

AOS-CX 10.17 IP Services Guide

8100, 83xx, 93xx, 100xx Switch Series



**Hewlett Packard
Enterprise**

Published: November 2025

Version: 1

Copyright Information

© Copyright 2025 Hewlett Packard Enterprise Development LP.

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components 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, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.



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.

About this document	11
Applicable products	11
Latest version available online	11
Command syntax notation conventions	11
About the examples	12
Identifying switch ports and interfaces	13
IRDP	14
Configuring IRDP	15
IRDP commands	16
diag-dump irdp basic	16
ip irdp	17
ip irdp holdtime	18
ip irdp maxadvertinterval	19
ip irdp minadvertinterval	20
ip irdp preference	20
show ip irdp	21
IPv6 Router Advertisement	23
Configuring IPv6 RA	23
IPv6 RA scenario	25
IPv6 RA commands	26
ipv6 address <global-unicast-address>	26
ipv6 address autoconfig	26
ipv6 address link-local	27
ipv6 nd cache-limit	28
ipv6 nd dad attempts	29
ipv6 nd hop-limit	29
ipv6 nd mtu	30
ipv6 nd ns-interval	31
ipv6 nd prefix	31
ipv6 nd ra dns search-list	33
ipv6 nd ra dns server	34
ipv6 nd ra lifetime	35
ipv6 nd ra managed-config-flag	35
ipv6 nd ra max-interval	36
ipv6 nd ra min-interval	37
ipv6 nd ra other-config-flag	38
ipv6 nd ra reachable-time	39
ipv6 nd ra retrans-timer	39
ipv6 nd route	40
ipv6 nd router-preference	41
ipv6 nd suppress-ra	42
show ipv6 nd global traffic	43
show ipv6 nd interface	44
show ipv6 nd interface prefix	48
show ipv6 nd interface route	50
show ipv6 nd ra dns search-list	51
show ipv6 nd ra dns server	51

sFlow	53
sFlow agent	53
Configuring the sFlow agent	54
sFlow scenario	55
sFlow scenario 2	56
sFlow agent commands	59
clear sflow statistics	59
sflow	60
sflow agent-ip	61
sflow collector	62
sflow disable	63
sflow header-size	63
sflow max-datagram-size	64
sflow mode	64
sflow polling	66
sflow sampling	66
show sflow	67
DHCP	70
DHCP client	70
Protocol and feature details	70
Supported platform and standards	70
Configuration task list	71
Considerations and best practices	71
Use case	71
DHCP client commands	73
ip dhcp preferred-vlan	73
ip dhcp	74
ipv6 dhcp	75
ip dhcp option	77
show ip dhcp	78
show ipv6 dhcp	79
show ip dhcp preferred-vlan	80
DHCP relay agent	80
Supported platform and standards	80
Protocol and feature details	81
DHCPv4 relay agent	82
Configuring the DHCPv4 relay agent	83
Use Case	84
DHCPv4 relay commands	90
DHCPv6 relay agent	103
Configuring the DHCPv6 relay agent	104
Use Case	105
DHCP relay (IPv6) commands	108
Troubleshooting	116
One or more DHCP clients not getting IP address	116
DHCP server	117
Protocol and feature details	117
Supported platform and standards	118
Configuring a DHCPv4 server on a VRF	118
Configuring the DHCPv6 server on a VRF	120
DHCP server IPv4 commands	121
authoritative	121
bootp	122
clear dhcp-server leases	123
default-router	124

dhcp-server external-storage	125
dhcp-server vrf	126
disable	127
dns-server	128
domain-name	129
enable	130
lease	130
netbios-name-server	131
netbios-node-type	132
option	133
pool	135
range	136
show dhcp-server	137
static-bind	139
DHCP server IPv6 commands	140
authoritative	140
clear dhcpv6-server leases	141
dhcpv6-server external-storage	143
dhcpv6-server vrf	144
disable	145
dns-server	145
enable	146
lease	147
option	148
pool	149
range	150
show dhcpv6-server	151
static-bind	154
Troubleshooting	155
FAQ	156

DHCP snooping 159

Protocol details	160
Supported platform and standards	161
Configuring DHCPv4 and v6 snooping over VXLAN overlay	161
DHCPv4 Snooping Use case	162
DHCP snooping commands	164
clear dhcp-snooping binding	164
clear dhcp-snooping statistics	166
dhcp-snooping	166
dhcp-snooping (in config-vlan context)	167
dhcp-snooping allow-overwrite-binding	168
dhcp-snooping authorized-server	169
dhcp-snooping event-log client	170
dhcp-snooping external-storage	171
dhcp-snooping flash-storage	172
dhcp-snooping max-bindings	174
dhcp-snooping option 82	175
dhcp-snooping static-attributes	176
dhcp-snooping trust	177
dhcp-snooping tunnel vxlan trust	178
dhcp-snooping verify mac	179
show dhcp-snooping	180
show dhcp-snooping binding	182
show dhcp-snooping statistics	183
DHCPv6 snooping commands	185

clear dhcpv6-snooping binding	185
clear dhcpv6-snooping guard-policy statistics	186
clear dhcpv6-snooping statistics	187
dhcpv6-snooping	187
dhcpv6-snooping (in config-vlan context)	188
dhcpv6-snooping authorized-server	189
dhcpv6-snooping event-log client	190
dhcpv6-snooping external-storage	191
dhcpv6-snooping flash-storage	192
dhcpv6-snooping max-bindings	194
dhcpv6-snooping trust	195
dhcpv6-snooping tunnel vxlan trust	196
match server access-list	196
match client prefix-list	197
preference	198
show dhcpv6-snooping	199
show dhcpv6-snooping binding	201
dhcpv6-snooping guard-policy	202
show dhcpv6-snooping guard-policy	203
show dhcpv6-snooping guard-policy interface	204
show dhcpv6-snooping guard-policy vlan	205
show dhcpv6-snooping statistics	206
Troubleshooting	207

DHCP Options 210

DHCP options commands	210
http-proxy	210

ND snooping 213

Overview (applies to the 8325/8325H/8325P, 9300/9300S, and 10000 Switch Series)	213
Overview (applies to the 6300, 6400, 8100, and 8360 Switch Series)	213
Configuring ND snooping over VxLAN with IPv4 and IPv6 underlay	214
ND snooping commands	214
clear nd-snooping binding	214
clear nd-snooping ra-guard-policy statistics	216
clear nd-snooping statistics	216
diag-dump nd-snooping basic	217
nd-snooping	220
nd-snooping (in config-vlan context)	221
nd-snooping mac-check	222
nd-snooping prefix-list	223
nd-snooping max-bindings	223
nd-snooping nd-guard	224
nd-snooping ra-guard	225
nd-snooping ra-drop	226
nd-snooping trust	227
show nd-snooping	228
show nd-snooping binding	231
show nd-snooping prefix-list	231
show nd-snooping statistics	232
RA guard policy commands	234
hop limit	234
ipv6 nd-snooping ra-guard policy	235
managed-config-flag	236
match access-list	237
match prefix-list	238

nd-snooping ra-guard attach-policy	238
other-config-flag	240
router-preference	241
show nd-snooping ra-guard interface	242
show nd-snooping ra-guard policy	243
show nd-snooping ra-guard vlan	244
IPv6 destination guard	246
IPv6 destination guard commands	246
clear ipv6 destination-guard statistics vlan	246
ipv6 destination guard	247
show ipv6 destination-guard statistics vlan	247
show ipv6 destination-guard	248
IP Tunnels	250
VRF Aware GRE support	251
Example of VRF-aware GRE topology	252
IVRL using Static Route leaking	252
IVRL using Dynamic Route leaking via BGP	253
Configuring an IP tunnel	253
Creating a GRE tunnel for traversing a public network	254
Creating two GRE tunnels to different destination addresses	255
Creating an IPv6 in IPv4 tunnel for traversing a public network	258
Creating an IPv6 in IPv6 tunnel for traversing a public network	259
IP tunnels commands	260
description	260
destination ip	262
destination ipv6	263
interface tunnel	264
ip address	266
ipv6 address	267
ip mtu	268
show interface tunnel	270
show running-config interface tunnel	272
shutdown	273
source ip	274
source ipv6	275
ttl	276
transport vrf	278
vrf attach	278
IPsec Tunnel	281
IPsec tunnels commands	283
description	283
destination ip	283
interface tunnel	284
ip address	285
ip mtu	286
IPsec Tunnel backup route support	287
show capacities-status	287
show capacities-status tunneling	288
show interface tunnel	289
show interface tunnel brief	290
show running-config interface tunnel	291
show running-config current-context	291
source ip	292

vrf attach	293
IP Source Lockdown	295
IPv4 source lockdown commands	295
ipv4 source-binding	295
ipv4 source-lockdown	296
ipv4 source-lockdown hardware retry	297
show ipv4 source-binding	298
show ipv4 source-lockdown	299
IPv6 source lockdown commands	302
ipv6 source-binding	302
ipv6 source-lockdown	303
ipv6 source-lockdown hardware retry	304
show ipv6 source-binding	305
show ipv6 source-lockdown	306
Internet Control Message Protocol (ICMP)	310
ICMP message types	310
When ICMP messages are sent	310
ICMP redirect messages	311
When ICMP redirect messages are sent	311
ICMP commands	311
ip icmp redirect	311
ip icmp throttle	312
ip icmp unreachable	313
DNS	314
DNS client	314
Configuring the DNS client	314
Fully Qualified Domain Name Resolver	315
DNS client commands	316
ip dns domain-list	316
ip dns domain-name	317
ip dns fqdn-resolver force-refresh	318
ip dns fqdn-resolver refresh-interval	319
ip dns host	320
ip dns server address	321
show ip dns	322
show ip dns fqdn-resolver	324
show ip dns fqdn-resolver detail	325
show ip dns fqdn-resolver refresh-interval	327
ARP	329
Configuring proxy ARP	332
Configuring local proxy ARP	333
Configuring dynamic ARP inspection over VXLAN overlay	333
ARP commands	334
arp inspection	334
arp inspection trust	335
arp ip	335
arp process-grat-arp	336
clear arp	337
debug arp-security	339
ip local-proxy-arp	340
ip local-proxy-arp exclude <ip-address>	342
ipv6 local-proxy-nd	344

ipv6 local-proxy-nd exclude <ipv6-address>	345
ip proxy-arp	347
ipv6 neighbor mac	348
show arp	349
show arp inspection interface	350
show arp inspection statistics	351
show arp inspection vlan	352
show arp state	354
show arp summary	355
show arp timeout	356
show arp vlan	357
show arp vrf	358
show ipv6 neighbors	360
show ipv6 neighbors state	361
show ipv6 neighbors vlan	362
show tech arp-security	363
Network Load Balancing (NLB)	366
NLB commands	366
arp ip mac	366
show arp	367
show ip igmp snooping vlan group	368
Support and Other Resources	370
Accessing HPE Aruba Networking Support	370
Accessing Updates	371
Warranty Information	371
Regulatory Information	371
Documentation Feedback	371

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

Applicable products

This document applies to the following products:

- HPE Aruba Networking 8100 Switch Series (R9W94A, R9W95A, R9W96A, R9W97A)
- HPE Aruba Networking 8320 Switch Series (JL479A, JL579A, JL581A)
- HPE Aruba Networking 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)
- HPE Aruba Networking 8325H Switch Series (S4B20A, S4B21A, S4B22A, S4B23A, S2T42A, S2T46A, S2T47A, S2T48A)
- HPE Aruba Networking 8325P Switch Series (S0G12A, S4A48A)
- HPE Aruba Networking 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A, JL700C, JL701C, JL702C, JL703C, JL706C, JL707C, JL708C, JL709C, JL710C, JL711C, JL704C, JL705C, JL719C, JL718C, JL717C, JL720C, JL722C, JL721C)
- HPE Aruba Networking 9300 Switch Series (R9A29A, R9A30A, R8Z96A, S0F81A, S0F82A, S0F83A)
- HPE Aruba Networking 9300S Switch Series (S0F81A, S0F82A, S0F83A, S0F84A, S0F85A, S0F86A, S0F88A, S0F95A, S0F96A)
- HPE Aruba Networking 10000 Switch Series (R8P13A, R8P14A)

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

Convention	Usage
<code>example-text</code>	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 ([]).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: <ul style="list-style-type: none">▪ <code><example-text></code>▪ <code><example-text></code>	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: <ul style="list-style-type: none">▪ For output formats where italic text cannot be displayed, variables

Convention	Usage
<ul style="list-style-type: none"> ▪ <i>example-text</i> ▪ <i>example-text</i> 	<p>are enclosed in angle brackets (< >). Substitute the text—including the enclosing angle brackets—with an actual value.</p> <ul style="list-style-type: none"> ▪ 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.
	<p>Vertical bar. A logical OR that separates multiple items from which you can choose only one.</p> <p>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.</p>
{ }	Braces. Indicates that at least one of the enclosed items is required.
[]	Brackets. Indicates that the enclosed item or items are optional.
... or ...	<p>Ellipsis:</p> <ul style="list-style-type: none"> ▪ 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 HPE Aruba Networking 8xxx, 93xx, and 10xxx Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *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 the switch.



