf &lt;VRF-NAME&gt;}</td>
</tr>
<tr>
<td>pool &lt;POOL-NAME&gt; [vrf &lt;VRF-NAME&gt;]</td>
<td>Shows DHCPv6 server pool configuration settings for all VRFs or a specific VRF.</td>
</tr>
</tbody>
</table>

**Examples**

Showing all DHCPv6 server configuration settings.

switch# show dhcpv6-server

VRF Name : default
DHCPv6 Server : enabled
Operational State : operational
Authoritative Mode : true
Pool Name : test
Lease Duration : 00:01:00

DHCPv6 dynamic IP allocation

<table>
<thead>
<tr>
<th>Start-IPv6-Address</th>
<th>End-IPv6-Address</th>
<th>Prefix-Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::2</td>
<td>2001::10</td>
<td>64</td>
</tr>
</tbody>
</table>

DHCPv6 Server options

<table>
<thead>
<tr>
<th>Option-Number</th>
<th>Option-Type</th>
<th>Option-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>ipv6</td>
<td>2001::15</td>
</tr>
</tbody>
</table>

DHCPv6 Server static IP allocation

DHCPv6 Server static host is not configured.

Showing DHCPv6 server configuration settings for VRF primary-vrf.

switch# show dhcpv6-server vrf primary-vrf

VRF Name : primary-vrf
DHCPv6 Server : disabled
Operational State : standby
Authoritative Mode : false

Pool Name : test
Lease Duration : 00:01:00

DHCPv6 dynamic IP allocation

<table>
<thead>
<tr>
<th>Start-IPv6-Address</th>
<th>End-IPv6-Address</th>
<th>Prefix-Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000::1</td>
<td>2000::20</td>
<td>*</td>
</tr>
<tr>
<td>2001::20</td>
<td>2001::50</td>
<td>*</td>
</tr>
<tr>
<td>2001::2</td>
<td>2001::10</td>
<td>64</td>
</tr>
<tr>
<td>2010::20</td>
<td>2010::40</td>
<td>*</td>
</tr>
</tbody>
</table>

DHCPv6 Server options

<table>
<thead>
<tr>
<th>Option-Number</th>
<th>Option-Type</th>
<th>Option-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>ipv6</td>
<td>2001::15</td>
</tr>
<tr>
<td>23</td>
<td>ipv6</td>
<td>2001::30</td>
</tr>
<tr>
<td>30</td>
<td>ipv6</td>
<td>2001::10</td>
</tr>
</tbody>
</table>

DHCPv6 Server static IP allocation

DHCPv6 Server static host is not configured.

Pool Name : v6test
Lease Duration : 00:01:00

DHCPv6 dynamic IP allocation

<table>
<thead>
<tr>
<th>Start-IPv6-Address</th>
<th>End-IPv6-Address</th>
<th>Prefix-Length</th>
</tr>
</thead>
</table>
DHCPv6 Server options

<table>
<thead>
<tr>
<th>Option-Number</th>
<th>Option-Type</th>
<th>Option-Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>ipv6</td>
<td>2001::20</td>
</tr>
<tr>
<td>23</td>
<td>ipv6</td>
<td>2001::0db8:85a3:0000:0000:8a2e:0370:7334</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2001::0db8:85a3:0000:0000:8a2e:0370:7335</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2001::0db8:85a3:0000:0000:8a2e:0370:7336</td>
</tr>
</tbody>
</table>

DHCPv6 Server static IP allocation

<table>
<thead>
<tr>
<th>IPv6-Address</th>
<th>Client-Hostname</th>
<th>State</th>
<th>Client-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>2100::4</td>
<td>*</td>
<td>OPERATIONAL</td>
<td>1:0:a0:24:ab:fb:9c</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

static-bind

static-bind ipv6 <IPV6-ADDR> client-id <ID> [hostname <HOST>]
nostatic-bind ipv6 <IPV6-ADDR-LIST>

Description

Creates a static binding that associates an IP address in the current pool with a client identifier or DUID. This causes the DHCPv6 server to only assign the specified IP address to a client station with the specified client identifier or DUID.

The no form of this command removes the specified static binding from the pool.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the IP address to assign in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>client-id &lt;ID&gt;</td>
<td>Specifies the client identifier or DUID.</td>
</tr>
<tr>
<td>hostname &lt;HOST&gt;</td>
<td>Specifies the host name of the client station. Range: 1 to 255 printable ASCII characters</td>
</tr>
</tbody>
</table>

**Example**

Defines a static address for the DHCPv6 server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# static-bind ipv6 2001::10 client-id 1:0:a0:24:ab:fb:9c
```

Deletes a static address from the DHCPv6 server pool `primary-pool` on VRF `primary`.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no static-bind ipv6 2001::10 client-id 1:0:a0:24:ab:fb:9c
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-dhcpv6-server-pool</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Overview

DHCP is a protocol used by DHCP servers in IP networks to dynamically allocate network configuration data to client devices (DHCP clients). Possible network configuration data includes user IP address, subnet mask, default gateway IP address, DNS server IP address, and lease duration. The DHCP protocol enables DHCP clients to be dynamically configured with such network configuration data without any manual setup process.

DHCP snooping is a security feature that helps avoid problems caused by an unauthorized DHCP server on the network that provides invalid configuration data to DHCP clients. A user without malicious intent may cause this problem by unknowingly adding to the network a switch or other device that includes a DHCP server enabled by default. In some cases, a user with malicious intent adds a DHCP server to the network as part of their Denial of Service or Man in the Middle attack.

DHCP snooping helps prevent such problems by distinguishing between trusted ports connected to legitimate DHCP servers, and untrusted ports connected to general users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. DHCP Packets from untrusted sources are dropped.

In addition, in support of the separate IP source lockdown feature, DHCP snooping also dynamically collects client information (VLAN, IPv4 address, MAC address, interface), adding the information to the switch IP binding database. Alternatively, also in support of IP lockdown, the IP binding database can be statically updated using the **ipv4 source-binding** or **ipv6 source-binding** commands. Statically configured IP binding information supersedes any dynamically collected information for the same client.

---

DHCP Snooping and DHCP relay can be configured on the same switch.

When DHCP snooping and DHCP relay are both enabled on a VLAN, the following actions occur:

- Received packet: DHCP snooping processes the DHCP packet before (possibly) handing it to DHCP relay.
- Transmitted packet: DHCP packets sent by DHCP relay are intercepted by DHCP snooping to learn IP bindings.

---

For even more rigorous security that is applied in hardware on a packet-by-packet basis, you can use IP source lockdown feature as described in **IP source lockdown**.

---

**DHCP server interoperation**

DHCP server may not be configured with DHCP snooping.

**DHCPv4 snooping conditions for dropping DHCPv4 packets**

Applies only to DHCPv4 snooping.
### Packet types that are dropped

<table>
<thead>
<tr>
<th>Conditions for dropping the packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP OFFER, DHCPACK, DHCPNAK</td>
</tr>
</tbody>
</table>
| A packet from a DHCP server is received on an untrusted port.  
  The switch is configured with a list of authorized DHCP server addresses and a packet is received from a DHCP server on a trusted port with a source IP address that is not in the list of authorized DHCP server addresses. |
| DHCPRELEASE, DHCPDECLINE            |
| A broadcast packet that has a MAC address in the DHCP binding database, but the port in the DHCP binding database does not match the port on which the packet is received. |
| All DHCP packet types               |
| When enabled (the default) a DHCP packet received on an untrusted port in which the DHCP client hardware MAC address does not match the source MAC address in the packet.  
  When enabled (the default), a DHCP packet containing DHCP relay information (option 82) is received from an untrusted port. |

---

### DHCPv4 snooping commands

**clear dhcpv4-snooping binding**

clear dhcpv4-snooping binding {all | ip <IPV4-ADDR> vlan <VLAN-ID> | port <PORT-NUM> | vlan <VLAN-ID>}

**Description**

Clears DHCPv4 snooping binding entries.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies that all DHCPv4 binding information is to be cleared.</td>
</tr>
<tr>
<td>ip &lt;IPV4-ADDR&gt;</td>
<td>Specifies the IPv4 address and VLAN for which all DHCPv4 binding information is to be cleared.</td>
</tr>
<tr>
<td>vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the VLAN for which all DHCPv4 binding information is to be cleared.</td>
</tr>
<tr>
<td>port &lt;PORT-NUM&gt;</td>
<td>Specifies the port number for which all DHCPv4 binding information is to be cleared.</td>
</tr>
</tbody>
</table>

**Examples**

On the 6400 Switch Series, *interface identification differs.*

Clearing all DHCPv4 binding information for IP address 192.168.2.4 and VLAN 5:

```
switch(config)# clear dhcpv4-snooping binding ip 192.168.2.4 vlan 5
```

Clearing all DHCPv4 binding information for port 1/1/1:
Clearing all DHCPv4 binding information for VLAN 10:

```
switch(config)# clear dhcpv4-snooping binding vlan 10
```

Clearing all DHCPv4 binding information:

```
switch(config)# clear dhcpv4-snooping binding all
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**clear dhcpv4-snooping statistics**

```
clear dhcpv4-snooping statistics
```

**Description**

Clears all DHCPv4 snooping statistics.

**Examples**

Clear all DHCPv4 snooping statistics:

```
switch# clear dhcpv4-snooping statistics
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;) or Manager</td>
<td>Operators or Administrators or local user group members with</td>
</tr>
</tbody>
</table>
The document contains information about the `dhcpv4-snooping` command, including its description, examples, command history, and command information. The `dhcpv4-snooping` command enables DHCPv4 snooping, which is disabled by default. The `no dhcpv4-snooping` command disables DHCPv4 snooping on a specified VLAN, flushing all the IP bindings learned since DHCPv4 snooping was enabled. Examples provided include enabling DHCPv4 snooping on VLAN 100.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### dhcpv4-snooping (in config-vlan context)

The `dhcpv4-snooping` command is used within the `config-vlan` context to enable DHCPv4 snooping on a specific VLAN. The `no dhcpv4-snooping` command disables DHCPv4 snooping on that VLAN. The examples demonstrate enabling DHCPv4 snooping on VLAN 100.
Disabling DHCPv4 snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no dhcpv4-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-vlan</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-vlan</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dhcpv4-snooping allow-overwrite-binding**

```
dhcpv4-snooping allow-overwrite-binding
no dhcpv4-snooping allow-overwrite-binding
```

**Description**

Allows binding to be overwritten for the same IP address. When enabled, and a DHCP server offers a host an IP address that is already bound to an existing host in the binding table, the existing binding is overwritten for the new host if the new host is successfully able to acquire the same IP address. This overwriting is disabled by default, causing the DHCP server offers to be dropped.

The no form of the command disables DHCPv4 snooping overwrite binding.

**Examples**

Enabling DHCPv4 snooping overwrite binding:

```
switch(config)# dhcpv4-snooping allow-overwrite-binding
```

Disabling DHCPv4 snooping overwrite binding:

```
switch(config)# no dhcpv4-snooping allow-overwrite-binding
```
DHCP snooping authorized-server

dhcpv4-snooping authorized-server <IPV4-ADDR> [vrf <VRF-NAME>]
no dhcpv4-snooping authorized-server <IPV4-ADDR> [vrf <VRF-NAME>]

Description
Adds an authorized (trusted) DHCP server to a list of authorized servers for use by DHCPv4 snooping. This command can be issued multiple times, adding a maximum of 20 authorized servers per VRF. By default, with an empty list of authorized servers, all DHCP servers are considered to be trusted for DHCPv4 snooping purposes.

The mgmt VRF cannot be used with this command.

The no form of this command deletes the specified DHCP server from the authorized list.

Parameter | Description
--- | ---
<IPV4-ADDR> | Specifies the IPv4 address of the trusted DHCPv4 server.
vrf <VRF-NAME> | Specifies the VRF name. The name can be default or a configured VRF instance but it cannot be mgmt.

Usage
For authorized server lookup, the VRF is derived from the Switch Virtual Interface (SVI) configured for the incoming VLAN. If the SVI is not configured, the default VRF is assumed.

Examples
Adding DHCP servers 192.168.2.2, 192.168.2.3, and 192.168.2.10 to the authorized server list:

```
switch(config)# dhcpv4-snooping authorized-server 192.168.2.2
switch(config)# dhcpv4-snooping authorized-server 192.168.2.3 vrf default
switch(config)# dhcpv4-snooping authorized-server 192.168.2.10 vrf default
```

Removing DHCP server 192.168.2.3 from the authorized server list:

```
switch(config)# no dhcpv4-snooping authorized-server 192.168.2.3 vrf default
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dhcpv4-snooping external-storage**

dhcpv4-snooping external-storage volume `<VOL-NAME>` file `<FILE-NAME>`

no dhcpv4-snooping external-storage volume `<VOL-NAME>` file `<FILE-NAME>`

**Description**

Configures external storage to be used for backing up IP bindings (used by DHCPv4 snooping) to a file. When configured, the switch stores all the IP bindings in an external storage file so that they are retained after the switch restarts. When the switch restarts, it reads the IP bindings from the configured external storage file to populate its local cache.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IP bindings in an external storage file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volume <code>&lt;VOL-NAME&gt;</code></td>
<td>Specifies the name of the existing external storage volume where the IP bindings file will be saved. Before running the <code>dhcpv4-snooping external-storage volume</code> command, first create the external storage volume using command <code>external-storage &lt;VOLUME-NAME&gt;</code>. See External storage commands in the Command-Line Interface Guide.</td>
</tr>
<tr>
<td>file <code>&lt;FILE-NAME&gt;</code></td>
<td>Specifies the file name to use for storing IP bindings. Maximum 255 characters.</td>
</tr>
</tbody>
</table>

Configuring IP bindings storage in file `dsnoop_ipbindings` on existing volume `dhcp_snoop`:

```
switch(config)# dhcpv4-snooping external-storage volume dhcp_snoop file dsnoop_ipbindings
```

Disabling external storage:

```
switch(config)# no dhcpv4-snooping external-storage volume dhcp_snoop
```
Disabling external storage when flash storage is also configured (note the message indicating that flash storage will be used):

```
switch(config)# no dhcpv4-snooping external-storage volume dhcp_snoop
DHCPv4-Snooping will use flash storage to store IP Binding database
switch(config)#
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Added flash storage information.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td></td>
</tr>
</tbody>
</table>

**dhcppv4-snooping flash-storage**

```
dhcppv4-snooping flash-storage [delay <DELAY>]
no dhcppv4-snooping flash-storage [delay <DELAY>]
```

**Description**

Configures switch flash storage to be used for backing up client IP bindings (used by DHCPv4 snooping). When flash storage is configured (and external storage is not already configured for this purpose), the switch stores the IP bindings in switch flash storage. When the switch restarts, it reads the IP bindings from the switch flash storage to populate its local cache. Writing the IP bindings to flash storage only occurs after the configured delay and if there has been a change in client IP bindings. Writing is skipped when client IP bindings have not changed since the previous write. Omitting `delay <DELAY>` sets the default delay of 900 seconds.

To reduce switch flash aging it is recommended that you use external storage (command `dhcppv4-snooping external-storage`) to backup DHCP snooping IP bindings. Alternatively, consider configuring flash storage with a substantial delay between writes.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IP bindings in flash storage.
### Examples

Configuring switch flash storage for DHCP snooping IP binding storage with a write delay of 1200 seconds:

```
switch(config)# dhcpv4-snooping flash-storage delay 1200
Warning: Using flash storage reduces switch lifetime. It is recommended to use an external-storage.
Do you want to continue (y/n)? y
switch(config)#
```

Unconfiguring usage of switch flash storage for IP bindings:

```
switch(config)# no dhcpv4-snooping flash-storage
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td><code>config</code></td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### dhcpv4-snooping max-bindings

```
dhcpv4-snooping max-bindings <MAX-BINDINGS>
no dhcpv4-snooping max-bindings <MAX-BINDINGS>
```

### Description

Sets the maximum number of DHCP bindings allowed on the selected interface. For all interfaces on which this command is not run, the default max bindings applies.

The no form of the command reverts max bindings for the selected interface to its default.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAX-BINDINGS&gt;</code></td>
<td>Specifies the maximum number of DHCP bindings. You can use the <code>show capacities</code> command to see the maximum available for your switch model.</td>
</tr>
</tbody>
</table>

### Examples

*On the 6400 Switch Series, interface identification differs.*

Set the DHCP max bindings to 512 on interface 2/2/1:
```
switch(config)# interface 2/2/1
switch(config-if)# dhcpv4-snooping max-bindings 512
switch(config-if)# exit
switch(config)#
```

Revert DHCP max bindings to its default on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no dhcpv4-snooping max-bindings 512
switch(config-if)# exit
switch(config)#
```

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

## Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

### dhcpv4-snooping option 82

```
dhcpv4-snooping option 82 [remote-id {mac | subnet-ip | mgmt-ip}]
  [untrusted-policy {drop | keep | replace}]
no dhcpv4-snooping option 82 [remote-id {mac | subnet-ip | mgmt-ip}]
  [untrusted-policy {drop | keep | replace}]
```

## Description

Configures the addition of option 82 DHCP relay information to DHCP client packets that are being forwarded on trusted ports. DHCP relay is enabled by default.

In the switch default state and when this command is entered without parameters (`dhcpv4-snooping option 82`), this default configuration is used:

```
dhcpv4-snooping option 82 remote-id mac untrusted-policy drop
```

When `remote-id` is omitted, its default (`mac`) is used. When `untrusted-policy` is omitted, its default (`drop`) is used.

The no form of this command disables DHCPv4 snooping option 82.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote-id</td>
<td>Specifies what address to use as the remote ID for the <code>replace</code> option of <code>untrusted-policy</code>. Specify one of these address types:</td>
</tr>
<tr>
<td>mac</td>
<td>The default. Uses the switch MAC address as the remote ID.</td>
</tr>
<tr>
<td>subnet-ip</td>
<td>Uses the IP address of the client VLAN as the remote ID.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mgmt-ip</td>
<td>Uses the management interface IP address as the remote ID.</td>
</tr>
<tr>
<td>untrusted-policy</td>
<td>Specifies what action to take for DHCP packets (with option 82) that are received on untrusted ports. Specify one of these actions:</td>
</tr>
<tr>
<td>drop</td>
<td>The default. Drop DHCP packets (with option 82) without forwarding them.</td>
</tr>
<tr>
<td>keep</td>
<td>Forward DHCP packets (with option 82).</td>
</tr>
<tr>
<td>replace</td>
<td>Replace the option 82 information in the DHCP packets with whatever is set for remote-id (one of: mac, subnet-ip, or mgmt-ip) and forward the packets.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring DHCPv4 snooping option 82 with the keep action:

```bash
switch(config)# dhcpv4-snooping option 82 untrusted-policy keep
```

Configuring DHCPv4 snooping option 82 with mgmt-ip as the remote-id and the replace action:

```bash
switch(config)# dhcpv4-snooping option 82 remote-id mgmt-ip untrusted-policy replace
```

Disabling DHCPv4 snooping option 82:

```bash
switch(config)# no dhcpv4-snooping option 82 untrusted-policy keep
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dhcpv4-snooping trust**

```bash
dhcpv4-snooping trust
no dhcpv4-snooping trust
```

**Description**

Enables DHCPv4 snooping trust on the selected port. Only server packets received on trusted ports are forwarded. All the ports are untrusted by default.
The no form of the command disables DHCPv4 snooping trust on the selected port.