If using breakout cables, the port designation changes to x:y, where x is the physical port and y is the lane when split. For example, the logical interface 1/1/4:2 in software is associated with lane 2 on physical port 4 in slot 1 on member 1.

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.

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

```
switch(config-if)# ip irdp holdtime 5000
switch(config-if)# ip irdp maxadvertinterval 30
switch(config-if)# ip irdp minadvertinterval 25
switch(config-if)# ip irdp preference 25
```

IRDP commands

diag-dump irdp basic

```
diag-dump irdp basic
```

Description

Displays diagnostic information for IRDP.

Example

```
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
```

```
switch# diag-dump irdp basic
=====
[Start] Feature irdp Time : Thu Jan  7 04:46:25 2021
=====
-----
[Start] Daemon hpe-rdiscd
-----
Interface: vlan2 (state : Down)
rdisc ipv4 (enabled: 1, max:600, min:450, hold:1800, pref:0, isBcast:0)
No advertisable IPv4 addresses on the interface
Interface: vlan1 (state : Down)
rdisc ipv4 (enabled: 0, max:600, min:450, hold:1800, pref:0, isBcast:0)
No advertisable IPv4 addresses on the interface
-----
[End] Daemon hpe-rdiscd
-----
```

```
=====
[End] Feature irdp
=====
Diagnostic-dump captured for feature irdp
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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.

ip irdp

```
ip irdp [broadcast | multicast]
no ip irdp
```

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.

Parameter	Description
<code>broadcast</code>	Advertisements are sent as broadcast packets to IP address 255.255.255.255.
<code>multicast</code>	Advertisements are sent as multicast packets to the multicast group with IP address 24.0.0.1. Default.

Examples

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

Release	Modification
10.07 or earlier	--

Command Information

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

ip irdp holdtime

```
ip irdp holdtime <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.

Parameter	Description
<TIME>	Specifies the lifetime of router advertisements sent from this interface. Range: 4 to 9000 seconds. Default: 1800 seconds.

Example

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

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
<TIME>	Specifies the maximum time allowed between the sending of unsolicited router advertisements. Range: 4 to 1800 seconds. Default: 600 seconds.

Example

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

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
<TIME>	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).

Example

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

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
<code><LEVEL></code>	Specifies the IRDP preference level. Range: -2147483648 to 2147483647. Default: 0.

Example

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-if</code>	Administrators or local user group members with execution rights for this command.

show ip irdp

```
show ip irdp [vsx-peer]
```

Description

Displays IRDP configuration settings.

Parameter	Description
<code><location></code>	Specifies one of these values: <ul style="list-style-type: none">▪ <code><FQDN></code>: a fully qualified domain name.▪ <code><IPv4></code>: an IPv4 address.▪ <code><IPv6></code>: 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

```
switch# show ip irdp
```

```
ICMP Router Discovery Protocol
```

Interface	Status	Advertising Address	Minimum Interval	Maximum Interval	Holdtime	Preference
1/1/1	Enabled	multicast	6	8	10	10
1/1/2	Disabled	multicast	450	600	1800	0
1/1/3	Enabled	broadcast	450	600	1800	115

```
switch# sh ip irdp
```

```
ICMP Router Discovery Protocol
```

Interface	Status	Advertising Address	Minimum Interval	Maximum Interval	Holdtime	Preference
vlan1	Disabled	multicast	450	600	1800	0
bridge_normal	Disabled	multicast	450	600	1800	0

Command History

Release

Modification

10.07 or earlier

--

Command Information

Platforms

Command context

Authority

All platforms

Manager (#)

Administrators or local user group members with execution rights for this command.

Chapter 3

IPv6 Router Advertisement

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).

M flag	O flag	Description
0	0	Indicates that no information is available via DHCPv6.
0	1	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.
1	0	Indicates that addresses are available via Dynamic Host Configuration Protocol (DHCPv6).
1	1	If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.

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:

IPv6 RA setting	Default value	Command to change it
Number of neighbor solicitations to be sent when performing DAD.	1	<code>ipv6 nd dad attempts</code>
Number of neighbor entries in the ND cache.	131072	<code>ipv6 nd cache-limit</code>

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

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

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:
```

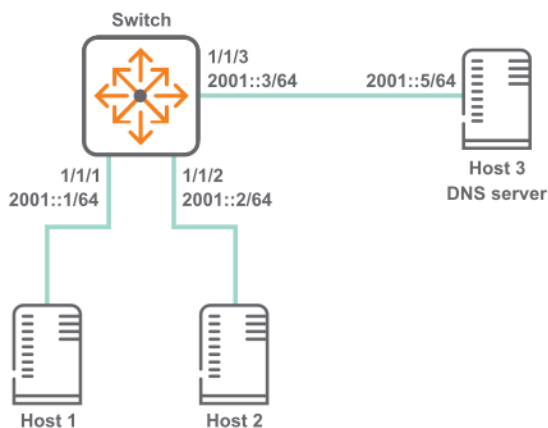
```

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:



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

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

Enabling unicast autoconfiguring:

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

Disabling unicast autoconfiguring:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-if</code>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (<code>></code>) only.

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.

Parameter	Description
<IPV6-ADDR>	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 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55 .
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Example

Enabling IPv6 link-local on the interface:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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.

Parameter	Description
<CACHELIMIT>	Specifies the neighbor cache entries limit. Range: 1-131072. Default: 131072.

Examples

Setting the cache limit to 20.

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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. If the active gateway is configured with the same IP as an SVI IP, then IPv6 DAD cannot be configured.

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

Parameter	Description
dad attempts <NUM-ATTEMPTS>	Specifies the number of neighbor solicitations to send. Range: 0-15. Default: 1.

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
hop-limit <HOPLIMIT>	Specifies the hop limit. Range: 0-255. Default: 64.

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd mtu

```
ipv6 nd mtu <MTU-VALUE>
no 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
<MTU-VALUE>	Specifies the MTU size. Range: 1280-65535 bytes. Default: 1500 bytes.

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd ns-interval

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

Description

Configures the ND time in milliseconds between DAD neighbor solicitations sent for an unresolved destination. Increase the ns-interval time if the network is slow or if there are persistent retry failures. If the active gateway is configured with the same IP as an SVI IP, then IPv6 DAD cannot be configured. The **no** form of this command sets the ns-interval to the default value.

Parameter	Description
<TIME>	Specifies the neighbor solicitation interval. Range: 1000-3600000 milliseconds. Default: 1000 milliseconds.

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd prefix

```
ipv6 nd prefix <IPV6-ADDR>/<PREFIX-LEN>
    [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	Description
<IPV6-ADDR>/<PREFIX-LEN>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X/M
default	Specifies apply configuration to all on-link prefixes that are not individually set by the ipv6 ra prefix <IPV6-ADDR>/<PREFIX-LEN> 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.
no-advertise	Specifies do not advertise prefix in RA.
valid <LIFETIME-VALUE>	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.
preferred <LIFETIME-VALUE>	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.
no-autoconfig	Specifies do not use prefix for autoconfiguration.
no-onlink	Specifies do not use prefix for onlink determination.

Examples

```
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

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
<DOMAIN-NAME>	Specifies the domain names for DNS queries.
lifetime <TIME>	Specifies lifetime in seconds. Range: 4-4294967295 seconds. Default: 1800 seconds.

Usage

- DNSSL contains the domain names of DNS suffixes or IPv6 hosts to append to short, unqualified domain names for DNS queries.
- Multiple DNS domain names can be added to the DNSSL by using the command repeatedly.
- A maximum of eight server addresses are allowed.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns search-list test.com lifetime 500
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd ra dns server

```
ipv6 nd ra dns server <IPV6-ADDR> [lifetime <TIME>]  
no ipv6 nd ra dns server <IPV6-ADDR>
```

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 zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55 .
lifetime <TIME>	Specifies IPv6 DNS server lifetime in seconds. Range: 4-4294967295 seconds. Default: 1800 seconds.

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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
<TIME>	Specifies lifetime in seconds of a default router. A setting of 0 for default router lifetime in an RA indicates that the routing switch is not a default router on the interface. Range: 0-9000 seconds. Default: 1800 seconds.

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd ra managed-config-flag

```
ipv6 nd ra managed-config-flag
no 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.

M flag	O flag	Description
0	0	Indicates that no information is available via DHCPv6.
0	1	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.
1	0	Indicates that addresses are available via Dynamic Host Configuration Protocol (DHCPv6).
1	1	If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
<TIME>	Specifies the maximum advertisement time in seconds. Range: 4-1800. Default: 600 seconds.

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
<TIME>	Specifies a minimum advertisement time in seconds. Range: 3-1350. Default: 200 seconds.

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd ra other-config-flag

```
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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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 occur, or in a "slow" (WAN) network. The **no** form of this command sets the value to the default of 0.

Parameter	Description
<TIME>	Specifies the retransmit timer value in milliseconds. Range: 0 - 4294967295 milliseconds. Default: 0 (Use locally configured NS-interval).

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd route

```
ipv6 nd route <IPV6-ADDR>/<PREFIX-LEN> [no-advertise | lifetime {<SECONDS> | infinite} | preference {low | medium | high}]
no ipv6 nd route <IPV6-ADDR>/<PREFIX-LEN> [no-advertise | lifetime {<SECONDS> | infinite} | preference {low | medium | high}]
```

Description

Configures the routing switch to include the routing information in the RAs transmitted on the interface. The routing switch includes the route information in the RA packets only if the configured routes are present in the routing table. After receiving the RA packets carrying the route information, the IPv6 host updates its routing table. The hosts lookup their routing table and selects the best possible route to forward packets.

The **no** form of this command removes the settings for including the routing information in the RA packets.

Parameter	Description
<IPV6-ADDR>/<PREFIX-LEN>	Specifies the IPv6 route prefix to advertise in RA. Format: X:X::X/M
no-advertise	Specifies to not advertise the route information.
lifetime {<SECONDS> infinite}	Specifies the duration in seconds that the route is valid for the route determination. If this parameter is configured with 0 , the route becomes invalid. Default: 1800 . Range: 0-4294967295 .
preference {low medium high}	Specifies the preference for the hosts to choose the router associated with the route over other routers when multiple identical route prefixes from different routers are received. Default: medium

Examples

Configuring routing information on interface **1/1/1**.

```
switch(config)# int 1/1/1
switch(config-if)# ipv6 nd route 1::1/64 lifetime 200 preference high
```

Command History

Release	Modification
10.10	Command introduced

Command Information

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

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.

Parameter	Description
high	Sets DRP to high.
medium	Sets DRP to medium. Default.

Parameter	Description
low	Sets DRP to low.

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 nd suppress-ra

```
ipv6 nd suppress-ra [<SUPPRESS-OPTION>]
no ipv6 nd ra supress-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.

Parameter	Description
suppress-ra [<SUPPRESS-OPTION>]	Specifies suppressing RA transmissions. Entering suppress-ra without any options, suppresses all RA messages (default). Or you can enter one of the following options.
dnssl	Specifies suppressing DNSSL options in RA messages.
mtu	Specifies suppressing MTU options in RA messages.
rdnss	Specifies suppressing RDNSS options in RA messages.

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ipv6 nd global traffic

```
show ipv6 nd global traffic [vsx-peer]
```

Description

Displays IPV6 Neighbor Discovery traffic details on a device.

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

```
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

Release	Modification
10.07 or earlier	--

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.

Parameter	Description
<IF-NAME>	Displays information about the specified IPv6 enabled interface.
all-vrfs	Displays information about interfaces in all VRFs.
vrf <VRF-NAME>	Displays information about interfaces in a particular VRF. Or, if <VRF-NAME> is not specified, information for the default VRF is displayed.
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

Two examples 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: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

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

switch# **show ipv6 nd interface all-vrfs**

List of IPv6 Interfaces for VRF default

Interface vlan2 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: 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 vlan3 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

```

```

switch# show ipv6 nd interface vlan 2
Interface vlan2 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:cfff: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
```

```
switch# show ipv6 nd interface

List of IPv6 Interfaces for VRF default
Interface vlan2 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: 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

Release	Modification
10.07 or earlier	--

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 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.

Parameter	Description
all-vrfs	Shows prefix information for all VRFs.
vrf <VRF-NAME>	Name of a VRF.
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 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
```

```
switch# show ipv6 nd interface prefix

List of IPv6 Interfaces for VRF default
List of IPv6 Prefix advertised on vlan2
  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
```

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

List of IPv6 Interfaces for VRF red
List of IPv6 Prefix advertised on vlan3
  Prefix : 2001::/64
  Enabled : Yes
  Validlife time : 2592000
  Preferred lifetime : 604800
  On-link : Yes
  Autonomous : Yes
```

Command History

Release	Modification
10.07 or earlier	--

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 route

```
show ipv6 nd interface route [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays route information of all interfaces in the default VRF.