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Enabling DHCPv4 snooping trust on interface 2/2/1:

```bash
switch(config)# interface 2/2/1
switch(config-if)# dhcpv4-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling DHCPv4 snooping trust on interface 2/2/1:

```bash
switch(config)# interface 2/2/1
switch(config-if)# no dhcpv4-snooping trust
switch(config-if)# exit
switch(config)#
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300, 6400</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dhcpv4-snooping verify mac**

dhcpv4-snooping verify mac
no dhcpv4-snooping verify mac

**Description**

This command enables verification of the hardware address field in DHCP client packets. When enabled, the DHCP client hardware address field and the source MAC address must be the same for packets received on untrusted ports or else the packet is dropped. This DHCP snooping MAC verification is enabled by default. The no form of the command disables DHCPv4 snooping MAC verification.

**Examples**

Enabling DHCPv4 snooping MAC verification:

```
switch(config)# dhcpv4-snooping verify mac
```

Disabling DHCPv4 snooping MAC verification:
switch(config)# no dhcpv4-snooping verify mac

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show dhcpv4-snooping

show dhcpv4-snooping [vsx-peer]

Description

Shows the DHCPv4 snooping configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

Examples

On the 6400 Switch Series, interface identification differs.

Showing the DHCPv4 snooping configuration:

```
switch(config)# show dhcpv4-snooping

DHCPv4-Snooping Information

DHCPv4-Snooping : Yes          Verify MAC Address : Yes
Allow Overwrite Binding : Yes   Enabled VLANs : 1,5,7,100-110

Option 82 Configurations

Untrusted Policy : replace   Insertion : Yes
Option 82 Remote-id : mac

External Storage Information

Volume Name : ipbinding
File Name : ipv4Bindings
Inactive Since : 01:23:20 09/10/2021
Error : File Write Failure
```
Flash Storage Information

File Write Delay : 300 seconds
Active Storage : External

Authorized Server Configurations

<table>
<thead>
<tr>
<th>VRF</th>
<th>Authorized Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>1.1.10.3</td>
</tr>
<tr>
<td>default</td>
<td>10.10.10.1</td>
</tr>
<tr>
<td>default</td>
<td>10.10.10.56</td>
</tr>
<tr>
<td>default</td>
<td>200.10.10.3</td>
</tr>
<tr>
<td>green</td>
<td>1.1.10.3</td>
</tr>
<tr>
<td>green</td>
<td>1.10.10.3</td>
</tr>
<tr>
<td>green</td>
<td>10.10.100.3</td>
</tr>
<tr>
<td>red</td>
<td>192.168.122.53</td>
</tr>
<tr>
<td>red</td>
<td>192.168.122.121</td>
</tr>
</tbody>
</table>

Port Information

<table>
<thead>
<tr>
<th>Port</th>
<th>Trust</th>
<th>Max Bindings</th>
<th>Static Bindings</th>
<th>Dynamic Bindings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>Yes</td>
<td>5000</td>
<td>50</td>
<td>0</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Yes</td>
<td>8192</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Yes</td>
<td>8192</td>
<td>0</td>
<td>22</td>
</tr>
<tr>
<td>1/1/16</td>
<td>No</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10/10/10</td>
<td>No</td>
<td>8100</td>
<td>320</td>
<td>200</td>
</tr>
<tr>
<td>lag120</td>
<td>No</td>
<td>512</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

VLAN Information

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Guard</th>
<th>Bind</th>
<th>Guard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>POL1</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>5</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>POL2</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Updated example with flash storage information.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;) or Manager (+)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**show dhcpv4-snooping binding**

**show dhcpv4-snooping binding [vsx-peer]**

**Description**

Shows the DHCPv4 snooping binding configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Showing the DHCPv4 snooping binding configuration:

```
switch(config)# show dhcpv4-snooping binding
```

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MacAddress</td>
<td>IP</td>
<td>VLAN</td>
<td>Interface</td>
<td>Time-Left</td>
</tr>
<tr>
<td>aa:b1:c1:dd:ee:ff</td>
<td>10.2.3.4</td>
<td>1</td>
<td>1/1/2</td>
<td>582</td>
</tr>
<tr>
<td>aa:b2:c2:dd:ee:ff</td>
<td>10.2.3.5</td>
<td>1</td>
<td>1/1/2</td>
<td>584</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show dhcpv4-snooping statistics**

**show dhcpv4-snooping statistics [vsx-peer]**

**Description**

Shows the DHCPv4 snooping statistics.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>switch switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

Showing the DHCPv4 snooping statistics:

```
switch(config)# show dhcpv4-snooping statistics
```

<table>
<thead>
<tr>
<th>Packet-Type</th>
<th>Action</th>
<th>Reason</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>forward</td>
<td>from trusted port</td>
<td>5425</td>
</tr>
<tr>
<td>client</td>
<td>forward</td>
<td>to trusted port</td>
<td>3895</td>
</tr>
<tr>
<td>server</td>
<td>drop</td>
<td>received on untrusted port</td>
<td>117</td>
</tr>
<tr>
<td>server</td>
<td>drop</td>
<td>unauthorized server</td>
<td>214</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>destination on untrusted port</td>
<td>78</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>untrusted option 82 field</td>
<td>85</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>bad DHCP release request</td>
<td>0</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>failed verify MAC check</td>
<td>5</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>failed on max-binding limit</td>
<td>15</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;), Manager ( # )</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DHCPv6 snooping commands**

**clear dhcpv6-snooping binding**

clear dhcpv6-snooping binding {all | ip <IPV6-ADDR> vlan <VLAN-ID> | interface <IFNAME> | vlan <VLAN-ID>}

**Description**

Clears DHCPv6 snooping binding entries.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies that all DHCPv6 binding information is to be cleared.</td>
</tr>
<tr>
<td>ip &lt;IPV6-ADDR&gt; vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the IPv6 address and VLAN for which all DHCPv6 binding information is to be cleared.</td>
</tr>
<tr>
<td>interface &lt;IFNAME&gt;</td>
<td>Specifies the interface for which all DHCPv6 binding information is to be cleared.</td>
</tr>
<tr>
<td>vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the VLAN for which all DHCPv6 binding information is to be cleared. Range: 1 to 4094.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Clearing all DHCPv6 binding information for 5000::1 vlan 1:

```
switch(config)# clear dhcpv6-snooping binding ip 5000::1 vlan 1
```

Clearing all DHCPv6 binding information for interface 1/1/10:

```
switch(config)# clear dhcpv6-snooping binding interface 1/1/10
```

Clearing all DHCPv6 binding information for VLAN 10:

```
switch(config)# clear dhcpv6-snooping binding vlan 10
```

Clearing all DHCPv6 binding information:

```
switch(config)# clear dhcpv6-snooping binding all
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;) or Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**clear dhcpv6-snooping statistics**

*clear dhcpv6-snooping statistics*

**Description**
Clears all DHCPv6 snooping statistics.

**Examples**
Clear all DHCPv6 snooping statistics:

```
switch# clear dhcpv6-snooping statistics
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dhcpv6-snooping**

dhcpv6-snooping

no dhcpv6-snooping

**Description**
Enables DHCPv6 snooping. DHCPv6 snooping is disabled by default. DHCPv6 snooping is not supported on the management interface.

The no form of the command disables DHCPv6 snooping, flushing all the IP bindings learned since DHCPv6 snooping was enabled.

**Examples**
Enabling DHCPv6 snooping:

```
switch(config)# dhcpv6-snooping
```

Disabling DHCPv6 snooping:

```
switch(config)# no dhcpv6-snooping
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**
**Platforms** | **Command context** | **Authority**
---|---|---
6300 6400 | config | Administrators or local user group members with execution rights for this command.

---

**dhcpv6-snooping (in config-vlan context)**

dhcpv6-snooping
no dhcpv6-snooping

**Description**

Enables DHCPv6 snooping in the config-vlan context. DHCPv6 snooping is disabled by default for all VLANs.

The no form of the command disables DHCPv6 snooping on the specified VLAN, flushing all the IPv6 bindings learned for this VLAN since DHCPv6 snooping was enabled for this VLAN.

**Examples**

Enabling DHCPv6 snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# dhcpv6-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Disabling DHCPv6 snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no dhcpv6-snooping
switch(config-vlan-100)# exit
switch(config)#
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-vlan</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

---

**dhcpv6-snooping authorized-server**

dhcpv6-snooping authorized-server <IPV6-ADDR> [vrf <VRF-NAME>]
no dhcpv6-snooping authorized-server <IPV6-ADDR> [vrf <VRF-NAME>]

**Description**
Adds an authorized (trusted) DHCPv6 server to a list of authorized servers for use by DHCPv6 snooping. This command can be issued multiple times, adding a maximum of 20 authorized servers per VRF. By default, with an empty list of authorized servers, all DHCPv6 servers are considered to be trusted for DHCPv6 snooping purposes.

The `mgmt` VRF cannot be used with this command.

Configure the link local IPv6 address instead of global IPv6 address of the DHCPv6 server as the authorized-server. For example:

```
switch(config)# dhcpv6-snooping authorized-server fe80::2ca4:fa40:d4cd:bc2f
```

The no form of this command deletes the specified DHCPv6 server from the authorized list.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV6-ADDR&gt;</code></td>
<td>Specifies the IPv6 address of the trusted DHCPv6 server.</td>
</tr>
</tbody>
</table>
| vrf `<VRF-NAME>`| Specifies the VRF name. The name can be `default` or a configured VRF instance but it cannot be `mgmt`.

Usage

For authorized server lookup, the VRF is derived from the Switch Virtual Interface (SVI) configured for the incoming VLAN. If the SVI is not configured, the `default` VRF is assumed.

Examples

Adding DHCP servers ABCD:5ACD::2000, and ABCD:5ACD::2010 to the authorized server list:

```
switch(config)# dhcpv6-snooping authorized-server ABCD:5ACD::2000 vrf default
switch(config)# dhcpv6-snooping authorized-server ABCD:5ACD::2010 vrf default
```

Removing DHCP server ABCD:5ACD::2000 from the authorized server list:

```
switch(config)# no dhcpv6-snooping authorized-server ABCD:5ACD::2000 vrf default
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td><code>config</code></td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
**dhcpv6-snooping external-storage**

dhcpv6-snooping external-storage volume <VOL-NAME> file <FILE-NAME>

no dhcpv6-snooping external-storage volume <VOL-NAME> file <FILE-NAME>

**Description**

Configures external storage to be used for backing up IPv6 bindings (used by DHCPv6 snooping) to a file. When configured, the switch stores all the IP bindings in an external storage file so that they are retained after the switch restarts. When the switch restarts, it reads the IPv6 bindings from the configured external storage file to populate its local cache.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IPv6 bindings in an external storage file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volume &lt;VOL-NAME&gt;</td>
<td>Specifies the name of the existing external storage volume where the IPv6 bindings file will be saved. Before running the dhcpv6-snooping external-storage volume command, first create the external storage volume using command external-storage &lt;VOLUME-NAME&gt;. See External storage commands in the Command-Line Interface Guide.</td>
</tr>
<tr>
<td>file &lt;FILE-NAME&gt;</td>
<td>Specifies the file name to use for storing IPv6 bindings. Maximum 255 characters.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring IPv6 bindings storage in file ipv6Bindings on existing volume dhcp_snoop:

```
switch(config)# dhcpv6-snooping external-storage volume dhcp_snoop file ipv6Bindings
```

Disabling external storage:

```
switch(config)# no dhcpv6-snooping external-storage volume dhcp_snoop
```

Disabling external storage when flash storage is also configured (note the message indicating that flash storage will be used):

```
switch(config)# no dhcpv6-snooping external-storage volume dhcp_snoop
DHCPv6-Snooping will use flash storage to store IP Binding database
switch(config)#
```

**Command History**
DHCP snooping

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Added flash storage information.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**dhcpv6-snooping flash-storage**

dhcpv6-snooping flash-storage [delay <DELAY>]
no dhcpv6-snooping flash-storage [delay <DELAY>]

**Description**

Configures switch flash storage to be used for backing up client IP bindings (used by DHCPv6 snooping). When flash storage is configured (and external storage is not already configured for this purpose), the switch stores the IP bindings in switch flash storage. When the switch restarts, it reads the IP bindings from the switch flash storage to populate its local cache.

Writing the IP bindings to flash storage only occurs after the configured delay and if there has been a change in client IP bindings. Writing is skipped when client IP bindings have not changed since the previous write.

Omitting `delay <DELAY>` sets the default delay of 900 seconds.

To reduce switch flash aging it is recommended that you use external storage (command `dhcpv6-snooping external-storage`) to backup DHCP snooping IP bindings. Alternatively, consider configuring flash storage with a substantial delay between writes.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The `no` form of this command disables the saving of IP bindings in flash storage.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay &lt;DELAY&gt;</td>
<td>Specifies the delay in seconds between writes (when necessary) to the flash storage, Default: 900. Range: 300 to 86400.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring switch flash storage for DHCP snooping IP binding storage with a write delay of 1200 seconds:
switch(config)# dhcpv6-snooping flash-storage delay 1200
Warning: Using flash storage reduces switch lifetime. It is recommended to use an external-storage.
Do you want to continue  (y/n)? y
switch(config)#

Unconfiguring usage of switch flash storage for IP bindings:

switch(config)# no dhcpv6-snooping flash-storage

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Command introduced.</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dhcpv6-snooping max-bindings**

dhcpv6-snooping max-bindings <MAX-BINDINGS>
no dhcpv6-snooping max-bindings <MAX-BINDINGS>

**Description**

Sets the maximum number of DHCPv6 bindings allowed on the selected interface. For all interfaces on which this command is not run, the default max bindings applies.

The no form of the command reverts max bindings for the selected interface to its default.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAX-BINDINGS&gt;</td>
<td>Specifies the maximum number of DHCPv6 bindings. You can use the show capacities command to see the maximum available for your switch model.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Set the DHCPv6 max bindings to 256 on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# dhcpv6-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

Revert DHCPv6 max bindings to its default on interface 2/2/1:

```
switch(config)# no dhcpv6-snooping max-bindings
```
switch(config)# interface 2/2/1
switch(config-if)# no dhcpv6-snooping max-bindings 256
switch(config-if)# exit
switch(config)#

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-if</td>
<td></td>
</tr>
</tbody>
</table>

**dhcpv6-snooping trust**

dhcpv6-snooping trust
no dhcpv6-snooping trust

**Description**

Enables DHCPv6 snooping trust on the selected interface. Only server packets received on trusted interfaces are forwarded. All the interfaces are untrusted by default.

The no form of the command disables DHCPv6 snooping trust on the selected interface.
config-if

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Enabling DHCPv6 snooping trust on interface 2/2/1:

```bash
switch(config)# interface 2/2/1
switch(config-if)# dhcpv6-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling DHCPv6 snooping trust on interface 2/2/1:

```bash
switch(config)# interface 2/2/1
switch(config-if)# no dhcpv6-snooping trust
switch(config-if)# exit
switch(config)#
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show dhcpv6-snooping

show dhcpv6-snooping [vsx-peer]

Description

Shows the DHCPv6 snooping configuration.

Parameter | Description
---|---
vsx-peer | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

On the 6400 Switch Series, interface identification differs.

Showing the DHCPv6 snooping configuration:

```
switch(config)# show dhcpv6-snooping

DHCPv6-Snooping Information
DHCPv6-Snooping : Yes   Enabled VLANs : 1,5,7,100-110

External Storage Information
Volume Name       : dhcp_snoop
File Name         : ip_binding
Inactive Since   : 01:23:20 09/10/2021
Error             : Failed to write external storage

Flash Storage Information
File Write Delay : 300 seconds

Active Storage : External

Authorized Server Configurations

<table>
<thead>
<tr>
<th>VRF</th>
<th>Authorized Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>2001:0db8:85a3:0000:0000:8a2e:0370:7334</td>
</tr>
<tr>
<td>default</td>
<td>2002::2</td>
</tr>
<tr>
<td>default</td>
<td>2004::1</td>
</tr>
<tr>
<td>red</td>
<td>2002::1</td>
</tr>
<tr>
<td>red</td>
<td>2002::2</td>
</tr>
<tr>
<td>red</td>
<td>2002::9</td>
</tr>
<tr>
<td>green</td>
<td>5000::1</td>
</tr>
</tbody>
</table>
```
green 5000::2
green 5000::3
green 5000::7
green 5000::8

Port Information

<table>
<thead>
<tr>
<th>Port</th>
<th>Trust</th>
<th>Max Bindings</th>
<th>Static Bindings</th>
<th>Dynamic Bindings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Yes</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Yes</td>
<td>0</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>1/1/16</td>
<td>No</td>
<td>256</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>10/10/10</td>
<td>No</td>
<td>256</td>
<td>12</td>
<td>7</td>
</tr>
<tr>
<td>lag120</td>
<td>No</td>
<td>256</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

VLAN Information

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Guard Policy</th>
<th>Bind Disable</th>
<th>Guard Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>POL1</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>5</td>
<td>False</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>POL2</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Updated example with flash storage information.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show dhcpv6-snooping binding**

**show dhcpv6-snooping binding [vsx-peer]**

Description

Shows the DHCPv6 snooping binding configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not</td>
</tr>
</tbody>
</table>


## Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

### Examples

*On the 6400 Switch Series, interface identification differs.*

Showing the DHCPv6 snooping binding configuration:

```
switch# show dhcpv6-snooping binding

IP Binding Information
-----------------------
MAC-ADDRESS  IPv6-ADDRESS   VLAN INTERFACE TIME-
00:50:56:e4:cf aaaa:bbbb:cccc:dddd:eeee:1234:5678:abcd  1  1/1/1
00:50:56:04:4d 1000::3  134  1/1/2
00:50:56:96:d8:3d 2000:1000::4  2002  lag123
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;) or Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## show dhcpv6-snooping statistics

*show dhcpv6-snooping statistics [vsx-peer]*

### Description

Shows the DHCPv6 snooping statistics.
Examples
Showing the DHCPv6 snooping statistics:

```
switch(config)# show dhcpv6-snooping statistics

<table>
<thead>
<tr>
<th>Packet-Type</th>
<th>Action</th>
<th>Reason</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>forward</td>
<td>from trusted port</td>
<td>12</td>
</tr>
<tr>
<td>client</td>
<td>forward</td>
<td>to trusted port</td>
<td>20</td>
</tr>
<tr>
<td>server</td>
<td>drop</td>
<td>received on untrusted port</td>
<td>5</td>
</tr>
<tr>
<td>server</td>
<td>drop</td>
<td>unauthorized server</td>
<td>4</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>destination on untrusted port</td>
<td>2</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>bad DHCP release request</td>
<td>5</td>
</tr>
<tr>
<td>server</td>
<td>drop</td>
<td>relay reply on untrusted port</td>
<td>2</td>
</tr>
<tr>
<td>client</td>
<td>drop</td>
<td>failed on max-binding limit</td>
<td>5</td>
</tr>
</tbody>
</table>
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Overview

ND (Neighbor Discovery) snooping prevents ND attacks. ND snooping drops invalid ND packets, and together with DIPLDv6 (Dynamic IP Lockdown for IPv6), blocks data traffic from invalid hosts. ND snooping is used in Layer 2 switching networks. ND snooping learns the source MAC addresses, source IPv6 addresses, input interfaces, and VLANs of incoming ND messages and data packets to build IP binding entries.

When DHCPv6 snooping and ND snooping are both enabled, and DHCPv6 clients request an IPv6 address, entries are added to the DHCP snooping table and DHCP snooping takes priority over ND snooping.

ND snooping drops ND packets as follows:

- If the Ethernet source MAC address is mismatched with the address contained in the ICMPv6 Target link layer address field of the ND packet.
- If the global IPv6 address in the source address field is mismatched with the ND snooping prefix filter table.
- If the global IPv6 address or the link-local IPv6 address in the source IP address field is mismatched with the ND snooping binding table.

ND snooping drops RA and RR packets on untrusted ports. To block only RA packets on VLANs with ND snooping enabled, use `nd-snooping ra-drop`. RA (Router Advertisement) drop is disabled by default on VLANs. When enabled (with `nd-snooping ra-drop`), ND snooping blocks RA packets on both trusted and untrusted ports. When RA drop is disabled, ND snooping allows RA packets on trusted ports and blocks them on untrusted ports.

Dynamic IPv6 lockdown is performed for ND snooping entries. Based on the DAD NS received from the hosts by the switch, ND snooping entries are programmed into the IP binding table and the hardware (as allowed). And ND Binding table entries are added when NA packets are received from hosts. Therefore, data packets from invalid hosts and transit traffic are blocked.

ND snooping commands

**clear nd-snooping binding**

clear nd-snooping binding {all | ipv6 <IPV6-ADDR> vlan <VLAN-ID> | port <PORT-NUM> | vlan <VLAN-ID>}

**Description**

Clears ND snooping binding entries.
Command context

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies that all ND binding information is to be cleared.</td>
</tr>
<tr>
<td>ip &lt;IPV6-ADDR&gt; vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the IPv6 address and VLAN for which all ND binding information is to be cleared.</td>
</tr>
<tr>
<td>port &lt;PORT-NUM&gt;</td>
<td>Specifies the port for which all ND binding information is to be cleared.</td>
</tr>
<tr>
<td>vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the VLAN for which all ND binding information is to be cleared. Range: 1 to 4094.</td>
</tr>
</tbody>
</table>

Examples

*On the 6400 Switch Series, interface identification differs.*

Clearing all ND binding information for 5000::1:

```
switch(config)# clear nd-snooping binding ipv6 5000::1
```

Clearing all ND binding information for 5000::1 vlan 1:

```
switch(config)# clear nd-snooping binding ipv6 5000::1 vlan 1
```

Clearing all ND binding information for port 1/1/10:

```
switch(config)# clear nd-snooping binding port 1/1/10
```

Clearing all ND binding information for VLAN 10:

```
switch(config)# clear nd-snooping binding vlan 10
```

Clearing all ND binding information:

```
switch(config)# clear nd-snooping binding all
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
### clear nd-snooping statistics

**Description**
Clears all ND snooping statistics.

**Examples**
Clear all ND snooping statistics:

```
switch# clear nd-snooping statistics
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

### nd-snooping

**nd-snooping {enable|disable}

no nd-snooping {enable|disable}

**Description**
Enables or disables ND snooping. ND snooping is disabled by default. ND snooping is not supported on the management interface.

**Examples**
Enabling ND snooping:

```
switch(config)# nd-snooping enable
```

Disabling ND snooping:

```
switch(config)# nd-snooping disable
```
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**nd-snooping (in config-vlan context)**

```
nd-snooping
no nd-snooping
```

**Description**

Enables ND snooping in the `config-vlan` context. ND snooping is disabled by default for all VLANs. The `no` form of the command disables ND snooping on the specified VLAN, flushing all the IPv6 bindings learned for this VLAN since ND snooping was enabled for this VLAN.

**Examples**

Enabling ND snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# nd-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Disabling ND snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no nd-snooping
switch(config-vlan-100)# exit
switch(config)#
```
**nd-snooping mac-check**

*nd-snooping mac-check*

*no nd-snooping mac-check*

**Description**

This command enables verification of the hardware address field in ND snooping packets. When enabled, the ICMPv6 target link layer address field and the source MAC address must be the same for packets received on untrusted ports or else the packets are dropped. This ND snooping MAC verification is enabled by default.

The no form of the command disables ND snooping MAC verification.

**Examples**

Enabling ND snooping MAC verification:

```
switch(config)# nd-snooping mac-check
```

Disabling ND snooping MAC verification:

```
switch(config)# no nd-snooping mac-check
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**nd-snooping prefix-list**

*nd-snooping prefix-list <IPV6-ADDR>*

*no nd-snooping prefix-list <IPV6-ADDR>*

**Description**

Configures the ND snooping prefix list for the selected VLAN and the specified IPv6 address prefix. ND snooping must be enabled both globally and on this VLAN before this prefix list configuration takes effect.

The no form of this command removes the prefix list configuration for the selected VLAN and IPv6 address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the IPv6 address.</td>
</tr>
</tbody>
</table>

**Examples**

Configuring ND snooping prefix-list on VLAN 1:
Remove configuration of ND snooping prefix-list on VLAN 100:

```plaintext
switch(config)# vlan 1
switch(config-vlan-1)# no nd-snooping prefix-list 2001::1/64
switch(config-vlan-1)# exit
switch(config)#
```

**nd-snooping max-bindings**

`nd-snooping max-bindings <MAX-BINDINGS>`

`no nd-snooping max-bindings`

**Description**

Sets the maximum number of ND bindings allowed on the selected interface. For all interfaces on which this command is not run, the default max bindings applies.

The no form of the command reverts max bindings for the selected interface to its default.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAX-BINDINGS&gt;</code></td>
<td>Specifies the maximum number of ND bindings. You can use the show capacities command to see the maximum available for your switch model.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Set the ND max bindings to 768 on interface 2/2/1:

```plaintext
switch(config)# interface 2/2/1
switch(config-if)# nd-snooping max-bindings 768
switch(config-if)# exit
switch(config)#
```
Revert ND max bindings to its default on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no nd-snooping max-bindings
switch(config-if)# exit
switch(config)#
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

nd-snooping nd-guard

```
nd-snooping nd-guard
no nd-snooping nd-guard
```

Description

This command enables ND guard on the selected VLAN.
The no form of the command disables ND guard and deletes all the IPv6 bindings learned on the VLAN.

ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

Examples

Enabling ND snooping ND guard on VLAN 100:

```
switch(config)# nd-snooping enable
switch(config)# vlan 100
switch(config-vlan-100)# nd-snooping nd-guard
switch(config-vlan-100)# exit
switch(config)#
```

Disabling ND snooping ND guard on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no nd-snooping nd-guard
switch(config-vlan-100)# exit
switch(config)#
```
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-vlan</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**nd-snooping ra-guard**

*nd-snooping ra-guard [log]*  
*no nd-snooping ra-guard*

**Description**

This command enables Routing Advertisement (RA) guard on the selected VLAN. When enabled, ingress Routing Advertisement (RA) and Routing Redirect (RR) packets on the selected VLAN are blocked on untrusted ports. The packets are forwarded when received on trusted ports.

The no form of the command disables RA guard on the VLAN.

ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

**Parameter** | **Description**
---|---
[log] | Logs messages along with drop functionality.

**Examples**

Enabling ND snooping RA guard on VLAN 100:

```plaintext
switch(config)# nd-snooping enable
switch(config)# vlan 100
switch(config-vlan-100)# nd-snooping ra-guard
switch(config-vlan-100)# exit
switch(config)#
```

Enabling ND snooping RA guard on VLAN 100 with event logging on dropped packets:

```plaintext
switch(config)# nd-snooping enable
switch(config)# vlan 100
switch(config-vlan-100)# nd-snooping ra-guard log
switch(config-vlan-100)# exit
switch(config)#
```

Disabling ND snooping RA guard on VLAN 100:
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-vlan-&lt;VLAN-ID&gt;</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**nd-snooping ra-drop**

*nd-snooping ra-drop*

*no nd-snooping ra-drop*

**Description**

This command enables Routing Advertisement (RA) drop on the selected VLAN. When enabled, ingress RA packets on the selected VLAN are blocked on both trusted and untrusted ports. When disabled, RA packets are forwarded on the selected VLAN with ND snooping trusted port validation. RA drop is disabled by default.

ND snooping must be enabled in both the config context and the config-vlan context before this command can be used.

The no form of the command disables ND snooping RA drop on the selected VLAN.

**Examples**

Enabling ND snooping RA drop on VLAN 100:

```
switch(config)# nd-snooping enable vlan 100
switch(config-vlan-100)# nd-snooping ra-drop
switch(config-vlan-100)# exit
switch(config)#
```

Disabling ND snooping RA drop on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no nd-snooping ra-drop
switch(config-vlan-100)# exit
switch(config)#
```
### nd-snooping trust

**nd-snooping trust**

**no nd-snooping trust**

#### Description

Enables ND snooping trust on the selected interface (port). Only server packets received on trusted ports are forwarded. All the ports are untrusted by default.

The no form of the command disables ND snooping trust on the selected port.

#### Examples

*On the 6400 Switch Series, interface identification differs.*

Enabling ND snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# nd-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling ND snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no nd-snooping trust
switch(config-if)# exit
switch(config)#
```

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config-vlan-&lt;VLAN-ID&gt;</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
show nd-snooping

show nd-snooping [vlan <VLAN-ID>] [vsx-peer]

Description

Shows either all ND snooping configuration or the configuration for the specified VLAN.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the VLAN for which the ND configuration is to be shown. Range: 1 to 4094.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

Examples

On the 6400 Switch Series, interface identification differs.

Showing all ND snooping configuration:

```plaintext
switch(config)# show nd-snooping
ND Snooping Information
---------------------------
 ND Snooping               : Enabled
 ND Snooping Enabled VLANs : 1
 RA Drop Enabled VLANs    : 2-3
 MAC Address Check        : Disabled

 PORT   TRUST MAX-BINDINGS CURRENT-BINDINGS
-------- ------ ------------- -------------
 1/1/1   Yes   -             -             
 1/1/2   Yes   -             -             
 1/1/3   No    100           10            
 1/1/4   No    200           10            
 1/1/5   No    300           10            
```

Showing ND snooping configuration for VLAN 2:

```plaintext
switch(config)# show nd-snooping vlan 2
ND Snooping Information
---------------------------
 ND Snooping               : Enabled
 MAC Address Check        : Enabled
 RA Drop                  : Disabled

 PORT   TRUST MAX-BINDINGS CURRENT-BINDINGS
-------- ------ ------------- -------------
 1/1/1   Yes   -             -             
 1/1/2   Yes   -             -             
 1/1/3   No    100           10            
```
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show nd-snooping binding**

**show nd-snooping binding [vsx-peer]**

**Description**

Shows the ND snooping binding configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

On the 6400 Switch Series, interface identification differs.

Showing the ND snooping binding configuration:

```
switch# show nd-snooping binding

<table>
<thead>
<tr>
<th>PORT</th>
<th>IPV6-ADDRESS</th>
<th>MAC-ADDRESS</th>
<th>VLAN</th>
<th>TIME-LEFT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>2001::1</td>
<td>00:00:0A:01:02:03</td>
<td>1</td>
<td>600</td>
</tr>
<tr>
<td>Valid</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/2</td>
<td>fe80::250:56ff:fe9a:143c</td>
<td>00:00:0B:01:02:03</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>Tentative</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/3</td>
<td>2001:111:2222:3333:4444:5555:6666:7777</td>
<td>00:00:0C:01:02:03</td>
<td>4094</td>
<td>-</td>
</tr>
</tbody>
</table>

Testing|
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show nd-snooping prefix-list**

*show nd-snooping prefix-list [vsx-peer]*

**Description**

Shows the ND snooping prefix list information.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

Showing the ND snooping prefix list information:

```
switch# show nd-snooping prefix-list

VLAN IPV6-ADDRESS-PREFIX   SOURCE
----------------------------------
1   2001::/64               Static
4094 3001::/64              Dynamic
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show nd-snooping statistics**

*show nd-snooping statistics [vsx-peer]*

**Description**
Shows the global ND snooping statistics.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

Showing the global ND snooping statistics:

```
switch(config)# show nd-snooping statistics
```

<table>
<thead>
<tr>
<th>PACKET-TYPE</th>
<th>ACTION</th>
<th>REASON</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA</td>
<td>forward</td>
<td>RA packets received on trusted port</td>
<td>20</td>
</tr>
<tr>
<td>RA</td>
<td>drop</td>
<td>RA packets received on untrusted port</td>
<td>45</td>
</tr>
<tr>
<td>NS</td>
<td>forward</td>
<td>NS packets received on trusted port</td>
<td>52</td>
</tr>
<tr>
<td>NS</td>
<td>forward</td>
<td>NS packets received on untrusted port</td>
<td>95</td>
</tr>
<tr>
<td>NS</td>
<td>drop</td>
<td>NS packets failed MAC check</td>
<td>14</td>
</tr>
<tr>
<td>NS</td>
<td>drop</td>
<td>NS packets failed Prefix check</td>
<td>12</td>
</tr>
<tr>
<td>NS</td>
<td>drop</td>
<td>NS packets failed on max-binding limit</td>
<td>0</td>
</tr>
<tr>
<td>NS</td>
<td>drop</td>
<td>NS packets failed ND snooping validation checks</td>
<td>20</td>
</tr>
<tr>
<td>NA</td>
<td>forward</td>
<td>NA packets received on trusted port</td>
<td>17</td>
</tr>
<tr>
<td>NA</td>
<td>forward</td>
<td>NA packets received on untrusted port</td>
<td>30</td>
</tr>
<tr>
<td>NA</td>
<td>drop</td>
<td>NA packets failed Prefix check</td>
<td>15</td>
</tr>
<tr>
<td>NA</td>
<td>drop</td>
<td>NA packets failed on max-binding limit</td>
<td>2</td>
</tr>
<tr>
<td>NA</td>
<td>drop</td>
<td>NA packets failed ND snooping validation checks</td>
<td>5</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
True point-to-point networks are not always possible in corporate networking environment. Many networks deploy nontraditional methods of connection (for example, DSL or broadband) at remote sites or branch offices. The branch office, telecommuter, or business traveler then becomes separated from the corporate network. Some method of tunneling becomes imperative to connect all the network sites together.

Virtual Private Networking (VPN) is often deployed to create private tunnels through the public network system for passing data to remote sites. While VPN is sufficient for the average business traveler, it is not a good solution for branch site connectivity. VPN configurations must include statically maintained access lists to identify traffic through the tunnel. These access lists are often tedious to configure for larger networks and are prone to errors.

VPNs do not permit multicast traffic to pass; therefore routing protocols such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) are no longer options for dynamic routing updates. All new additions to the network topology must be manually added to the various configured access lists. Without dynamic routing from one site to another, network management is severely hampered. Network managers need their non-heterogeneous networks to function like traditional point-to-point networks so that traditional management methods (once available only on point-to-point circuits) can apply to the entire network.

The solution to these challenges is to use IP tunnels. An IP tunnel provides a virtual link between endpoints on two different networks enabling data to be exchanged as if the endpoints were directly connected on the same network. Traffic between the devices is isolated from the intervening networks that the tunnel spans. For example, the following diagram shows an IP tunnel (using GRE) that connects two IPv4 networks over an IPv4 network.

If network 1 and network 3 are using IPv6 addressing, the tunnel connects them by encapsulating the IPv6 traffic in IPv4 packets to traverse network 2. The intermediate network devices do not know about Network 1 and Network 2 because the packets are encapsulated. An IP tunnel can also be used to create a point-to-point link for IPv6 traffic over an IPv6 network.

**IP tunnels supported features**

- Up to 127 tunnels can be defined on a switch shared between different tunnel types.

**Unsupported features**

- GRE IPv4 over IPv6.
- QoS cannot be applied to a GRE tunnel interface.
- Key support can be added for security and identification purposes when there are multiple applications.
- VPN across public IP network.
- MPLS over GRE.
- Multipoint GRE for scalable network to reach multiple remote sites.

## Configuring an IP tunnel

### Prerequisites
An enabled layer 3 interface with an IP address assigned to it, created with the command `interface`.

### Procedure
1. Create an IP tunnel with the command `interface tunnel`.
2. Set the IP address for the tunnel. For a GRE tunnel, enter the command `ip address`. For an IPv6 in IPv4 or an IPv6 in IPv6 tunnel, enter the command `ipv6 address`.
3. Set the source IP address for the tunnel. For a GRE or an IPv6 in IPv4 tunnel, enter the command `source ip`. For an IPv6 in IPv6 tunnel, enter the command `source ipv6`.
4. Set the destination IP address for the tunnel. For a GRE or an IPv6 in IPv4 tunnel, enter the command `destination ip`. For an IPv6 in IPv6 tunnel, enter the command `destination ipv6`.
5. Optionally, set the TTL (hop count) for the tunnel with the command `ttl`.
6. Optionally, set the MTU for the tunnel with the command `ip mtu`.
7. Optionally, add a description to the tunnel with the command `description`.
8. By default, the tunnel is attached to the default VRF. Attach it to a different VRF with the command `vrf attach`.
9. Enable the tunnel with the command `no shutdown`.
10. Review tunnel settings with the command `show interface tunnel`.

### Example
This example creates the following configuration:

- Creates GRE tunnel 33.
- Set the tunnel IP address to 10.10.209/24.
- Sets the tunnel source IP address to 10.10.10.1.
- Sets the tunnel destination IP address to 10.10.10.2.
- Enables the tunnel.