Parameter	Description
all-vrfs	Displays information about interfaces in all VRFs.
vrf <VRF-NAME>	Displays information about interfaces in a particular VRF. Or, if <VRF-NAME> is not specified, displays information for the default VRF.

Examples

Showing routing information for interface **1/1/1** in the default VRF:

```
switch# show ipv6 nd interface route

List of IPv6 Interfaces for VRF default
List of IPv6 Routes advertised on 1/1/1
Route : 1::/64
Enabled : Yes
Route lifetime : 200
Route preference : high
```

Showing routing information for interface **1/1/1** in VRF red:

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

List of IPv6 Interfaces for VRF red
List of IPv6 Routes advertised on 1/1/2
Route : 2::/64
Enabled : No
Route lifetime : 1800
Route preference : low
```

Command History

Release	Modification
10.10	Command introduced

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 ra dns search-list

```
show ipv6 nd ra dns search-list [vsx-peer]
```

Description

Displays domain name information on all interfaces.

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

```
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

Release	Modification
10.07 or earlier	--

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 ra dns server

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

Description

Displays DNS server information on all interfaces.

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

```
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

Release	Modification
10.07 or earlier	--

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.

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.



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 on the default VRF and non-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.
- sflow sampling mode: Ingress
- Sampling rate: 4096.
- Polling interval: 30 seconds.
- Header size: 128 bytes.
- Max datagram size: 1400 bytes.

Supported features

- Global sampling rate
- Global sampling mode (Ingress, Egress, and Both)

- 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)
- Egress sampling for all forwarded traffic (L2, L3)
- Enable/Disable sFlow per interface
- Support for three remote collectors
- A collector can be defined on the default and 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)



For the 4100i, 6000, and 6100 switch series, collector can be defined only on the default VRF. Also, there is no sampling of egress traffic.

Limitations

- Sampling rate cannot be set per interface (global only)
- sFlow is not configurable through SNMP.
- sFlow egress global counters will increase for broadcast, unknown-unicast, & multicast (BUM) traffic. However, the interface counters will not increase because it is flooded traffic. The output port in the sFlow sampled packet for BUM traffic will be 0x80000000.
- When the sampling mode is configured as both, the ingress and egress packets may not be sampled in equal proportions.
- The sampled packet count will not match the configured value when sFlow is configured but it will converge after sampling around 500 packets.
- sFlow egress sampling is supported only on certain types of CPU generated traffic.
- The sFlow egress sampling on VxLAN tunnel is not supported and there will not be any indication to the user when configuring sFlow.

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:

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

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

Example

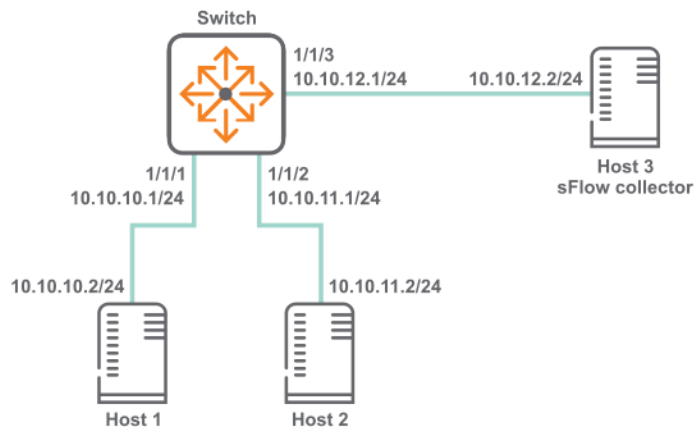
This example creates the following configuration:

- 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:



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 **10.10.10.1/24**.  

```
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 **10.10.11.1/24**.  

```
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# ip address 10.10.11.1/24
switch(config)# quit
```
  7. Configure interface **1/1/3** with IP address **10.10.12.1/24**.  

```
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

The following example is only applicable for the 8100, 8360 series switch

```
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:

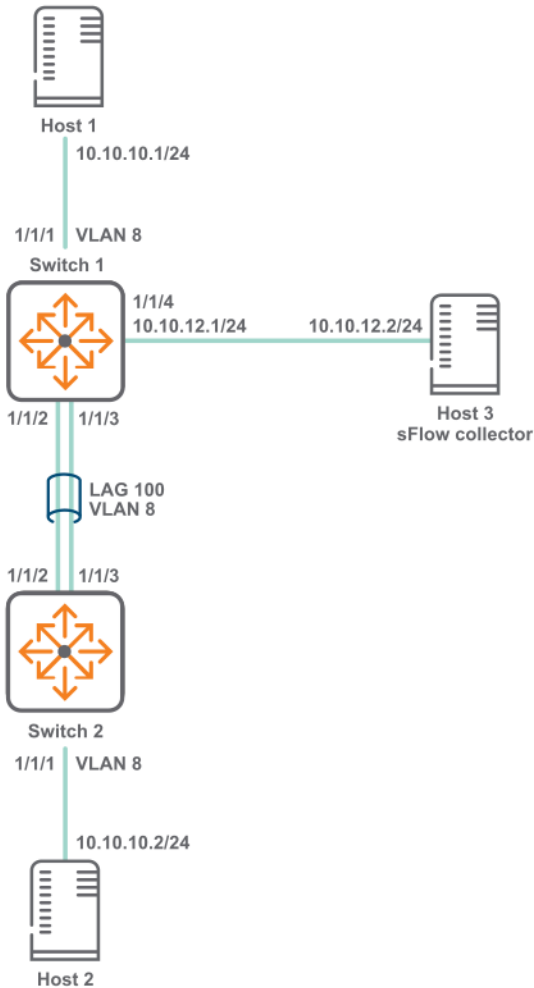
lag100

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:



## 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)# no routing
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.

The following example is only applicable for the 8100, 8360 Series switch

```
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)# no routing
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
switch(config-if)# no shutdown
switch(config-lag-if)# no routing
switch(config-if)# vlan access 8
```
- d. 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)-if# interface 1/1/3
switch(config-if)# no shutdown
switch(config-if)# lag 100
switch(config-if)# exit
```

## 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.

| Parameter                  | Description                                       |
|----------------------------|---------------------------------------------------|
| global                     | Specifies all interfaces on the switch.           |
| interface <INTERFACE-NAME> | Specifies the name of an interface on the switch. |

#### 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

#### Command Information

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

## sflow

```
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

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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| All platforms | config<br>config-if | Administrators or local user group members with execution rights for this command. |

## sflow agent-ip

```
sflow agent-ip <IP-ADDR>
no 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 | Description                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP-ADDR> | Specifies an IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255, or IPv6 format ( <b>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</b> ), where <b>x</b> 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 an sFlow collector. |

### 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
```

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

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

## 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.

| Parameter           | Description                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| collector <IP-ADDR> | Specifies the IP address of a collector in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255, or IPv6 format ( <b>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</b> ), where <b>x</b> is a hexadecimal number from 0 to F. |
| port <PORT>         | Specifies the UDP port on which to send information to the sFlow collector. Range: 0 to 65536. Default: 6343.                                                                                                                                       |
| vrf <VRF>           | 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 ( <b>default</b> ) is used.                                                                   |

### 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

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

# 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

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

# 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.

| Parameter          | Description                                                               |
|--------------------|---------------------------------------------------------------------------|
| header-size <SIZE> | Specifies the sFlow header size in bytes. Range: 64 to 256. Default: 128. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

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

## 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.

| Parameter                | Description                                                                    |
|--------------------------|--------------------------------------------------------------------------------|
| max-datagram-size <SIZE> | Specifies the maximum datagram size in bytes. Range: 1 to 9000. Default: 1400. |

### 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## 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.

| Parameter | Description                              |
|-----------|------------------------------------------|
| ingress   | Samples only ingress traffic.            |
| egress    | Samples only egress traffic.             |
| both      | Samples both ingress and egress traffic. |

## Examples

Setting the sFlow mode to only sample egress traffic:

```
switch# configure terminal
switch(config)# sflow mode egress
```

Setting the sFlow mode to only sample ingress traffic:

```
switch# configure terminal
switch(config)# sflow mode ingress
```

Setting the sFlow mode to sample both sample ingress and egress traffic:

```
switch# configure terminal
switch(config)# sflow mode both
```

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

| Release          | Modification                                                      |
|------------------|-------------------------------------------------------------------|
| 10.10            | Command enabled on the 8320, 8325, 9300, and 10000 Switch Series. |
| 10.07 or earlier | --                                                                |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## sflow polling

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

### 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.

| Parameter  | Description                                                                |
|------------|----------------------------------------------------------------------------|
| <INTERVAL> | Specifies the polling interval in seconds. Range: 10 to 3600. Default: 30. |

### 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

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

## 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.

| Parameter                          | Description                                                         |
|------------------------------------|---------------------------------------------------------------------|
| <code>sampling &lt;RATE&gt;</code> | Specifies the sampling rate. Range: 1 to 1000000000. Default: 4096. |

## Examples

Setting the sampling rate to **5000**:

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

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config</code> | Administrators or local user group members with execution rights for this command. |

## show sflow

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

## Description

Shows sFlow configuration settings and statistics for all interfaces, or for a specific interface. It also displays the current status of sFlow on the device and reports any errors that require attention.



If sFlow is enabled on the interfaces associated with a lag interface, then the interfaces will not be shown as separate entries under sFlow enabled on Interface in the output. Only the associated lag interface will have an entry in the column.

| Parameter                  | Description                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface <INTERFACE-NAME> | Specifies the name of an interface on the switch.                                                                                                                                                                                |
| 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 sFlow information for all interfaces:

```
switch# show sflow
sFlow Global Configuration

sFlow enabled
Collector IP/Port/Vrf 10.0.0.2/6343/default
 10.0.0.3/6400/default
Agent Address 10.0.0.1
Sampling Rate 1024
Polling Interval 30
Header Size 128
Max Datagram Size 1400
Sampling Mode ingress

sFlow Status

Running - Yes

sFlow enabled on Interfaces:

1/1/2
1/1/3
lag100

sFlow Statistics

Number of Ingress Samples 200
Number of Egress Samples 120
```

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
```

Showing sFlow information for interface **lag 10**:

```
switch# show sflow interface lag 10
sFlow Configuration - Interface lag10

sFlow enabled
Sampling Rate 4096
Sampling Mode both
Number of Ingress Samples 0
Number of Egress Samples 0
sFlow Sampling Status error

Sampling Status on LAG members

Intf 1/1/2 no agent
Intf 1/1/3 no agent
```

## Command History

| Release          | Modification                                                                                                                                                                           |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.10            | Command output updated to display <code>Sampling Mode</code> , <b>Number of Ingress Samples</b> , and <b>Number of Egress Samples</b> for 8320, 8325, 9300, and 10000 series switches. |
| 10.07 or earlier | --                                                                                                                                                                                     |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

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 as 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 the management interface allowing it to automatically obtain an IP address from a DHCP server on the network to which it is connected.

## Protocol and feature details

DHCP Client is supported on IPv4 and IPv6 (for IPv6 it is supported only on management VRF).

The IP DHCP assignment with HPE Aruba Networking AOS-CX switch is to allow the following:

- IP switch assignment.
- Managing the initial IP access to the switch.
- Prepare for Zero Touch Provisioning (ZTP) with HPE Aruba Networking Central.
- Prepare for Zero Touch Provisioning (ZTP) by using DHCP options along with a TFTP server.




---

Zero Touch Provisioning (ZTP) is only supported for IPv4 in HPE Aruba Networking Central

---

## Supported platform and standards

The following table lists the supported VLANs and ports for the AOS-CX Switch.

**Table 1:** Supported VLAN and Ports for DHCP

| Platform | VLAN 1 | Any Other VLAN | In band Port | Management VRF port |
|----------|--------|----------------|--------------|---------------------|
| 4100i    | Yes    | Yes            | Yes          | N/A                 |

| Platform               | VLAN 1 | Any Other VLAN | In band Port | Management VRF port |
|------------------------|--------|----------------|--------------|---------------------|
| 5400                   | Yes    | Yes            | Yes          | Yes                 |
| 6000                   | Yes    | Yes            | Yes          | N/A                 |
| 6100                   | Yes    | Yes            | Yes          | N/A                 |
| 6200                   | Yes    | Yes            | Yes          | Yes                 |
| 6300<br>6300L          | Yes    | Yes            | Yes          | Yes                 |
| 6400                   | Yes    | Yes            | Yes          | Yes                 |
| 8320                   | No     | No             | No           | Yes                 |
| 8325<br>8325H<br>8325P | No     | No             | No           | Yes                 |
| 8360                   | No     | No             | No           | Yes                 |
| 8400                   | No     | No             | No           | Yes                 |
| 9300<br>9300S          | No     | No             | No           | Yes                 |
| 10000                  | No     | No             | No           | Yes                 |

## Configuration task list

To run the DHCP Client do the following:

- Enter the interface VLAN or Management VRF context
- Enable DHCP

## Considerations and best practices

The IP DHCP can only be configured on one VLAN per switch.

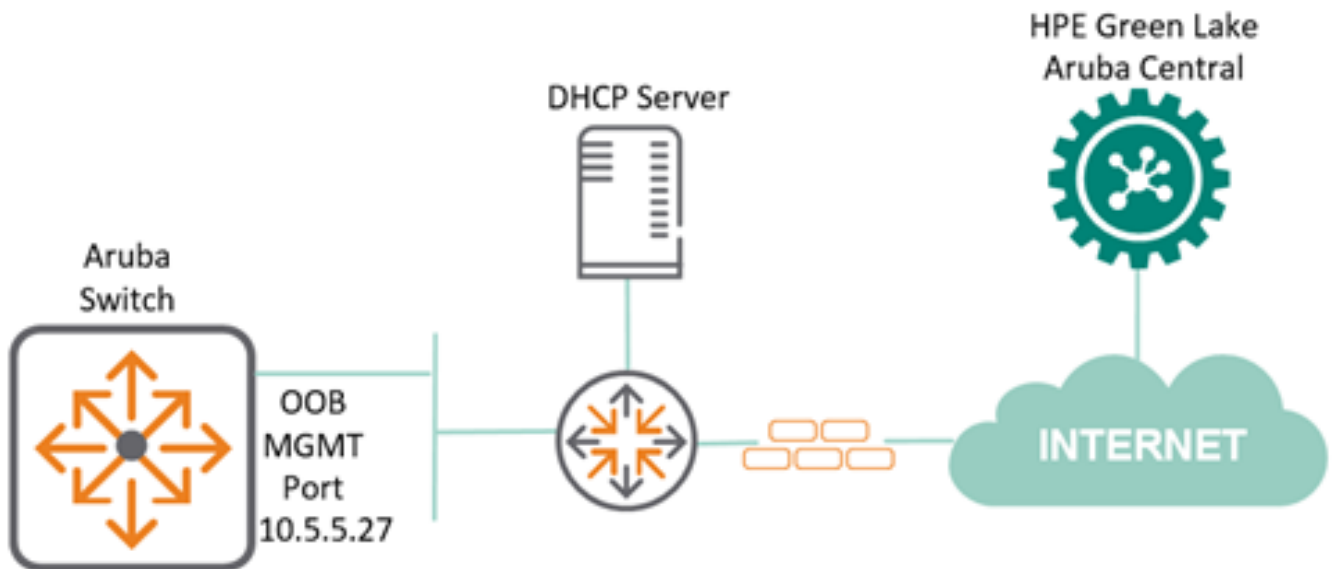
If an OOB Management port is available, you can configure the DHCP service simultaneously for the VLAN IN Band and the OOB Management port. When both the IN Band data port and the OOB Management port receive a DHCP address, then the DHCP address received on the OOBM port is preferred over the IN Band data port for ZTP.

## Use case

IP DHCP assignment with HPE Aruba Networking AOS-CX switches is to allow IP switch assignment and Zero Touch Provisioning using HPE Aruba Networking Central, as shown below.

In the following DHCP client scenario the OOB Management port is in use. The IN Band data ports can also be used for Zero Touch Provisioning (ZTP).

For more information related to the supported ports for the different switches, see [Supported platform and standards](#).



1. Switch configuration from factory on OOB Management port.

```
switch#
!
interface mgmt
 no shutdown
 ip dhcp
!
```

2. OOB Management port gets assigned with an IPv4 address 10.5.5.27 from DHCP server.

```
switch# show interface mgmt
Address Mode : dhcp
Admin State : up
Link State : up
Mac Address : 88:3a:30:9a:39:01
IPv4 address/subnet-mask : 10.5.5.27/24
Default gateway IPv4 : 10.5.5.254
IPv6 address/prefix : 2a00:23c5:ac8a:3e01:8a3a:30ff:fe9a:3901/64
IPv6 link local address/prefix: fe80::8a3a:30ff:fe9a:3901/64
Default gateway IPv6 : fe80::f286:20ff:fe0b:fe5
Primary Nameserver : 10.5.19.69
Secondary Nameserver : 10.5.19.79
Tertiary Nameserver : 8.8.4.4
```

The following output shows a switch connected to HPE Aruba Networking Central allocated with an IP address of 10.5.5.27 on its OOB MGMT port by a DHCP server. Based on its designated configuration in the public cloud, the switch can get its configuration parameters directly from HPE Aruba Networking Central.

```

switch# show hpe_anw-central
 Central admin state : enabled
 Central location : device-prod2-
d2.central.arubanetworks.com
 VRF for connection : mgmt
 Central connection status : connected
 Central source : activate
 Central source connection status : connected
 Central source last connected on : Wed Sep 22 18:39:05 UTC 2021
 System time synchronized from Activate : True
 Activate Server URL : devices-v2.arubanetworks.com
 CLI location : N/A
 CLI VRF : N/A
 Source IP : 10.5.5.27
 Source IP Overridden : False
 Central support mode : disabled

```

## DHCP client commands

### ip dhcp preferred-vlan

```

ip dhcp preferred-vlan <VLAN-ID> [vrf <VRF-NAME>]
no ip dhcp preferred-vlan vlan <VLAN-ID> [vrf <VRF-NAME>]

```

#### Description

Specifies the preferred VLAN for DHCP client options, including DNS, NTP, and Default Gateway. The preferred VLAN is the VLAN used to select DHCP client options within a specified VRF when multiple VLANs have DHCP client enabled in the same VRF. If no VRF is specified, the configuration applies to the default VRF. In cases where the preferred VLAN is not explicitly configured, the lowest VLAN with DHCP client enabled will be automatically selected.

The **no** form of the command removes the preferred VLAN configuration and restores the default behavior.

| Parameter  | Description                                                         |
|------------|---------------------------------------------------------------------|
| <VLAN-ID>  | VLAN ID to set as preferred VLAN. VLAN identifier range: 1 to 4094. |
| <VRF-NAME> | Specifies the VRF in which the preferred VLAN should be configured. |

#### General Considerations

If the preferred VLAN configuration status is not *success*, the DHCP client-enabled VLAN with the lowest VLAN ID will be used for DHCP attribute selection.

Use the command `show ip dhcp preferred-vlan` to check the configuration status.

The preferred or lowest VLAN will be inactive in the following scenarios:

- When the DHCP interface is in a shutdown state and corresponds to the preferred or lowest VLAN ID.
- When a static IP is configured on an interface that also has DHCP enabled — the static IP takes precedence over DHCP.
- When DHCP attributes are not received from the server on the preferred or lowest VLAN.

## Examples

Selecting VLAN 1 as the preferred VLAN:

```
switch(config)# ip dhcp preferred-vlan 1
```

Selecting VLAN 10 as the preferred VLAN with VRF name:

```
switch(config)# ip dhcp preferred-vlan 10 vrf red
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

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

## ip dhcp

```
ip dhcp
no ip dhcp
```

## Description

Enables the DHCP client on the management interface or any interface VLAN to automatically obtain an IP address from a DHCP server on the network. By default, the DHCP client is enabled on the management interface and VLAN 1.

The **no** form of the command disables DHCP mode and is supported only on interface VLANs; it is not supported on the management interface.

## Examples

Enabling the DHCP client on the management interface:

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

Enabling the DHCP client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp
switch(config-if-vlan)# no shutdown
```

Disabling the DHCP client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip dhcp
```

Enabling the DHCP client on the interface vlan 4 under non-default VRF:

```
switch(config)# interface vlan 4
switch(config-if-vlan)# vrf attach red
switch(config-if-vlan)# ip dhcp
```

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



---

DHCP client can be enabled on one or more user VLANs.

---

## General Limitations

1. ZTP (Zero Touch Provisioning) options from a DHCP server are only supported on VLAN 1. These options will be ignored if received on any other VLAN.
2. CoP and HTTPS-proxy DHCP options should be received on only one DHCP client-enabled VLAN. If multiple VLANs receive the same option, the selection of the VLAN from which the options are applied is non-deterministic. Therefore, configuring multiple VLANs to receive these options is not recommended.
3. It is recommended to limit the number of DHCP client VLANs in a system to 32. This total includes both DHCPv4 and DHCPv6 client instances.
4. The `ip dhcp option broadcast-flag` configuration must be enabled to successfully obtain DHCP IP addresses across multiple VLANs when the default gateway route is present.

## Command History

| Release          | Modification                                                                        |
|------------------|-------------------------------------------------------------------------------------|
| 10.17            | Support enabled on one or more user VLANs.                                          |
| 10.16.1000       | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.07 or earlier | --                                                                                  |

## Command Information

| Platforms     | Command context                                            | Authority                                                                          |
|---------------|------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config-if-mgmt</code><br><code>config-if-vlan</code> | Administrators or local user group members with execution rights for this command. |

### ipv6 dhcp

```
ipv6 dhcp
no ipv6 dhcp
```

### Description

Configure to enable DHCPv6 mode on a VLAN. In DHCPv6 Mode, the VLAN will get a DHCP-Server allocated IPv6 address along with DNS and NTP attributes.

The **no** form of the command disables DHCP mode and is supported only on interface VLANs; it is not supported on the management interface.



---

ZTPv6 attributes are included in the request packet, but they are not utilized by ZTP on the data port. Currently, ZTPv6 attributes are only supported on the management port. Also, IPv6 addresses assigned through DHCPv6 only support a /64 prefix.

---

## Examples

Enabling the DHCPv6 client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 dhcp
```

Enabling the DHCPv6 on two VLANs:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 dhcp

switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 dhcp
```

Enabling the DHCPv6 client on the interface vlan 4 under non-default VRF:

```
switch(config)# interface vlan 4
switch(config-if-vlan)# vrf attach red
switch(config-if-vlan)# ipv6 dhcp
```

Disabling the DHCPv6 client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 dhcp
```

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

## General Limitations

1. ZTP (Zero Touch Provisioning) options from a DHCP server are only supported on VLAN 1. These options will be ignored if received on any other VLAN.
2. CoP and HTTPS-proxy DHCP options should be received on only one DHCP client-enabled VLAN. If multiple VLANs receive the same option, the selection of the VLAN from which the options are applied is non-deterministic. Therefore, configuring multiple VLANs to receive these options is not recommended.
3. It is recommended to limit the number of DHCP client VLANs in a system to 32. This total includes both DHCPv4 and DHCPv6 client instances.
4. The `ip dhcp option broadcast-flag` configuration must be enabled to successfully obtain DHCP IP addresses across multiple VLANs when the default gateway route is present.

## Command History

| Release    | Modification                                                                        |
|------------|-------------------------------------------------------------------------------------|
| 10.17      | Support added for DHCPv6 on multiple VLANs.                                         |
| 10.16.1000 | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.15      | Command was introduced.                                                             |

## Command Information

| Platforms     | Command context                  | Authority                                                                          |
|---------------|----------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if-mgmt<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## ip dhcp option

```
ip dhcp option [host-name | broadcast-flag]
no ip dhcp option[host-name | broadcast-flag]
```

## Description

This command enables the DHCP client host name and broadcast flag globally.

If the **ip dhcp option broadcast-flag** command is enabled, then the DHCP offer and ack packets in the DHCP requests will be treated as broadcast packets. These packets will not be forwarded due to the presence of a default static route.

The **no** form of this command globally disables the host name and DHCP client broadcast flag options.



The **ip dhcp option broadcast-flag** command should be configured before configuring the **ip dhcp** command.

## Example

Enabling the DHCP client broadcast flag globally:

```
switch(config)# ip dhcp option
broadcast-flag DHCP Client broadcast-flag option (Default:disabled)
host-name DHCP Client hostname option
switch(config)# ip dhcp option
% Command incomplete.
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp
switch(config-if-vlan)# ip dhcp op
% There is no matched command.
switch(config-if-vlan)# ip dhcp op
Invalid input: ip
switch(config-if-vlan)#
```

Enabling the DHCP client host name globally:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp option host-name
```

Disabling the DHCP client broadcast flag globally:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip dhcp option broadcast-flag
```

Disabling the DHCP client host name globally:

```
switch(config)# ip dhcp option
broadcast-flag DHCP Client broadcast-flag option (Default:disabled)
host-name DHCP Client hostname option
switch(config)# ip dhcp option
% Command incomplete.
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp
switch(config-if-vlan)# no ip dhcp option host-name
% There is no matched command.
switch(config-if-vlan)# ip dhcp op
Invalid input: ip
switch(config-if-vlan)#
```

## Command History

| Release    | Modification                                                                        |
|------------|-------------------------------------------------------------------------------------|
| 10.16.1000 | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.13.1000 | Command Introduced                                                                  |

## Command Information

| Platforms     | Command context                  | Authority                                                                          |
|---------------|----------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if-mgmt<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## show ip dhcp

```
show ip dhcp
```

## Description

Displays DHCP IPv4 information on the ports.

## Examples

Displaying the DHCP IPv4 information on the ports:

```
switch# show ip dhcp
DHCP Options: Broadcast-flag, Hostname

INTERFACE-NAME ADDRESS DEFAULT_GATEWAY DOMAIN_NAME VRF DNS-SERVERS

vlan1 10.254.239.10/27 domain.com default 50.0.0.2,
50.0.0.3, 50.0.0.4
```

## Command History

| Release          | Modification                                                                        |
|------------------|-------------------------------------------------------------------------------------|
| 10.16.1000       | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.13.1000       | The output parameters, <b>Broadcast-flag</b> and <b>Hostname</b> were introduced.   |
| 10.09 or earlier | Command introduced.                                                                 |

## 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 dhcp

```
show ipv6 dhcp
```

## Description

This command displays DHCP IPv6 information on the ports.

## Examples

Displaying the DHCP IPv6 information on the ports:

```
6410(config)# show ipv6 dhcp

VRF default

Interface vlan1

IPv6 address : 3013::1050/64
Domain search : paramv6.org, test1.in, test2.in, test3.in, test4.in, test5.in
DNS servers : 3013::100, 3013::101, 3013::102
NTP servers : 3013::201, 3013::202
```

## Command History

| Release    | Modification                                                                        |
|------------|-------------------------------------------------------------------------------------|
| 10.16.1000 | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.15      | Command was introduced.                                                             |

## Command Information

| Platforms     | Command context                  | Authority                                                                          |
|---------------|----------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if-mgmt<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## show ip dhcp preferred-vlan

```
show ip dhcp preferred-vlan [{vrf <VRF-NAME> | all-vrfs}]
```

### Description

Displays the preferred DHCP client VLANs configured on the system.

| Parameter      | Description                           |
|----------------|---------------------------------------|
| vrf <VRF-NAME> | Show information for a specified VRF. |
| all-vrf        | Show information for all VRFs.        |

### Examples

Displaying the DHCP information for the preferred VLAN and VRF red:

```
switch# show ip dhcp preferred-vlan vrf red
VRF Preferred-VLAN Config-status

red 10 L3 interface not found
```

Displaying the DHCP information for the all VRFs:

```
switch# show ip dhcp preferred-vlan all-vrfs
VRF Preferred-VLAN Config-status

default 1 Success
red 9 VRF Mismatch
```

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

### 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. |

## 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 platform and standards

The following table list the supported platforms for DHCPv4 relay and DHCPv6 relay.

**Table 1:** Support platforms for DHCPv4 relay and DHCPv6 relay

| Platform | DHCPv4 Relay | DHCPv4 Smart Relay | DHCPv6 Relay |
|----------|--------------|--------------------|--------------|
| 8320     | Yes          | Yes                | Yes          |
| 8325     | Yes          | Yes                | Yes          |
| 8360     | Yes          | Yes                | Yes          |
| 9300     | Yes          | Yes                | Yes          |
| 1000     | Yes          | Yes                | Yes          |

**Table 2:** Scale

| Platform | DHCP v4/v6 enabled SVI | DHCP v4/v6 helper SVI |
|----------|------------------------|-----------------------|
| 8320     | 4040                   | 8                     |
| 8325     | 4040                   | 8                     |
| 8360     | 4094                   | 8                     |
| 9300     | 4040                   | 8                     |
| 1000     | 4040                   | 8                     |

DHCP relay behaviors are as follows:

- DHCPv6 relay is disabled by default.
- DHCPv4 Smart relay is disabled by default.
- DHCP relay hop count is enabled by default.
- In DHCPv4 relay the option 82 policy is replace by default.
- The MAC address of the switch is used as the option 82 remote ID by default.
- In DHCPv6 relay the option 79 policy is disabled by default.
- In DHCPv4 relay the source-interface is disabled by default.

## Protocol and feature details

### 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.

## DHCP Relay VxLAN support

DHCPv4 Relay is supported on VXLAN with IPv4 underlay on 8100, 8360, 9300/9300S, and 10000 Switch Series, or IPv6 underlay on 8100 and 8360 Switch Series.

DHCPv6 Relay is supported on VXLAN with IPv6 underlay on 8100 and 8360 Switch Series.



---

DHCPv6 Relay requires the egress interface to be configured for the IPv6 multicast helper address. DHCPv6 relay multicast helper configuration is not allowed over VxLAN tunnels.

---

## 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.



---

A DHCP relay option 82 source-interface needs to be enabled when a source interface is used for an Intra-VRF deployment. In this deployment type, the client and DHCP server are in same VRF, but the relay will use the source interface.

---

### 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 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 sent 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.



---

On configuring a bootp-gateway the dhcp-smart-relay is disabled. This can occur with dhcp-relay as well.

---

## DHCP smart relay

The DHCP Smart Relay feature first attempts to use the primary IP address from the client-connected interfaces as a gateway IP address (giaddr) and as an IP address for pool selection. If the DHCP server does not reply to the DHCP discover messages with the primary IP address, the feature attempts to use secondary IP addresses in sequential order from the lowest to the highest. The DHCP Smart Relay forwards three client discover messages with every IP address configured on the client interface until it receives a response from the server. If the list of IP addresses from the client-connected interface is exhausted or the client times out, the DHCP Smart Relay uses the primary IP address. If the DHCP Smart Relay is not configured, the giaddr is the lowest IP address on the interface.

The DHCP Smart Relay maintains the client cache which includes the information about the client, giaddr, retry count for giaddr, port, the total number of processed discovery messages the timestamp of the discover packets. This client cache is rebuilt upon high availability and VSF switchover, VSX-MM (redundancy) switchover, and when the switch reboots.



---

DHCP Smart Relay is only supported for IPv4.

---

## 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 relay 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 relay 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.




---

On 4100i, 6000 and 6100 series switches, only SVIs are supported.

---

```
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
switch# show dhcp-relay
```

```
DHCP Relay Agent : enabled
DHCP Request Hop Count Increment : enabled
Option 82 : 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:
```

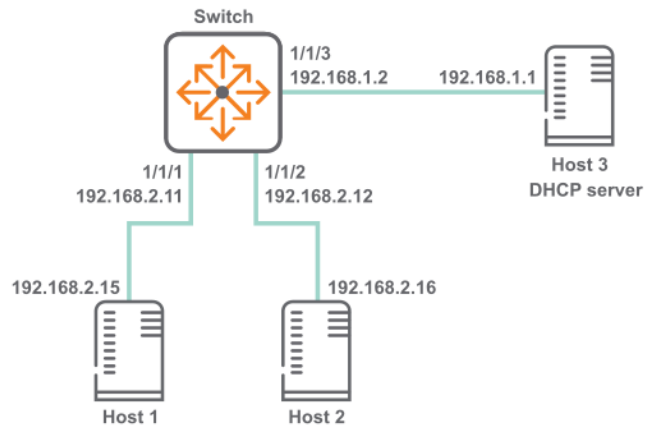
| Valid Requests | Dropped Requests | Valid Responses | Dropped Responses |
|----------------|------------------|-----------------|-------------------|
| 50             | 8                | 50              | 8                 |

## Use Case

This section explain the use cases for DHCPv4 relay agent.

### DHCPv4 relay scenario 1

In this scenario, DHCP relay on the switch 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:



### 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
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

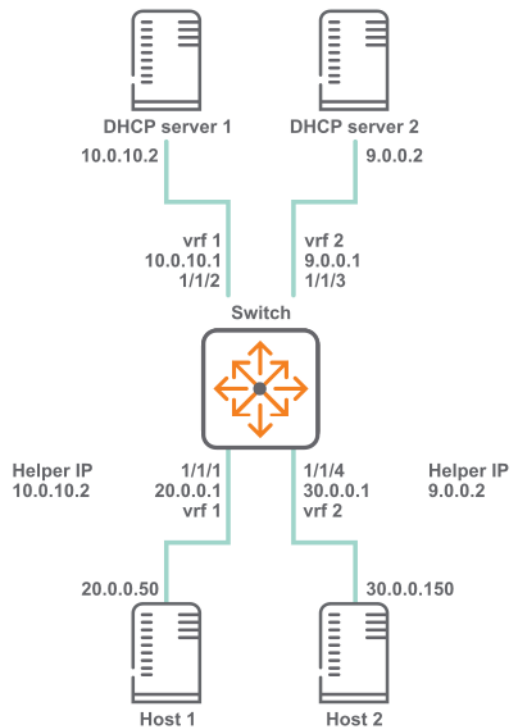
192.168.1.1 default

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# 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(configif)# interface 1/1/1
switch(configif)# vrf attach vrf1
switch(configif)# ip address 20.0.0.1/8
switch(configif)# ip helper-address 10.0.10.2
```

3. Configure interface **1/1/2**. Set its IP address and associate it with VRF 1.

```
switch(configif)# interface 1/1/2
switch(configif)# vrf attach vrf1
switch(configif)# ip address 10.0.10.1/24
```

4. Configure interface **1/1/3**. Set its IP address and associate it with VRF 2.

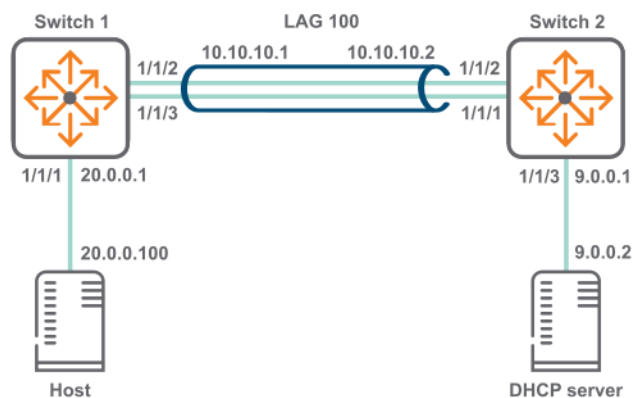
```
switch(configif)# interface 1/1/3
switch(configif)# vrf attach vrf2
switch(configif)# ip address 9.0.0.1/24
```

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(configif)# interface 1/1/4
switch(configif)# vrf attach vrf2
switch(configif)# ip address 30.0.0.1/8
switch(configif)# 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)# no shutdown
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 an IP 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
switch(config-if)# lag 100
```

- 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)# no shutdown
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 an IP address to interface 1/1/3.

```
switch(config)# interface 1/1/3
switch(config-if)# ip address 9.0.0.1/24
```

- c. Assign interfaces 1/1/1 and 1/1/2 to LAG 100.