```bash
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ip address 10.10.209/24
switch(config-gre-if)# source ip address 10.10.10.1
switch(config-gre-if)# destination ip address 10.10.10.2
switch(config-gre-if)# no shutdown
```

### Creating a GRE tunnel for traversing a public network
This example creates a GRE tunnel between two switches, enabling traffic from two networks to traverse a public network.
On the 6400 Switch Series, interface identification differs.

Procedure

1. On switch 1:
   a. Enable interface 1/1/1 and assign the IP address 10.1.1.1/24 to it.
      ```
      switch# config
      switch(config)# interface 1/1/1
      switch(config-if)# routing
      switch(config-if)# ip address 10.1.1.1/24
      switch(config-if)# no shutdown
      ```
   b. Enable interface 1/1/2 and assign the IP address 180.1.10.2/24 to it.
      ```
      switch# config
      switch(config)# interface 1/1/2
      switch(config-if)# routing
      switch(config-if)# ip address 180.1.10.2/24
      switch(config-if)# no shutdown
      ```
   c. Create GRE tunnel 10 and assign the IP address 192.168.10.1/24, source address 10.1.1.1, and destination address 20.1.1.1 to it.
      ```
      switch(config)# interface tunnel 10 mode gre ipv4
      switch(config-gre-if)# ip address 192.168.10.1/24
      switch(config-gre-if)# source ip 10.1.1.1
      switch(config-gre-if)# destination ip 20.1.1.1
      switch(config-gre-if)# no shutdown
      ```
   d. Defines routes so that traffic from network 1 can reach network 2 through the tunnel.
      ```
      switch(config)# ip route 20.1.1.0/24 10.1.1.2
      switch(config)# ip route 190.1.10.0/24 tunnel10
      ```

2. On switch 2:
   a. Enable interface 1/1/1 and assign the IP address 20.1.1.1/24 to it.
      ```
      switch# config
      switch(config)# interface 1/1/1
      switch(config-if)# routing
      switch(config-if)# ip address 20.1.1.1/24
      switch(config-if)# no shutdown
      ```
   b. Enable interface 1/1/2 and assign the IP address 190.1.10.2/24 to it.
      ```
      switch(config)# interface 1/1/2
      switch(config-if)# routing
      switch(config-if)# ip address 190.1.10.2/24
c. Create GRE tunnel 10 and assign the IP address 192.168.10.2/24, source address 20.1.1.1, and destination address 10.1.1.1 to it.

switch(config-if)# interface tunnel 10 mode gre ipv4
switch(config-gre-if)# ip address 192.168.10.2/24
switch(config-gre-if)# source ip 20.1.1.1
switch(config-gre-if)# destination ip 10.1.1.1
switch(config-gre-if)# no shutdown
switch(config-gre-if)# exit

d. Defines routes so that traffic from network 2 can reach network 1 through the tunnel.

switch(config)# ip route 10.1.1.0/24 20.1.1.2
switch(config)# ip route 180.1.10.0/24 tunnel10

Creating two GRE tunnels to different destination addresses

This example creates two GRE tunnels to different destination addresses. Traffic from network 1 can reach either network 2 or network 3 using the appropriate tunnel.

On the 6400 Switch Series, interface identification differs.

Procedure
1. On switch 1:
   a. Enable interface 1/1/1 and assign the IP address 10.1.1.1/24 to it.
      ```
      switch# config
      switch(config)# interface 1/1/1
      switch(config-if)# routing
      switch(config-if)# ip address 10.1.1.1/24
      switch(config-if)# no shutdown
      ```
   b. Enable interface 1/1/2 and assign the IP address 180.1.10.2/24 to it.
      ```
      switch# config
      switch(config)# interface 1/1/2
      switch(config-if)# routing
      switch(config-if)# ip address 180.1.10.2/24
      switch(config-if)# no shutdown
      ```
   c. Enable interface 1/1/3 and assign the IP address 30.1.1.1/24 to it.
      ```
      switch# config
      switch(config)# interface 1/1/3
      switch(config-if)# routing
      switch(config-if)# ip address 30.1.1.1/24
      switch(config-if)# no shutdown
      ```
   d. Create GRE tunnel 10 and assign the IP address 192.168.10.1/24, source address 10.1.1.1, and destination address 20.1.1.1 to it.
      ```
      switch(config)# interface tunnel 10 mode gre ipv4
      switch(config-gre-if)# ip address 192.168.10.1/24
      switch(config-gre-if)# source ip 10.1.1.1
      switch(config-gre-if)# destination ip 20.1.1.1
      switch(config-gre-if)# no shutdown
      ```
   e. Create GRE tunnel 20 and assign the IP address 192.168.20.1/24, source address 30.1.1.1, and destination address 40.1.1.1 to it.
      ```
      switch(config)# interface tunnel 20 mode gre ipv4
      switch(config-gre-if)# ip address 192.168.20.1/24
      switch(config-gre-if)# source ip 30.1.1.1
      switch(config-gre-if)# destination ip 40.1.1.1
      switch(config-gre-if)# no shutdown
      ```
   f. Defines routes so that traffic from network 1 can reach network 2 through tunnel 10.
      ```
      switch(config)# ip route 20.1.1.0/24 10.1.1.2
      ```
   g. Defines routes so that traffic from network 1 can reach network 3 through the tunnel 20.
      ```
      switch(config)# ip route 40.1.1.0/24 30.1.1.2
      ```

2. On switch 2:
   a. Enable interface 1/1/1 and assign the IP address 20.1.1.1/24 to it.
      ```
      switch# config
      switch(config)# interface 1/1/1
      switch(config-if)# routing
      switch(config-if)# ip address 20.1.1.1/24
      switch(config-if)# no shutdown
      ```
   b. Enable interface 1/1/2 and assign the IP address 190.1.10.2/24 to it.
      ```
      switch(config)# interface 1/1/2
      switch(config-if)# routing
      switch(config-if)# ip address 190.1.10.2/24
      switch(config-if)# no shutdown
      ```
c. Create GRE tunnel 10 and assign the IP address 192.168.10.2/24, source address 20.1.1.1, and destination address 10.1.1.1 to it.
   switch(config)# interface tunnel 10 mode gre ipv4
   switch(config-gre-if)# ip address 192.168.10.2/24
   switch(config-gre-if)# source ip 20.1.1.1
   switch(config-gre-if)# destination ip 10.1.1.1
   switch(config-gre-if)# no shutdown
   switch(config-gre-if)# exit

d. Defines routes so that traffic from network 2 can reach network 1 through tunnel 10.
   switch(config)# ip route 10.1.1.0/24 20.1.1.2
   switch(config)# ip route 180.1.10.0/24 tunnel10

3. On switch 3:
   a. Enable interface 1/1/1 and assign the IP address 40.1.1.1/24 to it.
      switch# config
      switch(config)# interface 1/1/1
      switch(config-if)# routing
      switch(config-if)# ip address 40.1.1.1/24
      switch(config-if)# no shutdown

   b. Enable interface 1/1/2 and assign the IP address 200.1.10.2/24 to it.
      switch(config)# interface 1/1/2
      switch(config-if)# routing
      switch(config-if)# ip address 200.1.10.2/24
      switch(config-if)# no shutdown
      switch(config-if)# exit

   c. Create GRE tunnel 20 and assign the IP address 192.168.20.2/24, source address 40.1.1.1, and destination address 30.1.1.1 to it.
      switch(config)# interface tunnel 10 mode gre ipv4
      switch(config-gre-if)# ip address 192.168.20.2/24
      switch(config-gre-if)# source ip 40.1.1.1
      switch(config-gre-if)# destination ip 30.1.1.1
      switch(config-gre-if)# no shutdown
      switch(config-gre-if)# exit

   d. Defines routes so that traffic from network 3 can reach network 1 through tunnel 20.
      switch(config)# ip route 30.1.1.0/24 40.1.1.2
      switch(config)# ip route 180.1.10.0/24 tunnel20

Creating an IPv6 in IPv4 tunnel for traversing a public network

This example creates an IPv6 in IPv4 tunnel between two switches, enabling traffic from two networks to traverse a public network.
On the 6400 Switch Series, interface identification differs.

Procedure

1. On switch 1:
   a. Enable interface 1/1/1 and assign the IP address 10.1.1.1/24 to it.
      
      ```
      switch# config
      switch(config)# interface 1/1/1
      switch(config-if)# routing
      switch(config-if)# ip address 10.1.1.1/24
      switch(config-if)# no shutdown
      ```
   b. Enable interface 1/1/2 and assign the IP address 2080::2/64 to it.
      
      ```
      switch# config
      switch(config)# interface 1/1/2
      switch(config-if)# routing
      switch(config-if)# ipv6 address 2080::2/64
      switch(config-if)# no shutdown
      switch(config-if)# exit
      ```
   c. Create IPv6 in IPv4 tunnel 10 and assign the IP address 2001:DB8::1/32, source address 10.1.1.1, and destination address 20.1.1.1 to it.
      
      ```
      switch(config)# interface tunnel 10 mode ip 6in4
      switch(config-ip-if)# ipv6 address 2001:DB8::1/62
      switch(config-ip-if)# source ip 10.1.1.1
      switch(config-ip-if)# destination ip 20.1.1.1
      switch(config-ip-if)# no shutdown
      switch(config-ip-if)# exit
      ```
   d. Defines routes so that traffic from network 1 can reach network 2 through the tunnel.
      
      ```
      switch(config)# ip route 20.1.1.0/24 10.1.1.2
      switch(config)# ipv6 route 290::0/64 tunnel10
      ```

2. On switch 2:
   a. Enable interface 1/1/1 and assign the IP address 20.1.1.1/24 to it.
      
      ```
      switch# config
      switch(config)# interface 1/1/1
      switch(config-if)# routing
      switch(config-if)# ip address 20.1.1.1/24
      switch(config-if)# no shutdown
      ```
   b. Enable interface 1/1/2 and assign the IP address 2090::2/64 to it.
      
      ```
      switch(config)# interface 1/1/2
      switch(config-if)# routing
      switch(config-if)# ipv6 address 2090::2/64
      ```
c. Create IPv6 in IPv4 tunnel 10 and assign the IP address 2001:DB8::2/32, source address 10.1.1.1, and destination address 20.1.1.1 to it.

switch(config)# interface tunnel 10 mode ip 6in4
switch(config-ip-if)# ipv6 address 2001:DB8::2/62
switch(config-ip-if)# source ip 20.1.1.1
switch(config-ip-if)# destination ip 10.1.1.1
switch(config-ip-if)# no shutdown
switch(config-ip-if)# exit

d. Defines routes so that traffic from network 2 can reach network 1 through the tunnel.

switch(config)# ip route 10.1.1.0/24 20.1.1.2
switch(config)# ip route 2080::0/64 tunnel10

Creating an IPv6 in IPv6 tunnel for traversing a public network

This example creates an IPv6 in IPv6 tunnel between two switches, enabling traffic from two networks to traverse a public network.

On the 6400 Switch Series, interface identification differs.

Procedure

1. On switch 1:
   a. Enable interface 1/1/1 and assign the IP address 2001:DB8:5::1/64 to it.

switch# config
switch(config)# interface 1/1/1
switch(config-if)# routing
switch(config-if)# ipv6 address 2001:DB8:5::1/64
switch(config-if)# no shutdown

b. Enable interface 1/1/2 and assign the IP address 2080::2/64 to it.

switch# config
switch(config)# interface 1/1/2
switch(config-if)# routing
switch(config-if)# ipv6 address 2080::2/64
switch(config-if)# no shutdown
switch(config-if)# exit
c. Create IPv6 in IPv6 tunnel 10 and assign the IP address 2001:DB8::1/32, source address 2001:DB8:5::1, and destination address 2001:DB8:9::1 to it. (Optional) Set the MTU and TTL parameters for this tunnel interface.

```
switch(config)# interface tunnel 10 mode ip 6in6
switch(config-ip-if)# ipv6 address 2001:DB8::1/62
switch(config-ip-if)# source ipv6 2001:DB8:5::1
switch(config-ip-if)# destination ipv6 2001:DB8:9::1
switch(config-ip-if)# no shutdown
switch(config-ip-if)# exit
```

d. Defines routes so that traffic from network 1 can reach network 2 through the tunnel.

```
switch(config)# ipv6 route 2001:DB8:9::0/64 2001:DB8:5::2
switch(config)# ipv6 route 2080::0/64 tunnel10
```

2. On switch 2:

a. Enable interface 1/1/1 and assign the IP address 2001:DB8:9::1/64 to it.

```
switch# config
switch(config)# interface 1/1/1
switch(config-if)# routing
switch(config-if)# ipv6 address 2001:DB8:9::1/64
switch(config-if)# no shutdown
```

b. Enable interface 1/1/2 and assign the IP address 2090::2/64 to it.

```
switch(config)# interface 1/1/2
switch(config-if)# routing
switch(config-if)# ipv6 address 2090::2/64
switch(config-if)# no shutdown
switch(config-if)# exit
```

c. Create IPv6 in IPv6 tunnel 10 and assign the IP address 2001:DB8:2/32, source address 2001:DB8:5::1, and destination address 2001:DB8:9::1 to it. (Optional) Set the MTU and TTL parameters for this tunnel interface.

```
switch(config)# interface tunnel 10 mode ip 6in6
switch(config-ip-if)# ipv6 address 2001:DB8:2/62
switch(config-ip-if)# source ipv6 2001:DB8:9::1
switch(config-ip-if)# destination ipv6 2001:DB8:5::1
switch(config-ip-if)# no shutdown
switch(config-ip-if)# exit
```

d. Defines routes so that traffic from network 2 can reach network 1 through the tunnel.

```
switch(config)# ipv6 route 2001:DB8:5::0/64 2001:DB8:9::2
switch(config)# ipv6 route 2080::0/64 tunnel10
```

## IP tunnels commands

### description

```
description <DESC>
no description
```

**Description**

Associates a text description with an IP tunnel for identification purposes. The `no` form of this command removes the description from an IP tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;DESC&gt;</code></td>
<td>Specifies the descriptive text to associate with the IP tunnel. Range: 1 to 64 printable ASCII characters.</td>
</tr>
</tbody>
</table>
**Examples**

Defines a description for GRE tunnel 33.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# description Network A Tunnel C
```

Removes the description for GRE tunnel 33.

```
switch(config)# interface tunnel 33
switch(config-gre-if)# no description
```

Defines a description for IPv6 in IPv4 tunnel 27.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# description Network 3 Tunnel 27
```

Removes the description for IPv6 in IPv4 tunnel 27.

```
switch(config)# interface tunnel 27
switch(config-ip-if)# no description
```

Defines a description for IPv6 in IPv6 tunnel 8.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# description Network 4 Tunnel 8
```

Removes the description for IPv6 in IPv6 tunnel 8.

```
switch(config)# interface tunnel 8
switch(config-ip-if)# no description
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-gre-if</td>
<td></td>
</tr>
<tr>
<td>6300</td>
<td>config-ip-if</td>
<td></td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td></td>
</tr>
</tbody>
</table>

**destination ip**

destination ip <IPV4-ADDR>
no destination ip <IPV4-ADDR>
**Description**
Sets the destination IP address for an IP tunnel. Specify the address of the interface on the remote device to which the tunnel will be established.
The `no` form of this command deletes the destination IP address from an IP tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV4-ADDR&gt;</code></td>
<td>Specifies the destination IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
</tbody>
</table>

**Examples**
Defines the destination IP address to be **10.10.10.1** for GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# destination ip 10.10.10.1
```

Deletes the destination IP address **10.10.10.1** from GRE tunnel **33**.

```
switch(config)# interface tunnel 33
switch(config-gre-if)# no destination ip 10.10.10.1
```

Defines the destination IP address to be **10.10.20.1** for IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# destination ip 10.10.20.1
```

Deletes the destination IP address **10.10.20.1** from IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27
switch(config-ip-if)# no destination ip 10.10.20.1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td></td>
</tr>
</tbody>
</table>

**destination ipv6**

destination ipv6 `<IPV6-ADDR>`
no destination ipv6 `[IPV6-ADDR]`
**Description**
Sets the destination IPv6 address for an IP tunnel. Specify the address of the interface on the remote device to which the tunnel will be established.
The no form of this command deletes the destination IPv6 address from an IP tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the tunnel IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a</td>
</tr>
<tr>
<td></td>
<td>hexadecimal number from 0 to F. This is optional in the no form of the command.</td>
</tr>
</tbody>
</table>

**Examples**
Defines the destination IPv6 address to be 2001:DB8::1 for IPv6 in IPv6 tunnel

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# destination ipv6 2001:DB8::1
```

Deletes the destination IPv6 address 2001:DB8::1 from IPv6 in IPv6 tunnel 8.

```
switch(config)# interface tunnel 8
switch(config-ip-if)# no destination ipv6 2001:DB8::1
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-ip-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**interface tunnel**

```
interface tunnel <TUNNEL-NUMBER> mode {gre ipv4 | ip 6in4 | ip 6in6}
interface tunnel <EXISTING-TUNNEL-NUMBER>
no interface tunnel <EXISTING-TUNNEL-NUMBER> [mode {gre ipv4 | ip 6in4 | ip 6in6}]
```

**Description**
Creates or updates an IP tunnel. After you enter the command, the firmware switches to the configuration context for the tunnel.
If the specified tunnel exists, this command switches to the context for the tunnel.
By default, all tunnels are automatically assigned to the default VRF when they are created.
The no form of this command deletes an existing IP tunnel. It is optional to include a mode in the no form, but if a mode has been entered, selecting a mode is required.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| mode {gre ipv4 | ip 6in4 | ip 6in6} | Creates an IP tunnel. Choose one of the following options:  
  - gre ipv4: Creates a GRE tunnel.  
  - ip 6in4: Creates an IPv4 tunnel for IPv6 traffic.  
  - ip 6in6: Creates an IPv6 tunnel for IPv6 traffic.  
  This is optional in the no form, unless a mode has already been entered. |
| <TUNNEL-NUMBER> | Specifies the number for a new tunnel. Range: 1 to 127.  
Numbering is shared between all tunnels, so the same tunnel number cannot be used for an IPv6 in IPv4 tunnel and a GRE tunnel. |
| <EXISTING-TUNNEL-NUMBER> | Specifies the number for an existing IP tunnel. Range: 1 to 127. |

**Examples**

Defines a new GRE tunnel with number **27**.