```
switch(config-if)# interface 1/1/1
switch(config-if)# lag 100
switch(config-if)# interface 1/1/2
switch(config-if)# lag 100
```

- d. Create a route between 20.0.0.0 and 10.0.10.1.

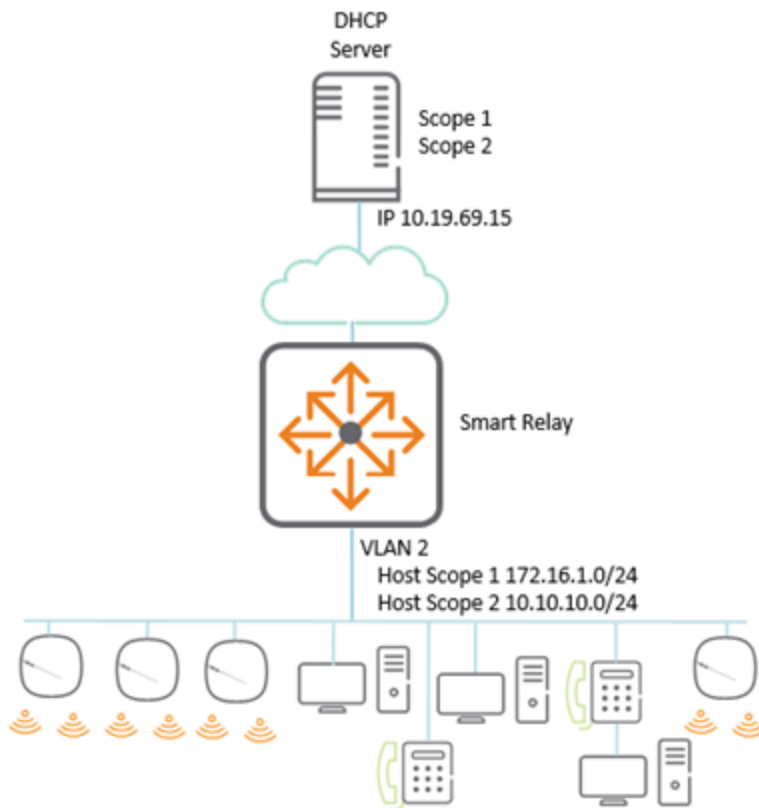
```
switch(config)# ip route 20.0.0.0/8 10.0.10.1
```

#### DHCPv4 relay scenario 4

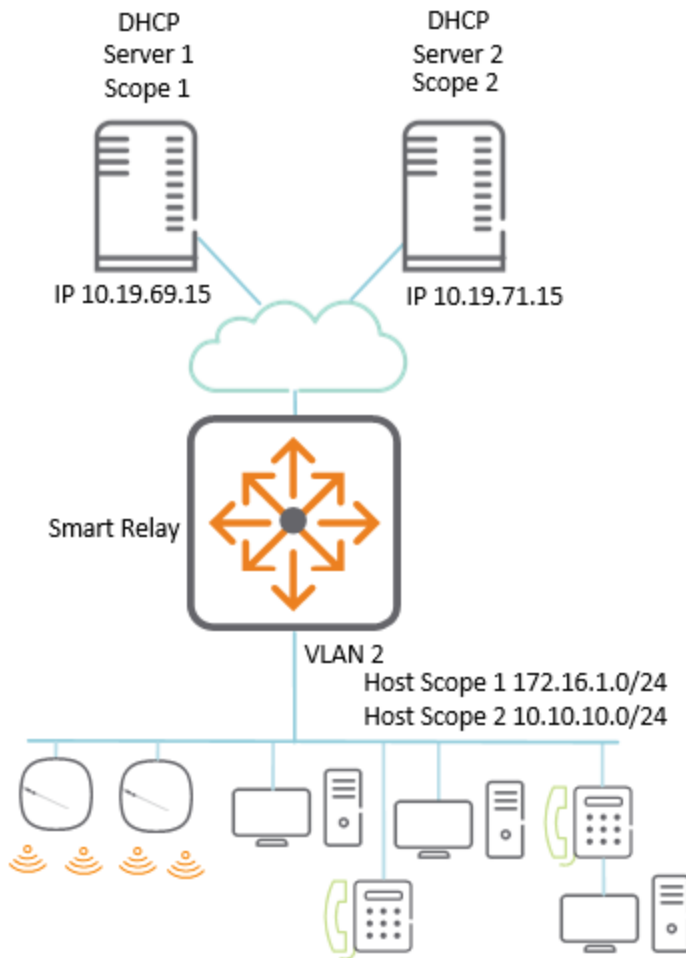
In the following scenario of the DHCP smart relay, the primary address is used as the GIADDR; if the server is unavailable, then the secondary address is used. From AOS-CX 10.10.1000 and later releases, the GIADDR use the secondary address in an ascending order when there is more than one secondary address.

1. If DHCP scope exhaustion happens at a site, an additional scope can be added to increase the IP address capacity while keeping the existing IP scope and subnet. The physical topology of the

network looks like this:



2. If the DHCP server is resilient or scope is required, then whole scopes can be placed on separate servers. If a server or scope becomes unavailable, then for address assignment, the next available scope is attempted.



In both the above topology, the access switch is set up the same way. The only difference is in the server which is used for helper addresses.

```

!
dhcp-smart-relay <-- Enable DHCP smart relay
!
interface vlan 2
 ip address 172.16.1.254/24 <-- Add the local IPS which will act
 as GIADDR
 ip address 10.10.610.254/24 secondary
 ip helper-address 10.19.69.15 <-- Add the IP helpers to reach the
 required DHCP servers
 ip helper-address 10.19.71.15

```

## 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 (and DHCP relay option 82) 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

### 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

### 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. Best practices is to disable this configuration on all the VXLAN tunnel endpoints (VTEPs), to avoid forwarding duplicate DHCP requests to the server.

The **no** form of this command disables forwarding of packets from L2 VPN clients.

### Usage

In Asymmetric/Symmetric Integrated Routing and Bridging (IRB) VXLAN deployments with a VLAN extension in subset of VTEPs, client DHCP broadcast requests are received by all the VTEPs where a client VLAN is configured. A DHCP-Relay agent on those VTEPs forward DHCP packets to configured DHCP server(s). As DHCP requests are forwarded by multiple DHCP relay agents, the DHCP server receives duplicate copies of the same packet.

When a VLAN is mapped to an L2VNI, any client requests that are received from that VLAN are considered as L2VPN clients.

When **dhcp-relay l2vpn-clients** is configured, MAC check validation is not performed on the VLAN.

All requests are being sent to the DHCP server. This can increase the load on the DHCP Server

When **no dhcp-relay l2vpn-clients** is configured, MAC check validation is performed on the VLAN.

When clients request an IP, a MAC check is performed and fails for the first packet as there is no MAC in DB by that time. The requests are dropped until the MAC Address is programmed learned. Once it is programmed learned, requests from the client are successful because the MAC entry is already present.

It is recommended to enable **dhcp-relay l2vpn-clients** on a few switches in the network topology if there are client systems that is sensitive to DHCP packet loss.

### Example

Enabling forwarding of packets from L2 VPN clients.

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

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

### dhcp-relay option 82

```
[no] dhcp-relay option 82
 replace {ip | mac | validate}
 drop {ip | mac | validate}
 keep {ip | mac}
 source-interface
 circuit-id port-id
 validate {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. Option 82 is disabled when DHCP relay is disabled globally. When DHCP relay is re-enabled, option 82 also needs to be re-enabled using the **dhcp-relay option 82** command.



---

DHCP Relay is supported over VXLAN with both IPv4 and IPv6 underlay.

---

| Parameter | Description                                                                                                                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| replace   | 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. |
| drop      | Drop any inbound client DHCP packet that contains option 82 information.                                                                                                                          |

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| keep               | 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.                                                                                                                                                                                                                                                                                        |
| source-interface   | Configures the DHCP relay to use a configured source IP address for inter-VRF server reachability. Set the source IP address with the command <code>ip source-interface</code> .                                                                                                                                                                                                                                                             |
| circuit-id port-id | Configures the circuit ID and remote ID options.<br><br><b>NOTE:</b> When enabled, DHCP Relay, unlike DHCP Snooping, drops packets from single-homed clients connected to only one switch in the VSX pair if they arrive on the VSX Secondary, unless the <code>dhcp-relay vsx active-active</code> command is enabled. To avoid this, connect single-homed clients to the VSX Primary or enable <code>dhcp-relay vsx active-active</code> . |
| validate           | Validate option 82 information in DHCP server responses and drop invalid responses.                                                                                                                                                                                                                                                                                                                                                          |
| ip                 | Use the IP address of the interface on which the client DHCP packet entered the switch as the option 82 remote ID.                                                                                                                                                                                                                                                                                                                           |
| mac                | Use the MAC address of the switch as the option 82 remote ID. Default.                                                                                                                                                                                                                                                                                                                                                                       |

## 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

| Release          | Modification                                            |
|------------------|---------------------------------------------------------|
| 10.17            | The <b>circuit-id port-id</b> parameter was introduced. |
| 10.07 or earlier | --                                                      |

## Command Information

| Platforms                                              | Command context | Authority                                                                          |
|--------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300 | config          | Administrators or local user group members with execution rights for this command. |

| Platforms      | Command context | Authority |
|----------------|-----------------|-----------|
| 9300S<br>10000 |                 |           |

### dhcp-relay vsx active-active

```
dhcp-relay vsx active-active
no dhcp-relay vsx active-active
```

### Description

Enables DHCP relay active-active mode in VSX. When enabled, DHCP relay is active on both VSX Primary and Secondary peers. DHCP client requests are processed on the same VSX peer that receives them. A VSX peer that receives DHCP client request packets from its peer silently ignores them.

By default, this feature is disabled, and DHCP request packets are forwarded to the configured helper addresses only by the VSX primary.

The **no** form of this command disables DHCP relay active-active mode, and DHCP request packets are forwarded to configured helper addresses only by the VSX primary.

### Example

Enabling relay active-active mode in VSX.

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

Disabling relay active-active mode in VSX.

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

### Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

### Command Information

| Platforms                             | Command context | Authority                                                                          |
|---------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8360<br>9300<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

### dhcp-smart-relay

```
dhcp-smart-relay
no dhcp-smart-relay
```

### Description

Enables DHCP Smart Relay on the device and on all the interfaces where IP helper addresses are configured. Disabled by default at the device level. Not supported on the management interface.

The **no** form of this command disables DHCP Smart Relay.



Prior to enabling DHCP Smart Relay, enable IP helper address configuration and configure secondary IP addresses on the interface.

## Examples

Enabling DHCP Smart Relay:

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

Disabling DHCP Smart Relay support:

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

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

### diag-dump dhcp-relay basic

```
diag-dump dhcp-relay basic
```

## Description

Dumps DHCP relay configurations for all interfaces.

## Examples

This example enables DHCP relay support.

```
switch# diag-dump dhcp-relay basic
=====
```

```
[Start] Feature dhcp-relay Time : Sun Apr 26 06:38:10 2020
=====
```

```
[Start] Daemon hpe-relay
=====
```

```

DHCP Relay : 1
DHCP Relay hop-count-increment : 1
DHCP Relay Option82 : 1
DHCP Relay Option82 validate : 0
DHCP Relay Option82 policy : keep
DHCP Relay Option82 remote-id : mac
DHCP Relay Option82 Source Intf : Disable
DHCP Smart Relay : Enable
System Mac [f4:03:43:80:27:00]
VRF :BLUE, Source Ip:200.0.0.10
vsx: Not Present
vsx: Present
isl_status: Up
remote_idl : 1
VSX Active-Active Mode : Enable
evpn VLANs: None
evpn MAC clause : unset
Allow IPv4 l2vpn client : enable

```

```
Interface vlan2: 1
```

```
Client Packet Statistics:
```

| Valid | Dropped | O82_Valid | O82_Dropped | vsx_drops |
|-------|---------|-----------|-------------|-----------|
| ----- | -----   | -----     | -----       | -----     |
| 0     | 0       | 0         | 0           | 0         |

```
Server Packet Statistics:
```

| Valid Dsnoop | Dropped | O82_Valid | O82_Dropped | Invalid_IP_Drops | To_   |
|--------------|---------|-----------|-------------|------------------|-------|
| -----        | -----   | -----     | -----       | -----            | ----- |
| 0            | 0       | 0         | 0           | 0                | 0     |

client request dropped packets with extn option 82 = 0  
client request valid packets with extn option 82 = 0  
server request dropped packets with extn option 82 = 0  
server request valid packets with extn option 82 = 0  
Port 67 - 200.0.0.100,2  
source vrf-BLUE.

```
Interface vlan3: 1
```

```
Client Packet Statistics:
```

| Valid | Dropped | O82_Valid | O82_Dropped | vsx_drops |
|-------|---------|-----------|-------------|-----------|
| ----- | -----   | -----     | -----       | -----     |
| 0     | 0       | 0         | 0           | 0         |

```
Server Packet Statistics:
```

| Valid Dsnoop | Dropped | O82_Valid | O82_Dropped | Invalid_IP_Drops | To_   |
|--------------|---------|-----------|-------------|------------------|-------|
| -----        | -----   | -----     | -----       | -----            | ----- |
| 0            | 0       | 0         | 0           | 0                | 0     |

client request dropped packets with extn option 82 = 0  
client request valid packets with extn option 82 = 0  
server request dropped packets with extn option 82 = 0  
server request valid packets with extn option 82 = 0  
Port 67 - 200.0.0.100,2  
source vrf-BLUE.

```

DHCP Smart Relay Client Cache:
Total Number of entries: 2

Client-MAC PortIndex Timestamp RetryCount DiscCount GWIP

00:50:56:bd:6a:7a 20 1636105218 1 4 30.0.0.1
00:50:56:bd:71:17 20 1636105214 1 4 30.0.0.1

[End] Daemon hpe-relay

[End] Feature dhcp-relay
=====
Diagnostic-dump captured for feature dhcp-relay

```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

### 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.

| Parameter   | Description                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------|
| <IPV4-ADDR> | Specifies the IP address of the gateway in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. |

### Examples

Setting 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-if       | Administrators or local user group members with execution rights for this command. |

### 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 relay agent forwards DHCP client requests to all defined servers.

If IP helper address is defined with VRF argument then this command requires 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.

| Parameter                  | Description                                                                                                          |
|----------------------------|----------------------------------------------------------------------------------------------------------------------|
| helper-address <IPV4-ADDR> | Specifies the helper IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. |
| vrf <VRF-NAME>             | Specifies the name of a VRF. Default: <b>default</b> .                                                               |

### Examples

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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-if       | Administrators or local user group members with execution rights for this command. |

## show dhcp-relay

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

## Description

Shows DHCP relay configuration settings.

| 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. |

## Example

Showing DHCP relay settings:

```

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 Reply Overwrite Source IP : enabled
Option 82 Circuit ID Port-ID : enabled
VSX Active-Active Mode : enabled

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

```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                                                                                                              |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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 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.

| Parameter        | Description                                       |
|------------------|---------------------------------------------------|
| <INTERFACE-NAME> | Specifies an interface. Format: member/slot/port. |

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vsx-peer</code> | 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 the designated bootp gateway for all interfaces:

```
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
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                                                                                                              |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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 ip helper-address

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

## Description

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

| Parameter                                   | Description                                                                                                                                                                                                                      |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>interface &lt;INTERFACE-ID&gt;</code> | Specifies an interface. Format: member/slot/port.                                                                                                                                                                                |
| <code>vsx-peer</code>                       | 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 the IP helper addresses for all interfaces:

```
switch# 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
```

Showing the IP helper addresses for interface 1/1/1:

```
switch# show ip helper-address interface 1/1/1
IP Helper Addresses

Interface: 1/1/1
IP Helper Address VRF

192.168.20.1 default
192.168.10.1 default
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                                                                                                              |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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. |

## DHCPv6 relay agent

### DHCPv6 relay VRF support

DHCPv6 relay is VRF aware. DHCPv6 client requests received on an interface are forwarded to the configured servers via that interface's VRF. DHCPv6 server responses received on an interface are forwarded to the client which is reachable via that interface's VRF.