```yaml
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)#
```

Switches to the `config-gre-if` context for existing tunnel **33**.

```yaml
switch(config)# interface tunnel 33
switch(config-gre-if)#
```

Deletes GRE tunnel **33**.

```yaml
switch(config)# no interface tunnel 33
```

Defines a new IPv6 in IPv4 tunnel with number **27**.

```yaml
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)#
```

Switches to the `config-ip-if` context for existing tunnel **27**.

```yaml
switch(config)# interface tunnel 27
switch(config-ip-if)#
```

Deletes IPv6 in IPv4 tunnel **27**.

```yaml
switch(config)# no interface tunnel 27
```
Defines a new IPv6 in IPv6 tunnel with number 8.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)#
```

Deletes IPv6 in IPv6 tunnel with number 3.

```
switch(config)# no interface tunnel 33 mode gre ipv4
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td></td>
</tr>
<tr>
<td></td>
<td>config</td>
<td></td>
</tr>
</tbody>
</table>

**ip address**

ip address `<IPV4-ADDR>/MASK>`
no ip address `<IPV4-ADDR>/MASK>`

**Description**

Sets the local IP address of a GRE tunnel. This address identifies the tunnel interface for routing. It must be on the same subnet as the tunnel address assigned on the remote device.

The no form of this command deletes the local IP address assigned to a GRE tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPV4-ADDR&gt;</code></td>
<td>Specifies the tunnel IP address in IPv4 format (<code>x.x.x.x</code>), where <code>x</code> is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100.</td>
</tr>
<tr>
<td><code>&lt;MASK&gt;</code></td>
<td>Specifies the number of bits in the address mask in CIDR format (<code>x</code>), where <code>x</code> is a decimal number from 0 to 32.</td>
</tr>
</tbody>
</table>

**Examples**

Defines the local IP address **10.10.10.1** for GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ip address 10.10.10.1/24
```

Deletes the local IP address **10.10.10.1** for GRE tunnel **33**.
switch(config)# interface tunnel 33
switch(config-gre-if)# no ip address 10.10.10.1/24

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ipv6 address**

ipv6 address <IPV6-ADDR>/<MASK>
no ipv6 address <IPV6-ADDR>/<MASK>

Description

Sets the local IP address of an IPv6 to IPv4 tunnel or of an IPv6 to IPv6 tunnel. This address identifies the tunnel interface for routing. It must be on the same subnet as the tunnel address assigned on the remote device.

The no form of this command deletes the local IP address assigned to an IPv6 to IPv4 tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the tunnel IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td>&lt;MASK&gt;</td>
<td>Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.</td>
</tr>
</tbody>
</table>

Examples

Defines the local IP address **2001:DB8:5::1/64** for tunnel **8** for an IPv6 to IPv6 tunnel.

```plaintext
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# ipv6 address 2001:DB8:5::1/64
```

Deletes the local IP address **2001:DB8::1/32** for tunnel **8**.

```plaintext
switch(config)# interface tunnel 8
switch(config-ip-if)# no ipv6 address 2001:DB8:5::1/64
```

Command History
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300, 6400</td>
<td>config-ip-if, config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip mtu**

*ip mtu <VALUE>*

**Description**

Sets the MTU (maximum transmission unit) for an IP interface. The default value is 1500 bytes. The *no* form of this command sets the MTU to the default value of 1500 bytes.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VALUE&gt;</td>
<td>Specifies the MTU in bytes. Range: 1,280 bytes to 9,192 bytes.</td>
</tr>
</tbody>
</table>

**Usage**

The IP MTU is the largest IP packet that can be sent or received by the interface. For a tunnel, the IP MTU is the maximum size of the IP payload. To enable jumbo packet forwarding through the tunnel, set the IP MTU of the tunnel to a value greater than 1500. Also set the MTU and the IP MTU values for the underlying physical interface that the tunnel is using to a value greater than 1,500 bytes. The IP MTU of the tunnel must also be greater than or equal to the MTU of the ingress interface on the switch. The IP MTU value of the tunnel must also be less than or equal to the IP MT of the underlying interface that the tunnel is using. When defining a GRE tunnel, the MTU has to account for 28 bytes of IP layer overhead, plus a GRE header. It must be larger than the MTU of the interface that the tunnel is using. Packets larger than the MTU are dropped.

**Examples**

Sets the MTU on GRE interface 33 to **1300** bytes.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# mtu 1300
```

Sets the MTU on GRE interface 33 to the default value.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ip mtu
```

Sets the MTU on IPv6 in IPv4 tunnel 27 to **1000** bytes.

```
switch(config)# interface tunnel 27 mode gre ipv6-ipv4
switch(config-gre-if)# ip mtu
```
Sets the MTU on IPv6 in IPv4 tunnel 27 to the default value.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# mtu 1000
```

Sets the MTU on IPv6 in IPv6 tunnel 8 to 900 bytes.

```
switch(config)# interface tunnel 8 mode ip 6in4
switch(config-ip-if)# ip mtu 9000
```

Sets the MTU on IPv6 in IPv6 tunnel 8 to the default value.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# ip mtu
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td></td>
</tr>
</tbody>
</table>

### show interface tunnel

```
show interface tunnel[<TUNNEL-NUMBER>] [vsx-peer]
```

#### Description

Shows configuration settings for all IP tunnels, or a specific tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TUNNEL-NUMBER&gt;</td>
<td>Specifies the number of an IP tunnel. Range: 1 to 127.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

### Examples
Shows configuration settings for tunnel 10, which is a GRE tunnel in the following example.

```
switch# show interface tunnel10
Interface tunnel10 is up
Admin state is up
tunnel type GRE IPv4
tunnel interface IPv4 address 192.0.2.0/24
tunnel source IPv4 address 1.1.1.1
tunnel destination IPv4 address 2.2.2.2
tunnel ttl 60
Statistics
L3 Packets RX TX Total
L3 Bytes 0 0 0
```

Shows configuration settings for tunnel 12, which is an IPv6 in IPv6 tunnel in the following example.

```
switch# show interface tunnel12
Interface tunnel12 is up
Admin state is up
tunnel type IPv6 in IPv6
tunnel interface IPv6 address 4::1/64
tunnel source IPv6 address 2::1
tunnel destination IPv6 address 2::2
tunnel ttl 60
Description: Network2 Tunnel
Statistics
L3 Packets RX TX Total
L3 Bytes 0 0 0
```

Shows configuration settings for all tunnels.

```
switch# show interface tunnel
Interface tunnel10 is up
Admin state is up
tunnel type GRE IPv4
tunnel interface IPv4 address 192.0.2.0/24
tunnel source IPv4 address 1.1.1.1
tunnel destination IPv4 address 2.2.2.2
tunnel ttl 60
Statistics
L3 Packets RX TX Total
L3 Bytes 0 0 0
```

```
Interface tunnel11 is up
Admin state is up
tunnel type IPv6 in IPv4
tunnel source IPv4 address 198.51.100.0
tunnel destination IPv4 address 198.51.200.5
tunnel ttl 80
Description: Network11
```
### Statistics

<table>
<thead>
<tr>
<th></th>
<th>RX</th>
<th>TX</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3 Packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L3 Bytes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Interface tunnel12 is up  
Admin state is up  
tunnel type IPv6 in IPv6  
tunnel interface IPv6 address 4::1/64  
tunnel source IPv6 address 2::1  
tunnel destination IPv6 address 2::2  
tunnel ttl 60  
Description: Network2 Tunnel

<table>
<thead>
<tr>
<th></th>
<th>RX</th>
<th>TX</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3 Packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>L3 Bytes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### show running-config interface tunnel

`show running-config interface tunnel<TUNNEL-NUMBER> [vsx-peer]`

### Description

Shows the commands used to configure an IP tunnel.

### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;TUNNEL-NUMBER&gt;</td>
<td>Specifies the number of an IP tunnel. Range: 1 to 127.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

### Examples

Shows the configuration for a GRE tunnel.
switch# show running-config interface tunnel2
  interface tunnel 2 mode gre ipv4
  source ip 10.10.20.11
  destination ip 10.20.1.2
  ip address 10.10.10.1/24
  ttl 60

Shows the configuration for IPv6 in IPv4 tunnel.

switch# show running-config interface tunnel5
  interface tunnel5 mode ip 6in4
  source ip 10.10.10.12
  destination ip 22.20.20.20
  ip6 address 2001:DB8:5::1/64
  ttl 60
  no shutdown
  description Network10

Shows the configuration for IPv6 in IPv6 tunnel.

switch# show running-config interface tunnel11
  interface tunnel 1 mode ip 6in6
  description Network2 Tunnel
  source ipv6 2::1
  destination ipv6 2::2
  ipv6 address 4::1/64
  ttl 60

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; only).</td>
</tr>
</tbody>
</table>

shutdown

shutdown
no shutdown

Description

This command disables an IP interface. IP interfaces are disabled by default when created.
The no form of this command enables an IP interface.

Examples

Enables GRE interface 33.
Disables GRE interface 33.

switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# no shutdown

Enables IPv6 in IPv4 interface 27.

switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# shutdown

switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# no shutdown

Disables IPv6 in IPv4 interface 27.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td>Administrator or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

source ip

source ip <IPV4-ADDR>
no source ip <IPV4-ADDR>

Description

Sets the source IP address for an IP tunnel. Specify the IP address of a layer 3 interface on the switch. Tunnels can have the same source IP address and different destination IP addresses. The no form of this command deletes the source IP address for an IP tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV4-ADDR&gt;</td>
<td>Specifies the source IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.</td>
</tr>
</tbody>
</table>

Examples

Defines the source IP address to be 10.10.20.1 for GRE tunnel 33.
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# source ip 10.10.20.1

Deletes the source IP address 10.1.20.1 from GRE tunnel 33.

switch(config)# interface tunnel 33
switch(config-gre-if)# no source ip 10.10.20.1

Defines the source IP address to be 10.10.10.1 for IPv6 in IPv4 tunnel 27.

switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# source ip 10.10.10.1

Deletes the source IP address 10.1.10.1 from IPv6 in IPv4 tunnel 27.

switch(config)# interface tunnel 27
switch(config-ip-if)# no source ip 10.10.10.1

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td></td>
</tr>
</tbody>
</table>

**source ipv6**

source ipv6 <IPV6-ADDR>
no source ipv6 [IPV6-ADDR]

**Description**

Sets the source IPv6 address to be used for the encapsulation.
The no form of this command deletes the source IPv6 address for an IP tunnel.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the tunnel IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. This is optional in the no form of the command.</td>
</tr>
</tbody>
</table>

**Examples**

Defines the source IPv6 address to be 2001:DB8::1 for IPv6 in IPv4 tunnel 8.
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# source ipv6 2001:DB8::1

Deletes the source IP address 2001:DB8::1 from IPv6 in IPv6 tunnel 8.

switch(config)# interface tunnel 8
switch(config-ip-if)# no source ipv6 2001:DB8::1

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-ip-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ttl**

ttl  <COUNT>
no ttl

Description

Sets the TTL (time-to-live), also known as the hop count, for tunneled packets. If not configured, the default value of 64 is used for the tunnel. (The hop count of the original packets is not changed.) A maximum of four different TTL values can be used at the same time by all tunnels on the switch. For example, if tunnel-1 has TTL 10, tunnel-2 has TTL 20, tunnel-3 has TTL 30, and tunnel-4 has TTL 40, then tunnel-5 cannot have a unique TTL value, it must reuse one of the values assigned to the other tunnels (10, 20, 30, 40).

The no form of this command sets TTL to the default value of 64.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;COUNT&gt;</td>
<td>Specifies the hop count. Range: 1 to 255. Default: 64.</td>
</tr>
</tbody>
</table>

Examples

Defines a TTL of 99 for GRE tunnel 33.

switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ttl 99

Sets the TTL for GRE tunnel 33 to the default value of 64.

switch(config)# interface tunnel 33
switch(config-gre-if)# no ttl
Defines a TTL of **55** for IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# ttl 55
```

Sets the TTL for IPv6 in IPv4 tunnel **27** to the default value of 64.

```
switch(config)# interface tunnel 27
switch(config-ip-if)# no ttl
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**vrf attach**

```
vrf attach <VRF-NAME>
no vrf attach <VRF-NAME>
```

**Description**

Assigns an IP tunnel to a VRF. By default, all tunnels are automatically assigned to the default VRF when they are created.

The `no` form of this command assigns a tunnel to the default VRF (default).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VRF-NAME&gt;</td>
<td>Specifies the VRF name to which to assign the tunnel.</td>
</tr>
</tbody>
</table>

**Examples**

Assigns GRE tunnel **33** to **vrf1**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# vrf attach vrf1
```

Reassigns GRE tunnel **33** to the default VRF.

```
switch(config)# interface tunnel 33
switch(config-gre-if)# no vrf attach vrf1
```

Assigns IPv6 in IPv4 tunnel **27** to **vrf2**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# ttl 55
switch(config)# interface tunnel 27
switch(config-ip-if)# no vrf attach vrf1
```

Assigns IPv6 in IPv4 tunnel **27** to **vrf2**.
Reassigns IPv6 in IPv4 tunnel 27 to the default VRF.

```
switch(config)# interface tunnel 27 mode gre ipv4
switch(config-ip-if)# vrf attach vrf2
```

Assigns IPv6 in IPv6 tunnel 8 to vrf3.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# vrf attach vrf3
```

Reassigns IPv6 in IPv6 tunnel 8 to the default VRF.

```
switch(config)# interface tunnel 8
switch(config-ip-if)# no vrf attach vrf3
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-gre-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-ip-if</td>
<td></td>
</tr>
</tbody>
</table>
IP source lockdown provides added security by preventing IP source address spoofing on a per-port basis. Every packet is inspected for this purpose in hardware. When IP source lockdown is enabled, IP traffic received on an interface (port) is forwarded only if the VLAN, IP address, MAC address, interface (port) matches the IP binding database entry.

It is best to configure IP source lockdown during a switch maintenance period as enabling it may cause client traffic to be dropped for 10 to 15 seconds.

To use IPv4 source lockdown, the IPv4 binding database must be populated. The binding database is typically dynamically populated by DHCPv4 snooping that learns and saves the binding information. Alternatively, the IPv4 binding database can be statically populated with the `ipv4 source-binding` command described in this chapter. Often DHCPv4 snooping is used to dynamically populate most of the IP binding database along with the `ipv4 source-binding` command that is used to add the binding information for several known and trusted clients, typically administrators. For dynamic IP binding database population with DHCPv4 snooping, see DHCP snooping.

To use IPv6 source lockdown, the IPv6 binding database must be populated. The binding database is typically dynamically populated by DHCPv6 snooping that learns and saves the binding information. Alternatively, the IPv6 binding database can be statically populated with the `ipv6 source-binding` command described in this chapter. Often DHCPv6 snooping is used to dynamically populate most of the IPv6 binding database along with the `ipv6 source-binding` command that is used to add the binding information for several known and trusted clients, typically administrators. For dynamic IPv6 binding database population with DHCPv6 snooping, see DHCP snooping.

IP source lockdown should not be configured on ISL (inter-switch link) ports.

### IPv4 source lockdown commands

#### `ipv4 source-binding`

`ipv4 source-binding <VLAN-ID> <IPv4-ADDR> <MAC-ADDR> <IFNAME>`

`no ipv4 source-binding <VLAN-ID> <IPv4-ADDR> <MAC-ADDR> <IFNAME>`

**Description**

Adds static IPv4 client source binding information to the switch IP binding database. Although DHCPv4 snooping is often used to dynamically populate the binding database, this command is available for manually adding entries to the switch IP binding database.

Statically configured IP binding information supersedes any dynamically collected binding information for the same client.

The no form of this command removes the specified binding that was statically configured with the `ipv4 source-binding` command. The no form has no effect on bindings that were dynamically configured with DHCPv4 snooping.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VLAN-ID&gt;</td>
<td>Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.</td>
</tr>
<tr>
<td>&lt;IPV4-ADDR&gt;</td>
<td>Specifies the client IPv4 unicast address.</td>
</tr>
<tr>
<td>&lt;MAC-ADDR&gt;</td>
<td>Specifies the client MAC address.</td>
</tr>
<tr>
<td>&lt;IFNAME&gt;</td>
<td>Specifies the interface on which the client is connected.</td>
</tr>
</tbody>
</table>

### Examples

*On the 6400 Switch Series, interface identification differs.*

**Adding a static IPv4 binding:**

```bash
switch(config)# ip4 source-binding 1 10.2.1.4 00:50:56:96:e4:cf 1/1/1
```

**Removing a IPv4 binding:**

```bash
switch(config)# no ip4 source-binding 1 10.2.1.4 00:50:56:96:e4:cf 1/1/1
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv4 source-lockdown**

ipv4 source-lockdown
no ipv4 source-lockdown

**Description**

Enables IPv4 source lockdown for all VLANs on the selected interface (port).

The no form of this command disables IPv4 source lockdown for the selected interface (port).

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Enabling IPv4 source lockdown on interface 1/1/1:
switch(config)# interface 1/1/1
switch(config-if)# ipv4 source-lockdown

Enabling IPv4 source lockdown on interface lag112:

switch(config)# interface lag112
switch(config-if)# ipv4 source-lockdown

Disabling IPv4 source lockdown on interface 1/1/1:

switch(config)# interface 1/1/1
switch(config-if)# no ipv4 source-lockdown

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

ipv4 source-lockdown hardware retry

ipv4 source-lockdown hardware retry <VLAN-ID> <IPV4-ADDR>

Description
Retries the IPv4 source lockdown hardware programming for a client identified by VLAN and IPv4 address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VLAN-ID&gt;</td>
<td>Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.</td>
</tr>
<tr>
<td>&lt;IPV4-ADDR&gt;</td>
<td>Specifies the client IPv4 unicast address.</td>
</tr>
</tbody>
</table>

Example
Configure IPv4 source lockdown hardware retry for the client on VLAN 10.

switch(config)# ipv4 source-lockdown hardware retry 10 1.1.2.1
**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>config</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show ipv4 source-binding**

*show ipv4 source-binding [vsx-peer]*

**Description**

Shows all IPv4 static source binding information irrespective of source lockdown configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Showing all IPv4 source binding information:

```
switch# show ipv4 source-binding
     PORT    VLAN  MAC-ADDRESS   HW-STATUS  FROM  IPv4-ADDRESS
    1/1/1      2     aa:bb:cc:dd:ee:ff  Yes    static      1.2.3.4
    1/1/2      12    aa:ab:cc:dd:ee:ff  Yes    static      10.20.30.40
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt;) or Manager(#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
show ipv4 source-lockdown

show ipv4 source-lockdown [binding [interface <IFNAME> | ip <IPV4-ADDR> | mac <MAC-ADDR> | vlan <VLAN-ID>] | interface <IFNAME>] [vsx-peer]

**Description**
Shows summary or detailed IPv4 source lockdown information. When entered without parameters, summary status information for all interfaces (ports) in the binding database is shown.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding</td>
<td>Specifies that detailed lockdown binding record information is to be displayed. The binding database record can be identified by any one of interface (port), ip, mac, or vlan.</td>
</tr>
<tr>
<td>interface &lt;IFNAME&gt;</td>
<td>Specifies the client interface (port). When entered without the binding parameter, the summary status information is displayed for the specified interface.</td>
</tr>
<tr>
<td>ip &lt;IPV4-ADDR&gt;</td>
<td>Specifies the client IPv4 unicast address.</td>
</tr>
<tr>
<td>mac &lt;MAC-ADDR&gt;</td>
<td>Specifies the client MAC address.</td>
</tr>
<tr>
<td>vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Showing the summary status information for all interfaces in the binding database:

```
switch# show ipv4 source-lockdown

INTERFACE  LOCKDOWN  HW-STATUS
----------  --------  ---------
1/1/1       Yes      Yes
1/1/2       Yes      No
lag112      Yes      Yes
```

Showing the summary status information for the specified interface in the binding database:

```
switch# show ipv4 source-lockdown interface 1/1/2

INTERFACE  LOCKDOWN  HW-STATUS
----------  --------  ---------
1/1/2       Yes      No
```

Showing the detailed binding record and related information for all interfaces in the binding database:
switch# show_ipv4_source-lockdown_binding

Interface Name        : 1/1/1
VLAN Id              : 2000
MAC Address          : 00:50:56:96:e4:cf
IP Address           : 192.168.142.113
Time Remaining       : static
Lockdown Status      : Yes
Hardware Status      : Yes
Hardware Error Reason: --

Interface Name        : 1/1/2
VLAN Id              : 100
MAC Address          : 00:50:56:96:04:4d
IP Address           : 120.168.43.52
Time Remaining       : 115 seconds
Lockdown Status      : Yes
Hardware Status      : No
Hardware Error Reason: Resource unavailable

Interface Name        : lag112
VLAN Id              : 12
MAC Address          : 00:50:56:96:d8:3d
IP Address           : 120.168.76.182
Time Remaining       : static
Lockdown Status      : Yes
Hardware Status      : Yes
Hardware Error Reason: --

Showing the detailed binding record and related information for interface 1/1/2:

switch# show_ipv4_source-lockdown_binding_interface 1/1/2

Interface Name        : 1/1/2
VLAN Id              : 100
MAC Address          : 00:50:56:96:04:4d
IP Address           : 120.168.43.52
Time Remaining       : 115 seconds
Lockdown Status      : Yes
Hardware Status      : No
Hardware Error Reason: Resource unavailable

Showing the detailed binding record and related information for interface lag112 (identified in this example command by the IP address):

switch# show_ipv4_source-lockdown_binding_ip 120.168.76.182

Interface Name        : lag112
VLAN Id              : 12
MAC Address          : 00:50:56:96:d8:3d
IP Address           : 120.168.76.182
Time Remaining       : static
Lockdown Status      : Yes
Hardware Status      : Yes
Hardware Error Reason: --

Showing the detailed binding record and related information for interface 1/1/1 (identified in this example command by the MAC address):
switch# show ipv4 source-lockdown binding mac 00:50:56:96:e4:cf

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>VLAN Id</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Time Remaining</th>
<th>Lockdown Status</th>
<th>Hardware Status</th>
<th>Hardware Error Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>2000</td>
<td>00:50:56:96:e4:cf</td>
<td>192.168.142.113</td>
<td>static</td>
<td>Yes</td>
<td>Yes</td>
<td>--</td>
</tr>
</tbody>
</table>

Showing the detailed binding record and related information for interface 1/1/2 (identified in this example command by the VLAN):

switch# show ipv4 source-lockdown binding vlan 100

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>VLAN Id</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Time Remaining</th>
<th>Lockdown Status</th>
<th>Hardware Status</th>
<th>Hardware Error Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>100</td>
<td>00:50:56:96:04:4d</td>
<td>120.168.43.52</td>
<td>115 seconds</td>
<td>Yes</td>
<td>No</td>
<td>Resource unavailable</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**IPv6 source lockdown commands**

**ipv6 source-binding**

ipv6 source-binding <VLAN-ID> <IPV6-ADDR> <MAC-ADDR> <IFNAME>

no ipv6 source-binding <VLAN-ID> <IPV6-ADDR> <MAC-ADDR> <IFNAME>

**Description**

Adds static IPv6 client source binding information to the switch IPv6 binding database. Although DHCPv6 snooping is often used to dynamically populate the binding database, this command is available for manually adding entries to the switch IPv6 binding database.
Statically configured IPv6 binding information supersedes any dynamically collected binding information for the same client.

The no form of this command removes the specified binding that was statically configured with the `ipv6 source-binding` command. The no form has no effect on bindings that were dynamically configured with DHCPv6 snooping.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;VLAN-ID&gt;</td>
<td>Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.</td>
</tr>
<tr>
<td>&lt;IPV6-ADDR&gt;</td>
<td>Specifies the client IPv6 address.</td>
</tr>
<tr>
<td>&lt;MAC-ADDR&gt;</td>
<td>Specifies the client MAC address.</td>
</tr>
<tr>
<td>&lt;IFNAME&gt;</td>
<td>Specifies the interface on which the client is connected.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Adding a static IPv6 binding:

```
switch(config)# ipv6 source-binding 2 2000::2 00:12:11:44:55:12 1/1/28
```

Removing a IPv6 binding:

```
switch(config)# no ipv6 source-binding 2 2000::2 00:12:11:44:55:12 1/1/28
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ipv6 source-lockdown**

*ipv6 source-lockdown

no ipv6 source-lockdown

**Description**

Enables IPv6 source lockdown for all VLANs on the selected interface (port).

The no form of this command disables IPv6 source lockdown for the selected interface (port).
Examples

On the 6400 Switch Series, interface identification differs.

Enabling IPv6 source lockdown on interface 1/1/1:

```bash
switch(config)# interface 1/1/1
switch(config-if)# ipv6 source-lockdown
```

Enabling IPv6 source lockdown on interface lag112:

```bash
switch(config)# interface lag112
switch(config-if)# ipv6 source-lockdown
```

Disabling IPv6 source lockdown on interface 1/1/1:

```bash
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 source-lockdown
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ipv6 source-lockdown hardware retry**

`ipv6 source-lockdown hardware retry <VLAN-ID> <IPV6-ADDR>`

Description

Retries the IPv6 source lockdown hardware programming for a client identified by VLAN and IPv6 address.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;VLAN-ID&gt;</code></td>
<td>Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.</td>
</tr>
<tr>
<td><code>&lt;IPV6-ADDR&gt;</code></td>
<td>Specifies the client IPv6 address.</td>
</tr>
</tbody>
</table>

Example

Configure IPv6 source lockdown hardware retry for the client on VLAN 1.

```bash
switch(config)# ipv6 source-lockdown hardware retry 1 2000::2
```
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**show ipv6 source-binding**

**show ipv6 source-binding [vsx-peer]**

**Description**

Shows all IPv6 static source binding information irrespective of source lockdown configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Examples**

*On the 6400 Switch Series, interface identification differs.*

Showing all IPv6 source binding information:

```
switch# show ipv6 source-binding

<table>
<thead>
<tr>
<th>PORT</th>
<th>VLAN</th>
<th>MAC-ADDRESS</th>
<th>HW-STATUS</th>
<th>FROM</th>
<th>IPv6-ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>1234</td>
<td>00:50:56:96:4e:cf</td>
<td>--</td>
<td>static</td>
<td>3000::1</td>
</tr>
<tr>
<td>1/1/1</td>
<td>1</td>
<td>00:50:56:96:04:4d</td>
<td>--</td>
<td>static</td>
<td>3000::2</td>
</tr>
<tr>
<td>1/1/24</td>
<td>1</td>
<td>00:01:01:00:00:1</td>
<td>Yes</td>
<td>static</td>
<td>1001::1</td>
</tr>
</tbody>
</table>
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
### Platforms

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator (&gt; or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; or Manager (#) only.</td>
</tr>
<tr>
<td>6400</td>
<td>Operator (&gt; or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; or Manager (#) only.</td>
</tr>
</tbody>
</table>

### show ipv6 source-lockdown

**show ipv6 source-lockdown [binding [interface <IFNAME> | ip <IPV6-ADDR> | mac <MAC-ADDR> | vlan <VLAN-ID>]] | interface <IFNAME>]] [vsx-peer]

#### Description

Shows summary or detailed IPv6 source lockdown information. When entered without parameters, summary status information for all interfaces (ports) in the binding database is shown.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>binding</td>
<td>Specifies that detailed lockdown binding record information is to be displayed. The binding database record can be identified by any one of interface (port), ip, mac, or vlan.</td>
</tr>
<tr>
<td>interface &lt;IFNAME&gt;</td>
<td>Specifies the client interface (port). When entered without the binding parameter, the summary status information is displayed for the specified interface.</td>
</tr>
<tr>
<td>ip &lt;IPV6-ADDR&gt;</td>
<td>Specifies the client IPv6 address.</td>
</tr>
<tr>
<td>mac &lt;MAC-ADDR&gt;</td>
<td>Specifies the client MAC address.</td>
</tr>
<tr>
<td>vlan &lt;VLAN-ID&gt;</td>
<td>Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

#### Examples

*On the 6400 Switch Series, interface identification differs.*

Showing the summary status information for all interfaces in the binding database:

```
switch# show ipv6 source-lockdown

INTERFACE  LOCKDOWN  HW-STATUS
------------  --------  --------
1/1/1        Yes      Yes
1/1/2        Yes      Yes
lag112       Yes      --
```

Showing the summary status information for the specified interface in the binding database:
switch# show ipv6 source-lockdown interface 1/1/2

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>LOCKDOWN</th>
<th>HW-STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Showing the detailed binding record and related information for all interfaces in the binding database:

switch# show ipv6 source-lockdown binding

Interface Name : 1/1/1  
VLAN Id : 1234  
MAC Address : 00:50:56:96:e4:cf  
IP Address : aaaa:bbbb:cccc:dddd:eeee:1234  
Time Remaining : static  
Lockdown Status : Yes  
Hardware Status : Yes  
Hardware Error Reason : --

Interface Name : 1/1/2  
VLAN Id : 1234  
MAC Address : 00:50:56:96:04:4d  
IP Address : 4000::1  
Time Remaining : 3290 seconds  
Lockdown Status : Yes  
Hardware Status : No  
Hardware Error Reason : Resource unavailable

Interface Name : lag112  
VLAN Id : 151  
MAC Address : 00:50:56:96:d8:3d  
IP Address : 1001::5  
Time Remaining : 1200 seconds  
Lockdown Status : No  
Hardware Status : --  
Hardware Error Reason : --

Showing the detailed binding record and related information for interface 1/1/2:

switch# show ipv6 source-lockdown binding interface 1/1/2

Interface Name : 1/1/2  
VLAN Id : 1234  
MAC Address : 00:50:56:96:04:4d  
IP Address : 4000::1  
Time Remaining : 3290 seconds  
Lockdown Status : Yes  
Hardware Status : No  
Hardware Error Reason : Resource unavailable

Showing the detailed binding record and related information for interface 1/1/2 (identified in this example command by the IP address):

switch# show ipv6 source-lockdown binding ip 4000::1

Interface Name : 1/1/2  
VLAN Id : 1234
MAC Address : 00:50:56:96:04:4d
IP Address : 4000::1
Time Remaining : 515 seconds
Lockdown Status : No
Hardware Status : --
Hardware Error Reason : --

Showing the detailed binding record and related information for interface 1/1/1 (identified in this example command by the MAC address):

```
switch# show ipv6 source-lockdown binding mac 00:50:56:96:e4:cf
```

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>1/1/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Id</td>
<td>1234</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:50:56:96:e4:cf</td>
</tr>
<tr>
<td>IP Address</td>
<td>aaaa:bbbb:cccc:dddd:eeee:1234</td>
</tr>
<tr>
<td>Time Remaining</td>
<td>static</td>
</tr>
<tr>
<td>Lockdown Status</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware Status</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware Error Reason</td>
<td>--</td>
</tr>
</tbody>
</table>

Showing the detailed binding record and related information for interface lag112 (identified in this example command by the VLAN):

```
switch# show ipv6 source-lockdown binding vlan 151
```

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>lag112</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Id</td>
<td>151</td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:50:56:96:d8:3d</td>
</tr>
<tr>
<td>IP Address</td>
<td>1001::5</td>
</tr>
<tr>
<td>Time Remaining</td>
<td>1200 seconds</td>
</tr>
<tr>
<td>Lockdown Status</td>
<td>No</td>
</tr>
<tr>
<td>Hardware Status</td>
<td>--</td>
</tr>
<tr>
<td>Hardware Error Reason</td>
<td>--</td>
</tr>
</tbody>
</table>

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>
The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. The protocol is used by network devices, including routers, to send error messages and operational information. For example, an ICMP message might indicate that a requested service is not available. Another example of an ICMP message might be that a host or router could not be reached.

**ICMP message types**

The type field identifies the type of message sent by the host or gateway.

<table>
<thead>
<tr>
<th>Type</th>
<th>ICMP messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Echo Reply (Ping Reply, used with Type 8, Ping Request)</td>
</tr>
<tr>
<td>3</td>
<td>Destination Unreachable</td>
</tr>
<tr>
<td>4</td>
<td>Source Quench</td>
</tr>
<tr>
<td>5</td>
<td>Redirect</td>
</tr>
<tr>
<td>8</td>
<td>Echo Request (Ping Request, used with Type 0, Ping Reply)</td>
</tr>
<tr>
<td>9</td>
<td>Router Advertisement (Used with Type 9)</td>
</tr>
<tr>
<td>10</td>
<td>Router Solicitation (Used with Type 10)</td>
</tr>
<tr>
<td>11</td>
<td>Time Exceeded</td>
</tr>
<tr>
<td>12</td>
<td>Parameter Problem</td>
</tr>
<tr>
<td>13</td>
<td>Timestamp Request (Used with Type 14)</td>
</tr>
<tr>
<td>14</td>
<td>Timestamp Reply (Used with Type 13)</td>
</tr>
<tr>
<td>15</td>
<td>Information Request (obsolete) (Used with Type 16)</td>
</tr>
<tr>
<td>16</td>
<td>Information Reply (obsolete) (Used with Type 15)</td>
</tr>
<tr>
<td>17</td>
<td>Address Mask Request (Used with Type 17)</td>
</tr>
<tr>
<td>18</td>
<td>Address Mask Reply (Used with Type 18)</td>
</tr>
</tbody>
</table>

**When ICMP messages are sent**
ICMP messages are sent when one or more of the following scenarios occur:

- A datagram cannot reach its destination.
- The gateway does not have the buffering capacity to forward a datagram.
- The gateway can direct the host to send traffic on a shorter route.

**ICMP redirect messages**

ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination.

**When ICMP redirect messages are sent**

The switch is configured to send redirects by default. ICMP redirect messages are sent when one or more of the following scenarios occur:

- The interface on which the packet comes into the router is the same interface on which the packet gets routed out.
- The subnet or network of the source IP address is on the same subnet or network of the next-hop IP address of the routed packet.
- The datagram is not source-routed.
- The destination unicast address is unreachable. In this case, the router generates the ICMP destination unreachable message to inform the source host about the situation.

**ICMP commands**

**ip icmp redirect**

```
ip icmp redirect
no ip icmp redirect
```

**Description**

Enables the sending of ICMPv4 and ICMPv6 redirect messages to the source host. Enabled by default. The no form of this command disables ICMPv4 and ICMPv6 redirect messages to the source host.

**Examples**

Enabling ICMP redirect messages:

```
switch(config)# ip icmp redirect
```

Disabling ICMP redirect messages:

```
switch(config)# no ip icmp redirect
```

**Command History**
Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

ip icmp throttle

*ip icmp throttle <PACKET-INTERVAL>*

*no ip icmp throttle [<PACKET-INTERVAL>]*

**Description**

Used to configure the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages.

The *no* form of this command disables the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages.

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

**Examples**

Enabling the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages:

```
switch(config)# ip icmp throttle 3000
```

Disabling the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages:

```
switch(config)# no ip icmp throttle
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.8</td>
<td>Added the optional &lt;PACKET-INTERVAL&gt; parameter to the no form of the command.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
**ip icmp unreachable**

**Description**
Enables the sending of ICMPv4 and ICMPv6 destination unreachable messages on the switch to a source host when a specific host is unreachable. The unreachable host address originates from the failed packed. Default setting.

The no form of this command disables the sending of ICMPv4 and ICMPv6 destination unreachable messages from the switch to a source host when a specific host is unreachable. This command does not prevent other hosts from sending an ICMP unreachable message.

**Examples**
Enabling ICMPv4 and ICMPv6 destination unreachable messages to a source host:

```
switch(config)# ip icmp unreachable
```

Disabling ICMPv4 and ICMPv6 destination unreachable messages to a source host:

```
switch(config)# no ip icmp unreachable
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
The Domain Name System (DNS) is the Internet protocol for mapping a hostname to its IP address. DNS allows users to enter more readily memorable and intuitive hostnames, rather than IP addresses, to identify devices connected to a network. It also allows a host to keep the same hostname even if it changes its IP address.

Hostname resolution can be either static or dynamic.

- In static resolution, a local table is defined on the switch that associates hostnames with their IP addresses. Static tables can be used to speed up the resolution of frequently queried hosts.
- Dynamic resolution requires that the switch query a DNS server located elsewhere on the network. Dynamic name resolution takes more time than static name resolution, but requires far less configuration and management.

**DNS client**

The DNS client resolves hostnames to IP addresses for protocols that are running on the switch. When the DNS client receives a request to resolve a hostname, it can do so in one of two ways:

- Forward the request to a DNS name server for resolution.
- Reply to the request without using a DNS name server, by resolving the name using a statically defined table of hostnames and their associated IP addresses.

### Configuring the DNS client

**Procedure**

1. Configure one or more DNS name servers with the command `ip dns server`.
2. To resolve DNS requests by appending a domain name to the requests, either configure a single domain name with the command `ip dns domain-name`, or configure a list of up to six domain names with the command `ip dns domain-list`.
3. To use static name resolution for certain hosts, associate an IP address to a host with the command `ip dns host`.
4. Review your DNS configuration settings with the command `show ip dns`.