## Limitations

DHCPv6 Relay requires an egress interface to be configured for the IPv6 multicast helper address. DHCPv6-Relay multicast helper configuration is not allowed over VxLAN tunnels.

The following configuration is required in order to use source interface for DHCPv6 relay.

Configuring the IPv6 source-interface interface to use for DHCPv6 relay:

```
switch(config)# ipv6 source-interface dhcp_relay interface loopback3 vrf test1
```

Enabling DHCPv6 relay to use the configured source interface:

```
switch(config)# dhcpv6-relay source-interface
```

## Configuring the DHCPv6 relay agent

### Prerequisites

- An enabled layer 3 interface.

### Procedure

1. Enable the DHCPv6 relay 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.

```
switch(config)# dhcpv6-relay
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# ipv6 address 2002::22/64
switch(config-if)# ipv6 helper-address unicast 2001::1
switch(config-if)# ipv6 helper-address multicast ff01::1:1000 egress 1/1/1
switch(config-if)# ipv6 helper-address multicast all-dhcp-servers egress 1/1/1
switch(config-if)# exit
switch(config)# interface 1/1/2
```

```

switch(config-if)# no shutdown
switch(config-if)# ipv6 address 2002::21/64
switch(config-if)# ipv6 helper-address unicast 2001::1
switch(config-if)# ipv6 helper-address multicast ff01::1:1000 egress 1/1/1
switch(config-if)# exit
switch(config)# end

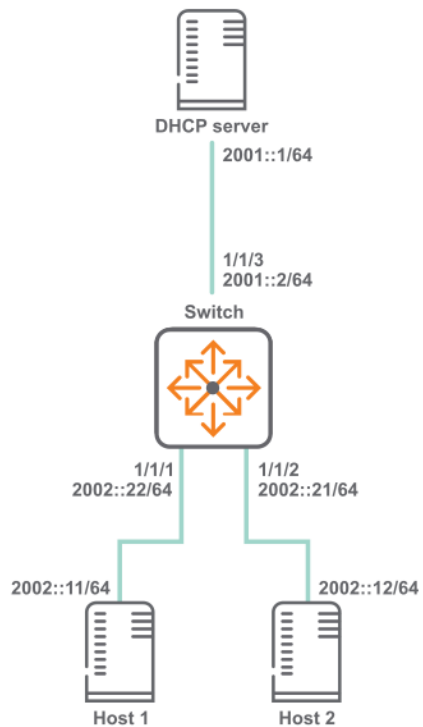
```

## Use Case

This section explain the use cases for DHCPv6 relay agent.

### DHCPv6 relay scenario 1

In this scenario, DHCP relay on the switch 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:



## Procedure

1. Enable DHCP relay.
 

```

switch# config
switch(config)# dhcpv6-relay

```
2. Define an IPv6 helper address.
  - On interface `vlan 10` and `vlan 20`.

```

switch(config)# dhcpv6-relay
switch(config)# interface 1/1/1
switch(config)# no shutdown
switch(config-if)# vlan access 10
switch(config-if)# exit
switch(config)# interface 1/1/2
switch(config)# no shutdown

```

```

switch(config-if)# vlan access 20
switch(config-if)# exit
switch(config)# interface vlan 10
switch(config-if-vlan)# no shutdown
switch(config-if-vlan)# ipv6 address 2002::22/64
switch(config-if-vlan)# ipv6 helper-address unicast 2001::1
switch(config-if-vlan)# ipv6 helper-address multicast ff01::1:1000 egress
vlan30
switch(config-if-vlan)# ipv6 helper-address multicast all-dhcp-servers
egress vlan50
switch(config-if-vlan)# exit
switch(config)# interface vlan 20
switch(config-if-vlan)# no shutdown
switch(config-if-vlan)# ipv6 address 2002::21/64
switch(config-if-vlan)# ipv6 helper-address unicast 2001::1
switch(config-if-vlan)# ipv6 helper-address multicast ff01::1:1000 egress
vlan30
switch(config-if-vlan)# ipv6 helper-address multicast all-dhcp-servers
egress vlan50
switch(config-if-vlan)# exit
switch(config)# end

```

- On interface 1/1/1 and 1/1/2.

```

switch(config)# dhcpv6-relay
switch(config)# interface 1/1/1
switch(config)# no shutdown
switch(config-if)# ipv6 address 2002::22/64
switch(config-if)# ipv6 helper-address unicast 2001::1
switch(config-if)# ipv6 helper-address multicast ff01::1:1000 egress 1/1/3
switch(config-if)# ipv6 helper-address multicast all-dhcp-servers egress
1/1/3
switch(config-if)# exit
switch(config)# interface 1/1/2
switch(config)# no shutdown
switch(config-if)# ipv6 address 2002::21/64
switch(config-if)# ipv6 helper-address unicast 2001::1
switch(config-if)# ipv6 helper-address multicast ff01::1:1000 egress 1/1/3
switch(config-if)# ipv6 helper-address multicast all-dhcp-servers egress
1/1/3
switch(config-if)# exit
switch(config)# end

```

### 3. Verify DHCP relay configuration.

- When interface `vlan 10` and `vlan 20` is configured as relay.

```

switch# show dhcpv6-relay
 DHCPv6 Relay Agent : enabled
 Option 79 : disabled
switch# show ipv6 helper-address

IP Helper Addresses

Interface: vlan10
IP Helper Address Egress Port

```

```

all-dhcp-servers vlan50
ff01::1:1000 vlan30
2001::1 -

Interface: vlan20
IP Helper Address Egress Port

all-dhcp-servers vlan50
ff01::1:1000 vlan30
2001::1 -

```

- When interface 1/1/1 and 1/1/2 is configured as relay.

```

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

all-dhcp-servers 1/1/3
ff01::1:1000 1/1/3
2001::1 -

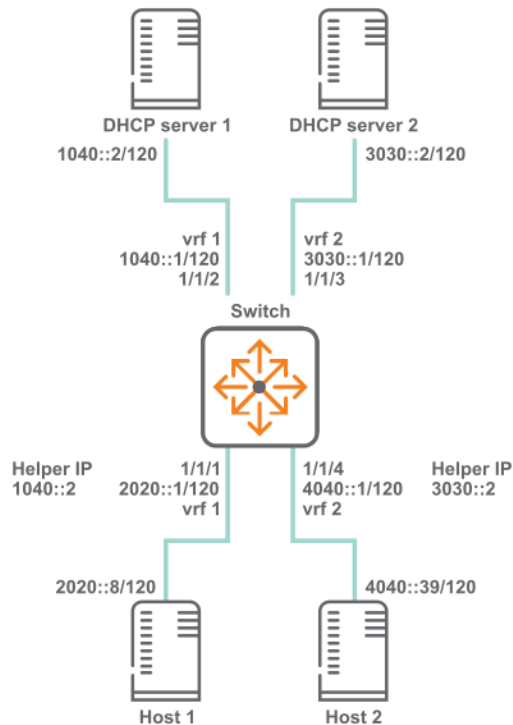
Interface: 1/1/2
IPv6 Helper Address Egress Port

all-dhcp-servers 1/1/3
ff01::1:1000 1/1/3
2001::1 -

```

## 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:



## Procedure

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(configif)# interface 1/1/1
switch(configif)# vrf attach vrf1
switch(configif)# ipv6 address 2020::1/120
switch(configif)# ipv6 helper-address unicast 1040::2
```
3. Configure interface **1/1/2**. Set its IP address and associate it with VRF 1.
 

```
switch(configif)# interface 1/1/2
switch(configif)# vrf attach vrf1
switch(configif)# ipv6 address 1040::1/120
```
4. Configure interface **1/1/3**. Set its IP address and associate it with VRF 2.
 

```
switch(configif)# interface 1/1/3
switch(configif)# vrf attach vrf2
switch(configif)# 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(configif)# interface 1/1/4
switch(configif)# vrf attach vrf2
switch(configif)# ipv6 address 4040::1/120
switch(configif)# ipv6 helper-address unicast 3030::2
```

## DHCP relay (IPv6) commands

### dhcpv6-relay

```
dhcpv6-relay [l2vpn-clients | source-interface]
no dhcpv6-relay [l2vpn-clients | source-interface]
```

## Description

Enables DHCPv6 relay support. DHCPv6 relay is disabled by default. DHCP relay is not supported on the management interface. Best practices is to disable this configuration on all the VXLAN tunnel endpoints (VTEPs), to avoid forwarding duplicate DHCPv6 requests to the server.

The **no** form of this command disables DHCP relay support.

DHCPv6 Relay requires that you configure the egress interface using the [ipv6 helper-address](#) command. The egress interface of a VTEP is used as an underlay, so a DHCPv6 Relay Multicast ipv6 address is not supported in a VXLAN topology.

| Parameter                     | Description                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------|
| <code>l2vpn-clients</code>    | Enables packets from l2vpn clients to be forwarded to configured servers. Enabled by default. |
| <code>source-interface</code> | Enables DHCPv6 relay to use the configured source interface.                                  |

## Usage

In Asymmetric/Symmetric Integrated Routing and Bridging (IRB) VXLAN deployments with a VLAN extension in subset of VTEPs, client DHCPv6 broadcast requests are received by all the VTEPs where a client VLAN is configured. A DHCPv6 relay agent on those VTEPs forward DHCPv6 packets to configured DHCPv6 server(s). As DHCPv6 requests are forwarded by multiple DHCPv6 relay agents, the DHCPv6 server receives duplicate copies of the same packet. When this configuration is disabled, the DHCPv6 relay agent on VTEPs ignores DHCPv6 request packets that are received from client MACs addresses learned via EVPN.

## Examples

Enables DHCPv6 relay support.

```
switch(config)# dhcpv6-relay
```

Removes DHCPv6 relay support.

```
switch(config)# no dhcpv6-relay
```

## Command History

| Release          | Modification                                            |
|------------------|---------------------------------------------------------|
| 10.12.1000       | <b>l2vpn-clients</b> and <b>source-interface</b> added. |
| 10.07 or earlier | --                                                      |

## Command Information

| Platforms    | Command context     | Authority                                                                          |
|--------------|---------------------|------------------------------------------------------------------------------------|
| 8100<br>8320 | <code>config</code> | Administrators or local user group members with execution rights for this command. |

| Platforms | Command context | Authority |
|-----------|-----------------|-----------|
| 8325      |                 |           |
| 8325H     |                 |           |
| 8325P     |                 |           |
| 8360      |                 |           |
| 9300      |                 |           |
| 9300S     |                 |           |
| 10000     |                 |           |

### 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 8100      | config          | Administrators or local user group members with execution rights for this command. |
| 8320      |                 |                                                                                    |
| 8325      |                 |                                                                                    |
| 8325H     |                 |                                                                                    |
| 8325P     |                 |                                                                                    |
| 8360      |                 |                                                                                    |
| 9300      |                 |                                                                                    |
| 9300S     |                 |                                                                                    |
| 10000     |                 |                                                                                    |

### dhcpv6-relay vsx active-active

dhcpv6-relay vsx active-active  
no dhcpv6-relay vsx active-active

## Description

Enables DHCPv6 relay active-active mode in VSX. When enabled, DHCPv6 relay is active on both VSX Primary and Secondary peers. DHCPv6 client requests are processed on the same VSX peer that receives them. A VSX peer that receives DHCPv6 client request packets from its peer silently ignores them.

By default, this feature is disabled, and DHCPv6 request packets are forwarded to the configured helper addresses only by the VSX primary.

The **no** form of this command disables DHCPv6 relay active-active mode, and DHCPv6 request packets are forwarded to configured helper addresses only by the VSX primary.

## Example

Enabling relay active-active mode in VSX.

```
switch(config)# dhcpv6-relay vsx active-active
```

Disabling relay active-active mode in VSX.

```
switch(config)# no dhcpv6-relay vsx active-active
```

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms                             | Command context | Authority                                                                          |
|---------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8360<br>9300<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

### diag-dump dhcpv6-relay basic

```
diag-dump dhcpv6-relay basic
```

## Description

Dumps DHCPv6 relay configurations for all interfaces.

## Examples

This example enables DHCP relay support.