**Examples**

This example creates the following configuration:

- Defines the domain `switch.com` to append to all requests.
- Defines a DNS server with IPv4 address of `1.1.1.1`.
- Defines a static DNS host named `myhost1` with an IPv4 address of `3.3.3.3`.
- DNS client traffic is sent on the default VRF (named `default`).
switch(config)# ip dns domain-name switch.com
switch(config)# ip dns server-address 1.1.1.1
switch(config)# ip dns host myhost 3.3.3.3
switch(config)# exit
switch# show ip dns

VRF Name : vrf_mgmt

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VRF Name : vrf_default
Domain Name : switch.com
DNS Domain list :
Name Domain list : 1.1.1.1

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

myhost1

This example creates the following configuration:

- Defines three domains to append to DNS requests domain1.com, domain2.com, domain3.com with traffic forwarding on VRF mainvrf.
- Defines a DNS server with an IPv6 address of c::13.
- Defines a DNS host named myhost with an IPv4 address of 3.3.3.3.

switch(config)# ip dns domain-list domain1.com vrf mainvrf
switch(config)# ip dns domain-list domain2.com vrf mainvrf
switch(config)# ip dns domain-list domain3.com vrf mainvrf
switch(config)# ip dns server-address c::13
switch(config)# ip dns host myhost 3.3.3.3 vrf mainvrf
switch(config)# quit
switch# show ip dns mainvrf

VRF Name : mainvrf
Domain Name :
DNS Domain list : domain1.com, domain2.com, domain3.com
Name Server(s) : c::13

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

myhost 3.3.3.3

**DNS client commands**

**ip dns domain-list**

```
ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
nop dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
```

**Description**

Configures one or more domain names that are appended to the DNS request. The DNS client appends each name in succession until the DNS server replies. Domains can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF.
The no form of this command removes a domain from the list.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list &lt;DOMAIN-NAME&gt;</td>
<td>Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies a VRF name. Default: default.</td>
</tr>
</tbody>
</table>

**Examples**

This example defines a list with two entries: **domain1.com** and **domain2.com**.

```
switch(config)# ip dns domain-list domain1.com
switch(config)# ip dns domain-list domain2.com
```

This example defines a list with two entries, **domain2.com** and **domain5.com**, with requests being sent on **mainvrf**.

```
switch(config)# ip dns domain-list domain2.com vrf mainvrf
switch(config)# ip dns domain-list domain5.com vrf mainvrf
```

This example removes the entry **domain1.com**.

```
switch(config)# no ip dns domain-list domain1.com
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip dns domain-name**

```
ip dns domain-name <DOMAIN-NAME> [ vrf <VRF-NAME> ]
no ip dns domain-name <DOMAIN-NAME> [ vrf <VRF-NAME> ]
```

**Description**

Configures a domain name that is appended to the DNS request. The domain can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF. If a domain list is defined with the command `ip dns domain-list`, the domain name defined with this command is ignored. The no form of this command removes the domain name.
DNS

Parameter | Description
---|---
<DOMAIN-NAME> | Specifies the domain name to append to DNS requests. Length: 1 to 256 characters.
vrf <VRF-NAME> | Specifies a VRF name. Default: default.

Examples
Setting the default domain name to domain.com:

```
switch(config)# ip dns domain-name domain.com
```

Removing the default domain name domain.com:

```
switch(config)# no ip dns domain-name domain.com
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip dns host**

```
ip dns host <HOST-NAME> <IP-ADDR> [ vrf <VRF-NAME> ]
no ip dns host <HOST-NAME> <IP-ADDR> [ vrf <VRF-NAME> ]
```

Description

Associates a static IP address with a hostname. The DNS client returns this IP address instead of querying a DNS server for an IP address for the hostname. Up to six hosts can be defined. If no VRF is defined, the default VRF is used.

The *no* form of this command removes a static IP address associated with a hostname.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host &lt;HOST-NAME&gt;</td>
<td>Specifies the name of a host. Length: 1 to 256 characters.</td>
</tr>
<tr>
<td>&lt;IP-ADDR&gt;</td>
<td>Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies a VRF name. Default: default.</td>
</tr>
</tbody>
</table>
Examples

This example defines an IPv4 address of 3.3.3.3 for host1.

```
switch(config)# ip dns host host1 3.3.3.3
```

This example defines an IPv6 address of b::5 for host 1.

```
switch(config)# ip dns host host1 b::5
```

This example defines removes the entry for host 1 with address b::5.

```
switch(config)# no ip dns host host1 b::5
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**ip dns server address**

```
ip dns server-address <IP-ADDR> [ vrf <VRF-NAME> ]
no ip dns server-address <IP-ADDR> [ vrf <VRF-NAME> ]
```

Description

Configures the DNS name servers that the DNS client queries to resolve DNS queries. Up to six name servers can be defined. The DNS client queries the servers in the order that they are defined. If no VRF is defined, the default VRF is used.

The no form of this command removes a name server from the list.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP-ADDR&gt;</td>
<td>Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies a VRF name. Default: default.</td>
</tr>
</tbody>
</table>

Examples

This example defines a name server at 1.1.1.1.
switch(config)# ip dns server-address 1.1.1.1

This example defines a name server at a::1.

switch(config)# ip dns server-address a::1

This example removes a name server at a::1.

switch(config)# no ip dns server-address a::1

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show ip dns

show ip dns [vrf <VRF-NAME>] [vsx-peer]

Description

Shows all DNS client configuration settings or the settings for a specific VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the VRF for which to show information. If no VRF is defined, the default VRF is used.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

Examples

These examples define DNS settings and then show how they are displayed with the show ip dns command.

switch(config)# ip dns domain-name domain.com
switch(config)# ip dns domain-list domain5.com
switch(config)# ip dns domain-list domain8.com
switch(config)# ip dns server-address 4.4.4.4
switch(config)# ip dns server-address 6.6.6.6
switch(config)# ip dns host host3 5.5.5.5
switch(config)# ip dns host host2 2.2.2.2
switch(config)# ip dns host host3 c::12
switch(config)# ip dns domain-name reddomain.com vrf red
switch(config)# ip dns domain-list reddomain5.com vrf red
switch(config)# ip dns domain-list reddomain8.com vrf red
switch(config)# ip dns server-address 4.4.4.5 vrf red
switch(config)# ip dns server-address 6.6.6.7 vrf red
switch(config)# ip dns host host3 5.5.5.6 vrf red
switch(config)# ip dns host host2 2.2.2.3 vrf red
switch(config)# ip dns host host3 c::13 vrf red
switch# show ip dns
VRF Name : default
Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>host2</td>
<td>2.2.2.2</td>
</tr>
<tr>
<td>host3</td>
<td>5.5.5.5</td>
</tr>
<tr>
<td>host3</td>
<td>c::12</td>
</tr>
</tbody>
</table>

VRF Name : red

Domain Name : reddomain.com
DNS Domain list : reddomain5.com, reddomain8.com
Name Server(s) : 4.4.4.5, 6.6.6.7

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>host2</td>
<td>2.2.2.3</td>
</tr>
<tr>
<td>host3</td>
<td>5.5.5.6</td>
</tr>
<tr>
<td>host3</td>
<td>c::13</td>
</tr>
</tbody>
</table>

switch(config)# ip dns domain-name domain.com vrf red
switch(config)# ip dns domain-list domain5.com vrf red
switch(config)# ip dns domain-list domain8.com vrf red
switch(config)# ip dns server-address 4.4.4.4 vrf red
switch(config)# ip dns server-address 6.6.6.6 vrf red
switch(config)# ip dns host host3 5.5.5.5 vrf red
switch(config)# no ip dns host host2 2.2.2.2 vrf red
switch(config)# ip dns host host3 c::12 vrf red

switch# show ip dns vrf red
VRF Name : red
Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>host3</td>
<td>5.5.5.5</td>
</tr>
<tr>
<td>host3</td>
<td>c::12</td>
</tr>
</tbody>
</table>

Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

## Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; ) only.</td>
</tr>
</tbody>
</table>
ARP (Address Resolution Protocol) is used to map the network address assigned to a device to its physical address. For example, on an Ethernet network, ARP maps layer 3 IPv4 network addresses to layer 2 MAC addresses. (ARP does not work with IPv6 addresses. Instead, the Neighbor discovery protocol is used.) ARP operates at layer 2. ARP requests are broadcast to all devices on the local network segment and are not forwarded by routers. ARP is enabled by default and cannot be disabled.

**Proxy ARP**

Proxy ARP allows a routing switch to answer ARP requests from devices on one network on behalf of devices on another network. The ARP proxy is aware of the location of the traffic destination, and offers its own MAC address as the final destination.

For example, if Proxy ARP is enabled on a routing switch connected to two subnets (10.10.10.0/24 and 20.20.20.0/24), the routing switch can respond to an ARP request from 10.10.10.69 for the MAC address of the device with IP address 20.20.20.69.

Typically, the host that sent the ARP request then sends its packets to the switch that has the ARP proxy. This switch then forwards the packets to the intended host through a mechanism such as a tunnel.

Proxy ARP is supported on L3 physical and VLAN interfaces. It is disabled by default. To enable proxy ARP, routing must be enabled on the interface.

**Local proxy ARP**

Local proxy ARP is a technique by which a device on a given network answers the ARP queries for a host address that is on the same network. It is primarily used to enable layer 3 communication between hosts within a common subnet that are separated by layer 2 boundaries (Example: PVLAN). Local proxy ARP is supported on L3 physical and VLAN interfaces.

Local proxy ARP is disabled by default. Routing must be enabled on the interface to enable local proxy ARP.

**Dynamic ARP Inspection**

ARP is used for resolving IP against MAC addresses on a broadcast network segment like the Ethernet and was originally defined by Internet Standard RFC 826. ARP does not support any inherent security mechanism and as such depends on simple datagram exchanges for the resolution, with many of these being broadcast.

Because it is an unreliable and non-secure protocol, ARP is vulnerable to attacks. Some attacks may be targeted toward the networks whereas other attacks may be targeted toward the switch itself. The attacks primarily intend to create denial of service (DoS) for the other entities present in the network.

Most of the attacks are carried out in one of the following three forms:

- Overwhelming the switch control plane with too many ARP packets.
- Overwhelming the switch control plane with too many unresolved data packets.
- Masquerading as a trusted gateway/server by wrongly advertising ARPs.
Several defense mechanisms can be put in place on a switch to protect against attacks:

- Limit the amount of ARP activity allowed from a host or on a port.
- Ensure that all ARP packets are consistent with one or more binding databases, which can be created through various means.
- Enforce integrity checks on the ARP packets to check against different MAC or IP addresses in the Ethernet or IP header.

This release implements Dynamic ARP Inspection to enforce DHCP snooping binding on all ARP packets and is limited to the 8400 platform. The feature will be disabled from the code, CLI, and schema by the use of appropriate config flags for other platforms.

Only the following is supported:

- Enabling and disabling of Dynamic ARP Inspection on a VLAN level (it does not have to be SVI).
- Defining the member ports of a VLAN as either trusted or untrusted.
- Only ARP traffic on untrusted ports subjected to checks.
- Routed ports (RoPs) always treated as trusted.
- Listening to the DHCP Bindings table and check every ARP packet to match against the binding.

ARP ACLs are not supported in this release and the DHCP snooping table will be the only source of binding.

### Configuring proxy ARP

#### Procedure

1. Switch to configuration context with the command `config`.
2. Switch to an interface with the command `interface`, or to an interface VLAN with the command `interface vlan`, or to a LAG with the command `interface lag`.
3. Enable local proxy ARP with the command `ip proxy-arp`.

#### Examples

*On the 6400 Switch Series, interface identification differs.*

This example configures proxy ARP on interface **1/1/2**

```plaintext
switch# config
switch(config)# interface 1/1/2
switch(config)# routing
switch(config-if)# ip proxy-arp
```

This example configures proxy ARP on interface **VLAN 30**.

```plaintext
switch# config
switch(config)# interface vlan 30
switch(config-vlan-30)# ip proxy-arp
```

### Configuring local proxy ARP

#### Procedure
1. Switch to configuration context with the command `config`.
2. Switch to an interface with the command `interface`, or to an interface VLAN with the command `interface vlan`, or to a LAG with the command `interface lag`.
3. Enable local proxy ARP with the command `ip local-proxy-arp`.

**Examples**

*On the 6400 Switch Series, interface identification differs.*

This example configures local proxy ARP on interface 1/1/2

```
switch# config
switch(config)# interface 1/1/2
switch(config)# routing
switch(config-if)# ip local-proxy-arp
```

This example configures local proxy ARP on interface VLAN 30.

```
switch# config
switch(config)# interface vlan 30
switch(config-vlan-30)# ip local-proxy-arp
```

**Dynamic ARP Inspection**

ARP is used for resolving IP against MAC addresses on a broadcast network segment like the Ethernet and was originally defined by Internet Standard RFC 826. ARP does not support any inherent security mechanism and as such depends on simple datagram exchanges for the resolution, with many of these being broadcast.

Because it is an unreliable and non-secure protocol, ARP is vulnerable to attacks. Some attacks may be targeted toward the networks whereas other attacks may be targeted toward the switch itself. The attacks primarily intend to create denial of service (DoS) for the other entities present in the network.

Most of the attacks are carried out in one of the following three forms:

- Overwhelming the switch control plane with too many ARP packets.
- Overwhelming the switch control plane with too many unresolved data packets.
- Masquerading as a trusted gateway/server by wrongly advertising ARPs.

Several defense mechanisms can be put in place on a switch to protect against attacks:

- Limit the amount of ARP activity allowed from a host or on a port.
- Ensure that all ARP packets are consistent with one or more binding databases, which can be created through various means.
- Enforce integrity checks on the ARP packets to check against different MAC or IP addresses in the Ethernet or IP header and ARP header.

This release implements Dynamic ARP Inspection to enforce DHCP snooping binding on all ARP packets and is supported on the 6300, 6400, and 8400 platforms. The feature will be disabled from the code, CLI, and schema by the use of appropriate config flags for other platforms.
Only the following is supported:

- Enabling and disabling of Dynamic ARP Inspection on a VLAN level (it does not have to be SVI).
- Defining the member ports of a VLAN as either trusted or untrusted.
- Only ARP traffic on untrusted ports subjected to checks.
- Routed ports (RoPs) always treated as trusted.
- Listening to the DHCP Bindings table and check every ARP packet to match against the binding.

ARP ACLs are not supported in this release and the DHCP snooping table will be the only source of binding.

**ARP commands**

**arp cache-limit**

`arp cache-limit <LIMIT>`

**Description**

Specifies the maximum number of entries in the ARP (Address Resolution Protocol) cache.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;LIMIT&gt;</code></td>
<td>Specifies the maximum number of entries in the ARP cache. Range: 4096 to 131072. Default: 131072.</td>
</tr>
</tbody>
</table>

**Examples**

```
switch(config)# arp cache-limit 4097
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td><code>config</code></td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

**arp inspection**

`arp inspection`

**Description**

Enables Dynamic ARP Inspection on the current VLAN, forcing all ARP packets from untrusted ports to be subjected to a MAC-IP association check against a binding table.

The `no` form of this command disables Dynamic ARP Inspection on the VLAN.
Examples

Enabling dynamic ARP inspection:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# arp inspection
```

Disabling dynamic ARP inspection:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# no arp inspection
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-vlan-&lt;VLAN-ID&gt;</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

arp inspection trust

```
arp inspection trust
no arp inspection trust
```

Description

ConfURES the interface as a trusted. All interfaces are untrusted by default. The no form of this command returns the interface to the default state (untrusted).

Example

Setting an interface as trusted:

```
switch(config-if)# arp inspection trust
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
arp ipv4 mac

arp ipv4 <IPV4_ADDR> mac <MAC_ADDR>
no arp ipv4 <IPV4_ADDR> mac <MAC_ADDR>

Description
Specifies a permanent static neighbor entry in the ARP table (for IPv4 neighbors).
The no form of this command deletes a permanent static neighbor entry from the ARP table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 &lt;IPV4-ADDR&gt;</td>
<td>Specifies the IP address of the neighbor or the virtual IP address of the cluster in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Range: 4096 to 131072. Default: 131072.</td>
</tr>
<tr>
<td>mac &lt;MAC-ADDR&gt;</td>
<td>Specifies the MAC address of the neighbor or the multicast MAC address in IANA format (xx:xx:xx:xx:xx:xx), where x is a hexadecimal number from 0 to F. Range: 4096 to 131072. Default: 131072.</td>
</tr>
</tbody>
</table>

Example
On the 6400 Switch Series, interface identification differs.
Configuring a static ARP entry on a interface VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# arp ipv4 2.2.2.2 mac 01:00:5e:00:00:01
```

Removing a static ARP entry on interface VLAN10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no arp ipv4 2.2.2.2 mac 01:00:5e:00:00:01
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td></td>
<td>config-if-vlan</td>
<td></td>
</tr>
</tbody>
</table>
clear arp

clear arp [port <PORT-ID> | vrf {all-vrfs | <VRF-NAME>}]  

Description

Clears IPv4 and IPv6 neighbor entries from the ARP table. If you do not specify any parameters, ARP table entries are cleared for the default VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port &lt;PORT-ID&gt;</td>
<td>Specifies a physical port on the switch. Format: member/slot/port. For example: 1/1/1.</td>
</tr>
<tr>
<td>all-vrfs</td>
<td>Selects all VRFs.</td>
</tr>
<tr>
<td>&lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF. Default: default.</td>
</tr>
</tbody>
</table>

Examples

Clearing all IPv4 and IPv6 neighbor ARP entries for the default VRF:

```
switch# clear arp
```

Clearing all ARP neighbor entries for a port (On the 6400 Switch Series, interface identification differs.):

```
switch# clear arp 1/1/35
```

Clearing all IPv4 and IPv6 neighbor ARP entries for all VRFs:

```
switch# clear arp vrf all-vrfs
```

Clearing all IPv4 and IPv6 neighbor ARP entries for a specific VRF instance:

```
switch# clear arp vrf RED
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
no ip local-proxy-arp

Description
Enables local proxy ARP on the specified interface. Local proxy ARP is supported on Layer 3 physical interfaces and on VLAN interfaces. To enable local proxy ARP on an interface, routing must be enabled on that interface.
The no form of this command disables local proxy ARP on the specified interface.

Examples
On the 6400 Switch Series, interface identification differs.
Enabling local proxy ARP on interface 1/1/1:

```
switch# interface 1/1/1
switch(config-if)# ip local-proxy-arp
```

Enabling local proxy ARP on interface VLAN 3:

```
switch# interface vlan 3
switch(config-if-vlan)# ip local-proxy-arp
```

Disabling local proxy ARP on interface 1/1/1.

```
switch# interface 1/1/1
switch(config-if)# no ip local-proxy-arp
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td></td>
<td>config-if-vlan</td>
<td></td>
</tr>
</tbody>
</table>

ipv6 neighbor mac

ipv6 neighbor <IPV6-ADDR> mac <MAC-ADDR>
no ipv6 neighbor <IPV6-ADDR> mac <MAC-ADDR>

Description
Specifies a permanent static neighbor entry in the ARP table (for IPv6 neighbors).
The no form of this command deletes a permanent static neighbor entry from the ARP table.
## Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IPV6-ADDR&gt;&gt;</td>
<td>Specifies an IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. Range: 4096 to 131072. Default: 131072.</td>
</tr>
<tr>
<td>mac &lt;MAC-ADDR&gt;&gt;</td>
<td>Specifies the MAC address of the neighbor (xx:xx:xx:xx:xx:xx), where x is a hexadecimal number from 0 to F. Range: 4096 to 131072. Default: 131072.</td>
</tr>
</tbody>
</table>

## Example

*On the 6400 Switch Series, interface identification differs.*

Creates a static ARP entry on interface 1/1/1.

```
switch(config)# interface 1/1/1
switch(config-if)# arp ipv6 neighbor 2001:0db8:85a3::8a2e:0370:7334 mac 00:50:56:96:df:c8
```

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

## Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

## ip proxy-arp

**ip proxy-arp**

**no ip proxy-arp**

### Description

Enables proxy ARP for the specified Layer 3 interface. Proxy ARP is supported on Layer 3 physical interfaces, LAG interfaces, and VLAN interfaces. It is disabled by default. To enable proxy ARP on an interface, routing must be enabled on that interface.

The **no** form of this command disables proxy ARP for the specified interface.

### Examples

Enabling proxy ARP on interface 1/1/1:

```
switch# interface 1/1/1
switch(config-if)# ip proxy-arp
```

Enabling proxy ARP on VLAN 3:
Enabling proxy ARP on a LAG 11:

```
switch(config)# int lag 11
switch(config-lag-if)# ip proxy-arp
```

Disabling proxy ARP on interface 1/1/1:

```
switch# interface 1/1/1
switch(config-if)# no ip proxy-arp
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td></td>
<td>config-if-vlan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>config-lag-vlan</td>
<td></td>
</tr>
</tbody>
</table>

**show arp**

`show arp [vsx-peer]`

**Description**

Shows the entries in the ARP (Address Resolution Protocol) table.

**Parameter** | **Description**
---|---
vsx-peer | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

**Usage**

This command displays information about ARP entries, including the IP address, MAC address, port, and state.

When no parameters are specified, the `show arp` command shows all ARP entries for the default VRF (Virtual Router Forwarding) instance.

**Examples**
switch# show arp

<table>
<thead>
<tr>
<th>IPv4 Address</th>
<th>MAC</th>
<th>Port</th>
<th>Physical Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>00:50:56:96:7b:e0</td>
<td>vlan10</td>
<td>1/1/29</td>
<td>stale</td>
</tr>
<tr>
<td>192.168.1.3</td>
<td>00:50:56:96:7b:ac</td>
<td>vlan10</td>
<td>1/1/1</td>
<td>reachable</td>
</tr>
</tbody>
</table>

Total Number Of ARP Entries Listed- 2.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Manager(#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show arp inspection interface

show arp inspection interface

Description

Displays the current configuration of dynamic ARP inspection on a VLAN or interface.

Examples

On the 6400 Switch Series, interface identification differs.

switch# show arp inspection interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust-State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Untrusted</td>
</tr>
</tbody>
</table>

switch# show arp inspection interface vsx-peer

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trust-State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Untrusted</td>
</tr>
<tr>
<td>lag100</td>
<td>Trusted</td>
</tr>
</tbody>
</table>

switch# show arp inspection interface 1/1/1
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (‡)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show arp inspection statistics**

**show arp inspection statistics**

**Description**

Displays statistics about forwarded and dropped ARP packets.

**Examples**

```
switch# show arp inspection statistics vlan 1-200

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Forwarded</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN_1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

```
switch# show arp inspection statistics vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Forwarded</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN_1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>200</td>
<td>VLAN200</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information
### Platforms

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

### show arp state

**show arp state {all | failed | incomplete | permanent | reachable | stale} [vsx-peer]**

**Description**

Shows ARP (Address Resolution Protocol) cache entries that are in the specified state.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows the ARP cache entries for all VRF (Virtual Router Forwarding) instances.</td>
</tr>
<tr>
<td>failed</td>
<td>Shows the ARP cache entries that are in failed state. The neighbor might have been deleted.</td>
</tr>
<tr>
<td>incomplete</td>
<td>Shows the ARP cache entries that are in incomplete state. An incomplete state means that address resolution is in progress and the link-layer address of the neighbor has not yet been determined. A solicitation request was sent, and the switch is waiting for a solicitation reply or a timeout.</td>
</tr>
<tr>
<td>permanent</td>
<td>Shows the ARP cache entries that are in permanent state. ARP entries that are in a permanent state can be removed by administrative action only.</td>
</tr>
<tr>
<td>reachable</td>
<td>Shows the ARP cache entries that are in reachable state, meaning that the neighbor is known to have been reachable recently.</td>
</tr>
<tr>
<td>stale</td>
<td>Shows ARP cache entries that are in stale state. ARP cache entries are in the stale state if the elapsed time is in excess of the ARP timeout in seconds since the last positive confirmation that the forwarding path was functioning properly.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

### Examples

**switch# show arp state failed**

<table>
<thead>
<tr>
<th>IPv4 Address</th>
<th>MAC</th>
<th>Port</th>
<th>Physical Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.4</td>
<td>vlan10</td>
<td></td>
<td></td>
<td>failed</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

show arp summary

show arp summary [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Shows a summary of the IPv4 and IPv6 neighbor entries on the switch for all VRFs or a specific VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-vrfs</td>
<td>Selects all VRFs.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

Examples

Showing summary ARP information for all VRFs:

```
switch# show arp summary all-vrfs
ARP Entry's State : IPv4  IPv6
---------------------------------------------------------------
Number of Reachable ARP entries : 2  0
Number of Stale ARP entries      : 0  0
Number of Failed ARP entries     : 2  2
Number of Incomplete ARP entries : 0  0
Number of Permanent ARP entries  : 0  0
---------------------------------------------------------------
Total ARP Entries: 6 : 4  2
```
Showing a summary of all IPv4 and IPv6 neighbor entries on the primary and secondary (peer) switches:

```
vsx-primary# show arp summary
ARP Entry's State       IPv4        IPv6
---------------------------------------------------------------
Number of Reachable ARP entries 25858       32231
Number of Stale ARP entries    0           1
Number of Failed ARP entries   0           257
Number of Incomplete ARP entries 0         0
Number of Permanent ARP entries 0         0
---------------------------------------------------------------
Total ARP Entries     58347       25858
```

```
vsx-primary# show arp summary vsx-peer
ARP Entry's State       IPv4        IPv6
---------------------------------------------------------------
Number of Reachable ARP entries 25858       3168
Number of Stale ARP entries    0           3
Number of Failed ARP entries   0           317
Number of Incomplete ARP entries 0         0
Number of Permanent ARP entries 0         0
---------------------------------------------------------------
Total ARP Entries     58346       25858
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show arp timeout**

```
show arp timeout [INTERFACE] [vsx-peer]
```

**Description**

Shows the age-out period for each ARP (Address Resolution Protocol) entry for a port, LAG, or VLAN interface.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE</td>
<td>Specifies a physical port, VLAN, or LAG on the switch. For physical ports, use the format member/slot/port (for example, 1/3/1).</td>
</tr>
</tbody>
</table>
vsx-peer | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

**Examples**

Showing ARP timeout information for a port:

```
switch# show arp timeout 1/1/1
ARP Timeout:
--------------
Port       VRF     Timeout
1/1/1       default 600
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

**Command Information**

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show arp vrf**

```
show arp {all-vrfs | vrf <VRF-NAME>} [vsx-peer]
```

**Description**

Shows the ARP table for all VRF instances, or for the named VRF.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-vrfs</td>
<td>Specifies all VRFs.</td>
</tr>
<tr>
<td>vrf &lt;VRF-NAME&gt;</td>
<td>Specifies the name of a VRF. Length: 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not</td>
</tr>
</tbody>
</table>
### Examples

Showing ARP entries for VRF test.

```
switch# show arp vrf test
ARP IPv4 Entries:
----------------------------------
IPv4 Address      MAC       Port  Physical Port  State     VRF
10.20.30.40       00:50:56:bd:6a:c5  1/1/29  1/1/29  reachable  test
----------------------------------
```

Showing ARP entries for all VRFs.

```
switch# show arp all-vrfs
ARP IPv4 Entries:
----------------------------------
IPv4 Address      MAC       Port  Physical Port  State     VRF
192.168.120.10    00:50:56:bd:10:be  1/1/32  1/1/32  reachable  red
10.20.30.40       00:50:56:bd:6a:c5  1/1/29  1/1/29  reachable  test
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt;) only.</td>
</tr>
</tbody>
</table>

**show ipv6 neighbors**
show ipv6 neighbors {all-vrfs | vrf <VRF-NAME>} [vsx-peer]

Description
Shows entries in the ARP table for all IPv6 neighbors for all VRFs or for a specific VRF. When no parameters are specified, this command shows all ARP entries for the default VRF, and state information for reachable and stale entries only.

Parameter | Description
--- | ---
all-vrfs | Specifies all VRFs.
vrf <VRF-NAME> | Specifies the name of a VRF. Length: 1 to 32 alphanumeric characters.
vsx-peer | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples
switch# show ipv6 neighbors
IPv6 Entries:
----------------------------------------
IPv6 Address | MAC | Port | Physical Port | State
---------- | ---- | ---- | ------------- | ----
fe80::a21d:48ff:fe8f:2700 | a0:1d:48:8f:27:00 | vlan2300 | 1/1/31 | reachable
fe80::f603:43ff:fe80:a600 | f4:03:43:80:a6:00 | vlan2300 | 1/1/30 | reachable
----------------------------------------
Total Number Of IPv6 Neighbors Entries Listed: 2.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt;) or Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>

show ipv6 neighbors state
show ipv6 neighbors state {all | failed | incomplete | permanent | reachable | stale} [vsx-peer]

**Description**
Shows all IPv6 neighbor ARP (Address Resolution Protocol) cache entries, or those cache entries that are in the specified state.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows all ARP cache entries.</td>
</tr>
<tr>
<td>failed</td>
<td>Shows ARP cache entries that are in failed state. The neighbor might have been deleted. Set the neighbor to be unreachable.</td>
</tr>
<tr>
<td>incomplete</td>
<td>Shows ARP cache entries that are in incomplete state. An incomplete state means that address resolution is in progress and the link-layer address of the neighbor has not yet been determined. This means that a solicitation request was sent, and you are waiting for a solicitation reply or a timeout.</td>
</tr>
<tr>
<td>permanent</td>
<td>Shows ARP cache entries that are in permanent state.</td>
</tr>
<tr>
<td>reachable</td>
<td>Shows ARP cache entries that are in reachable state, meaning that the neighbor is known to have been reachable recently.</td>
</tr>
<tr>
<td>stale</td>
<td>Shows ARP cache entries that are in stale state. ARP cache entries are in the stale state if the elapsed time is in excess of the ARP timeout in seconds since the last positive confirmation that the forwarding path was functioning properly.</td>
</tr>
<tr>
<td>vsx-peer</td>
<td>Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.</td>
</tr>
</tbody>
</table>

**Example**

```
switch# show ipv6 neighbors state all
IPv6 Address     MAC        Port       Physical Port  State
---------------------------------------------------------------
100::2            48:0f:cf:af:1:cc  lal1      lal1            reachable
300::3            48:0f:cf:af:33:be  vlan3   1/4/20          reachable
fe80::4af:cf:feaf:1cc  48:0f:cf:af:1:cc  lal1      lal1            reachable
200::3            48:0f:cf:af:33:be  1/4/11   1/4/11          reachable

Total Number Of IPv6 Neighbors Entries Listed- 5.  
---------------------------------------------------------------
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>
### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>All platforms</td>
<td>Operator (&gt; or Manager (#)</td>
<td>Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (&gt; or #) only.</td>
</tr>
</tbody>
</table>
Network Load Balancing (NLB) is a load balancing technology for server clustering. NLB supports load sharing and redundancy among servers within a cluster. To implement fast failover, NLB requires that the switch forwards network traffic to one or all servers in the cluster. Each server filters out the unexpected traffic. For more information, see Configuring network infrastructure to support the NLB operation mode.

NLB is used to spread incoming requests across as many as 32 servers. Currently, NLB in AOS-CX supports only IGMP multicast mode. The IGMP multicast mode sends the packets out of the ports which connect to the cluster members. Assign a static multicast MAC address within the Internet Assigned Numbers Authority (IANA) range to the cluster’s virtual unicast IP address. The clustered servers send IGMP joins to the configured multicast cluster group. If IGMP snooping is enabled, the switch dynamically populates the IGMP snooping table with the clustered servers, which prevents unicast flooding.

**NLB commands**

**arp ipv4 mac**

```
arp ipv4 <IPv4-ADDR> mac <MAC-ADDR>
no arp ipv4 <IPv4-ADDR> mac <MAC-ADDR>
```

**Description**

Configures static ARP multicast on the interface.

The `no` form of this command removes the static ARP multicast configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IPv4-ADDR&gt;</code></td>
<td>Specifies cluster’s virtual IPv4 address.</td>
</tr>
<tr>
<td><code>&lt;MAC-ADDR&gt;</code></td>
<td>Specifies multicast MAC address in IANA format (xx:xx:xx:xx:xx) and non IANA format (xxxx.xxxxxx.xxxxx).</td>
</tr>
</tbody>
</table>

**Examples**

Configuring static ARP multicast on an interface:

```
switch(config)# vlan 10
switch(config-vlan-10)# no shutdown
switch(config-vlan-10)# ip igmp snooping enable
switch(config-vlan-10)# exit
switch(config)# interface vlan10
switch(config-if-vlan)# ip igmp enable
switch(config-if-vlan)# arp ipv4 10.1.30.254 mac 01:00:5e:7F:1E:FE
```

If your NLB Virtual IP address is 10.1.30.254, then the server will join the 239.255.30.254 IGMP group. This IGMP group is mapped to the destination MAC address of 01:00:5e:7F:1E:FE.
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Added NLB support for 6300 and 6400 Switch series.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>config-if</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td>and config-if-vlan</td>
<td></td>
</tr>
</tbody>
</table>

### show arp

#### Description
Displays the static ARP multicast information.

#### Examples
Displaying the static ARP multicast information:

```text
switch# show arp
IPv4 Address       MAC       Port  Physical Port  State
------------------  ---------  ------  ------------  -----
3.3.3.3            01:00:5e:00:00:02  1/1/1    permanent
2.2.2.2            01:00:5e:00:00:01   vlan10    permanent
Total Number Of ARP Entries Listed- 2.                                    
```

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Added NLB support for 6300 and 6400 Switch series.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

### Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300</td>
<td>Operator(&gt;) or Manager(+)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
<tr>
<td>6400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### show ip igmp snooping vlan group

#### Description

A command to display the IGMP snooping VLAN group configuration.

### Examples

Displaying IGMP snooping VLAN group configuration:

```text
show ip igmp snooping vlan <VLAN-ID> group IGMP-Group
```
Description
Displays multicast joins (members of the cluster) participating in the IGMP group.

Examples
Displaying multicast joins participating in the IGMP group:

```
switch# show ip igmp snooping vlan 10 group 239.255.30.254
```

```
VLAN ID : 10
VLAN Name : VLAN10

Group Address : 239.255.30.254
Last Reporter : 10.1.30.254
Group Type : Filter

<table>
<thead>
<tr>
<th>Port</th>
<th>Vers</th>
<th>Mode</th>
<th>Uptime</th>
<th>Expires</th>
<th>V1 Timer</th>
<th>V2 Timer</th>
<th>Sources Forwarded</th>
<th>Sources Blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/6</td>
<td>2</td>
<td>EXC</td>
<td>0m 21s</td>
<td>1m 12s</td>
<td>2m 48s</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.08</td>
<td>Added NLB support for 6300 and 6400 Switch series.</td>
</tr>
<tr>
<td>10.07 or earlier</td>
<td>--</td>
</tr>
</tbody>
</table>

Command Information

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Command context</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>6300 6400</td>
<td>Operator (&gt; or Manager (#)</td>
<td>Administrators or local user group members with execution rights for this command.</td>
</tr>
</tbody>
</table>
Chapter 14
Support and Other Resources

Accessing Aruba Support

<table>
<thead>
<tr>
<th>Support Services</th>
<th><a href="https://www.arubanetworks.com/support-services/">https://www.arubanetworks.com/support-services/</a></th>
</tr>
</thead>
</table>
| North America telephone | 1-800-943-4526 (US & Canada Toll-Free Number)  
+1-408-754-1200 (Primary - Toll Number)  
+1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working) |
| International telephone | https://www.arubanetworks.com/support-services/contact-support/ |

Be sure to collect the following information before contacting Support:
- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

<table>
<thead>
<tr>
<th>Site</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airheads social forums and Knowledge Base</td>
<td><a href="https://community.arubanetworks.com/">https://community.arubanetworks.com/</a></td>
</tr>
<tr>
<td>Software licensing</td>
<td><a href="https://lms.arubanetworks.com/">https://lms.arubanetworks.com/</a></td>
</tr>
<tr>
<td>End-of-Life information</td>
<td><a href="https://www.arubanetworks.com/support-services/end-of-life/">https://www.arubanetworks.com/support-services/end-of-life/</a></td>
</tr>
<tr>
<td>Aruba software and documentation</td>
<td><a href="https://asp.arubanetworks.com/downloads">https://asp.arubanetworks.com/downloads</a></td>
</tr>
</tbody>
</table>

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal
https://asp.arubanetworks.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

**My Networking**

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page: https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://asp.arubanetworks.com/notifications/subscriptions (requires an active Aruba Support Portal (ASP) account to manage subscriptions). Security notices are viewable without an ASP account.

**Warranty Information**

To view warranty information for your product, go to https://www.arubanetworks.com/support-services/product-warranties/.

**Regulatory Information**


**Additional regulatory information**

Aruba is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see https://www.arubanetworks.com/company/about-us/environmental-citizenship/.

**Documentation Feedback**

Aruba is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.