```
switch# diag-dump dhcpv6-relay basic
=====
[Start] Feature dhcpv6-relay Time : Thu Jun 8 09:55:11 2017
=====
```

```

[Start] Daemon hpe-relay

DHCP Relay : 1
DHCPv6 Relay Option79 : 0
vsx: Present
vsx_status: Primary
isl_status: Up
VSX Active-Active Mode : Enable
evpn VLANs: None
evpn MAC clause : unset
Allow IPv6 l2vpn client : disable

System Mac [02:02:02:02:0a:0a]
Interface vlan10: 1
Intf selected IP - ifindex - 10 kernel ifindex - 1701::1, 1, egress = (null),
Server vrf = default

Client Packet Statistics:

Valid Dropped vsx_drops

0 0 0

Server Packet Statistics:

Valid Dropped To_Dsnoop

0 0 0

Total VRF source-ip entrie: 0

[End] Daemon hpe-relay

=====
[End] Feature dhcpv6-relay
=====
Diagnostic-dump captured for feature dhcpv6-relay

```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <UNICAST-IPV6-ADDR>   | Specifies the unicast helper IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F.                                                                            |
| <MULTICAST-IPV6-ADDR> | Specifies the multicast helper IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F.                                                                          |
| all-dhcp-servers      | Specifies all the DHCP server IPv6 addresses for the interface.                                                                                                                                                                  |
| egress <PORT-NUM>     | 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. |
| vrf <VRF-NAME>        | Specifies the name of the VRF from which the specified protocol sets its source IP address.                                                                                                                                      |

## Examples

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

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

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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.

| 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. |

### Example

```
switch(config)# show dhcpv6-relay
DHCPv6 Relay Agent : enabled
Option 79 : disabled
L2vpn-clients : enabled
Source-interface : enabled
VSX Active-Active Mode : enabled
```

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms                                                                | Command context | Authority                                                                                                                                                              |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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 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.

| Parameter                | Description                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface <INTERFACE-ID> | Specifies an interface. Format: <b>member/slot/port</b> .                                                                                                                                                                        |
| 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 helper-address

Interface: 1/1/1
IPv6 Helper Address Egress Port

2001:db8:0:1:: -
FF01::1:1000 1/1/2

Interface: 1/1/2
IPv6 Helper Address Egress Port

2001:db8:0:1:: -

switch# show ipv6 helper-address interface 1/1/1

Interface: 1/1/1
IPv6 Helper Address Egress Port

2001:db8:0:1:: -
FF01::1:1000 1/1/2
```

```
switch# show ipv6 helper-address interface vlan20
Interface: vlan20
IP Helper Address Egress Port

2001::1 -
ff01::1:1000 vlan30 default
```

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms                                                                | Command context | Authority                                                                                                                                                              |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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. |

## Troubleshooting

### One or more DHCP clients not getting IP address

#### Reachability between relay and server(s)

Server reachability is required for DHCP Relay function to work.

1. Ping to check IP reachability between switch and the server(s).
2. Confirm the ping test is made in the appropriate VRF and with the correct gateway IP. By default, DHCP Relay picks the lowest IP address on the client-connected interface as the gateway IP address.

When configured, the bootp-gateway IP address is used as the gateway IP.

#### Source-ip configuration

With the source-ip configuration in the VRF, DHCP relay uses it as a gateway IP address to communicate with the DHCP server.

1. It requires `dhcp_relay source-interface` configuration for `ip source-interface relay` to work.
2. Ping the server with `source-ip` as the configured `source-interface` IP. The same test is applicable for the Inter-VRF route leak (IVRL) configuration.
3. If the client and server are in different VRFs, test server reachability in server-VRF by using configured `source-interface` IP.

#### Option-82 conflict with DHCP snooping and Relay [DHCPv4 Specific]

AOS-CX supports configuring DHCP snooping and DHCP relay on the same VLAN. In cases where DHCP relay is configured to use `source-interface` along with `inter-vrf server`, Option 82 is added to the packet sent to the server.

If Option 82 is enabled for both DHCP snooping and DHCP relay, DHCP snooping gets the priority. In this scenario for DHCP relay to work, disable Option-82 for DHCP snooping.

- Check if the helper-address is configured to the correct VRF where the DHCP server is reachable
- CoPP drop checks—In case of excessive DHCP traffic, CoPP does the rate limit by dropping some of the packets.

#### Client packets are dropped

Check if client packets are getting dropped by CoPP using `show copp statistics class dhcp-ipv4` or `show copp statistics class dhcp-ipv6` commands.

#### Server pool configuration and exhaustion

1. Check the server side configuration to see if IP lease criteria is being met for the client.
2. Check if the right VRF selection is happening for the lease allocation.

## DHCP Smart-Relay

It allows the DHCP relay agent to use non-lower IP addresses from the client-connected interfaces as giaddr and for pool selection when the DHCP server does not reply to the DHCP discover messages with the lowest IP address. More than one IP address and helper address must be configured on the client-connected interfaces. The server must be configured with the DHCPv4 pools for the client-connected IP addresses

- Server Reachability

Ensure the ping test is made in the appropriate VRF and with the correct gateway IP (IPs from the client-connected interfaces).

- Bootp gateway IP configuration

When a bootp gateway IP is configured, it gets the highest priority and is used as a gateway IP.

- Source-ip configuration

When a source IP is configured, Option 82 needs to be enabled. The Source IP is used as a gateway IP, and Option 82 is used as sub-option 5 contains the IP used for the pool selection.

- Client Cache and timeout

For debugging, a client cache is built, which contains information on the gateway IP for every client.

The entry is added to the client cache for the client which does not have an existing entry. The client entries are deleted if the client is idle for 360 seconds. In other cases, a particular client entry might get deleted if it is the oldest entry in time and if the client cache is full. The client cache is deleted completely if the functionality is disabled.

It uses the lowest IP address as giaddr or for pool selection when all client-connected IPs are exhausted or the client retries after an idle timeout. The client cache is rebuilt upon HA and VSF switchover, VSX-MM (redundancy) switchover, and reboot of the switch.

## DHCP server

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.

## Protocol and feature details

### 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 can not be configured with DHCP server.

## Supported platform and standards

The following table list the supported platforms for DHCPv4 server and DHCPv6 server.

**Table 1:** Support platforms for DHCPv4 server and DHCPv6 server

| Platform | DHCPv4 server | DHCPv6 server |
|----------|---------------|---------------|
| 8320     | Yes           | Yes           |
| 8325     | Yes           | Yes           |
| 8360     | Yes           | Yes           |
| 9300     | Yes           | Yes           |
| 1000     | Yes           | Yes           |

The below limit is based on system stability.

- Single VRF
  - Maximum pools—64
  - Maximum range —64 (Every pool having one range)
  - One static host per pool
  - Maximum clients - 8192 (Every range providing 128 leases )
- Across 32 VRF's
  - Maximum pools - 64 (Every VRF having 2 pools)
  - Maximum range - 64 (Every pool having one range)
  - One static host per pool
  - Maximum clients - 8192 (Every range providing 128 leases )

## 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 options 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.

```
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 **dhcpv6-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 **dhcpv6-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::14** 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)# dhcpv6-server vrf primary
switch(config-dhcpv6-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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms    | Command context    | Authority                                                                          |
|--------------|--------------------|------------------------------------------------------------------------------------|
| 8100<br>8320 | config-dhcp-server | Administrators or local user group members with execution rights for this command. |

| Platforms                                                | Command context | Authority |
|----------------------------------------------------------|-----------------|-----------|
| 8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 |                 |           |

## 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.

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <REMOTE-URL> | <p>Specifies the name and location of a BOOTP file on a TFTP server in the format:</p> <pre>tftp://{&lt;IP&gt;   &lt;HOST&gt;}/&lt;FILE&gt;</pre> <ul style="list-style-type: none"> <li>▪ <b>&lt;IP&gt;</b>: Specifies the IP address of the TFTP server hosting the file in IPv4 format (<b>x.x.x.x</b>), where <b>x</b> 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.</li> <li>▪ <b>&lt;HOST&gt;</b>: Specifies the fully-qualified domain name of the TFTP server hosting the file. Range: 1 to 64 printable ASCII characters.</li> <li>▪ <b>&lt;FILE&gt;</b>: Specifies the name of the BOOTP file. Range: 1 to 64 printable ASCII characters.</li> </ul> |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context         | Authority                                                                          |
|--------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

### 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.

| Parameter                  | Description                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all-vrfs                   | Clears leases for all VRFs.                                                                                                                                                                                                                                             |
| <IPv4-ADDR> vrf <VRF-NAME> | Clears the lease for a specific client on a specific VRF. Specify the client address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> 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. |
| vrf <VRF-NAME>             | Clears leases for a specific VRF.                                                                                                                                                                                                                                       |

### Examples

Clearing all DHCPv4 server leases.

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

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

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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                                                                                                              |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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. |

## 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.

| Parameter        | Description                                                                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPV4-ADDR-LIST> | Specifies the IP addresses of the default routers in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> 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. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context         | Authority                                                                          |
|--------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## dhcp-server external-storage

```
dhcp-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
no dhcp-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             | Description                                                                            |
|-----------------------|----------------------------------------------------------------------------------------|
| <VOLUME-NAME>         | Specifies the external storage volume name. Range: 1 to 64 printable ASCII characters. |
| file <LEASE-FILENAME> | Specifies the external storage filename. Range: 1 to 255 printable                     |

| Parameter     | Description                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------|
|               | ASCII characters.                                                                                                 |
| delay <DELAY> | Specifies the interval in seconds between updates to the external storage file. Range: 15 to 86400. Default: 300. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter  | Description    |
|------------|----------------|
| <VRF-NAME> | Name of a VRF. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context    | Authority                                                                          |
|--------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server | Administrators or local user group members with execution rights for this command. |

## 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        | Description                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPV4-ADDR-LIST> | Specifies the IP addresses of the DNS servers in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. Separate addresses with a space. |

## Example

Defines 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms | Command context         | Authority                                       |
|-----------|-------------------------|-------------------------------------------------|
| 8100      | config-dhcp-server-pool | Administrators or local user group members with |

| Platforms                                                        | Command context | Authority                          |
|------------------------------------------------------------------|-----------------|------------------------------------|
| 8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 |                 | execution rights for this command. |

## 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.

| Parameter     | Description                                                          |
|---------------|----------------------------------------------------------------------|
| <DOMAIN-NAME> | Specifies a domain name. Range: 1 to 255 printable ASCII characters. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms            | Command context         | Authority                                                                          |
|----------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

| Platforms                                        | Command context | Authority |
|--------------------------------------------------|-----------------|-----------|
| 8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 |                 |           |

## enable

enable

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context    | Authority                                                                          |
|--------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| <TIME>    | Sets the DHCPv4 lease time. Format: DD:HH:MM. Default: 01:00:00.                             |
| infinite  | Sets the DHCPv4 lease time to infinite. This means that addresses do not need to be renewed. |

## 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
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context         | Authority                                                                          |
|--------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## 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 ( <b>x.x.x.x</b> ), where <b>x</b> 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**.

```
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**.

```
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
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context         | Authority                                                                          |
|--------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

### netbios-node-type

```
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 | Description                                                                 |
|-----------|-----------------------------------------------------------------------------|
| <TYPE>    | Specifies the NetBIOS node type: broadcast, hybrid, mixed, or peer-to-peer. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context         | Authority                                                                          |
|--------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

### option

```
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.

| Parameter           | Description                                                                                                                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <OPTION-NUM>        | 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. |
| ascii <ASCII-STR>   | Specifies a value for the selected option as an ASCII string. Range: 1 to 255 ASCII characters.<br><br><b>NOTE:</b> If you specify <b>18</b> as the <OPTION-NUM> parameter, the ASCII string must be enclosed within quotation marks (").                                         |
| hex <HEX-STR>       | Specifies a value for the selected option as a hexadecimal string. Range: 1 to 255 hexadecimal characters.                                                                                                                                                                        |
| ip <IPV4-ADDR-LIST> | Specifies a list of IP addresses in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. Separate addresses with a space. A maximum of four IP addresses can be defined.                                                                             |

## 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
```

Defines DHCPv4 option 18 for the server pool **mgmt-test** on VRF **mgmt**.

```
switch(config)# dhcp-server vrf mgmt
switch(config-dhcp-server)# pool mgmt-test
switch(config-dhcp-server-pool)# option 18 ascii "aswed"
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                     | Command context         | Authority                                                                          |
|-------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

| Platforms                               | Command context | Authority |
|-----------------------------------------|-----------------|-----------|
| 8325P<br>8360<br>9300<br>9300S<br>10000 |                 |           |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms            | Command context                 | Authority                                                                          |
|----------------------|---------------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325 | <code>config-dhcp-server</code> | Administrators or local user group members with execution rights for this command. |

| Platforms                                        | Command context | Authority |
|--------------------------------------------------|-----------------|-----------|
| 8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 |                 |           |

## 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.

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LOW-IPV4-ADDR>   | Specifies the lowest IP address in the pool in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <HIGH-IPV4-ADDR>  | Specifies the highest IP address in the pool in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| prefix-len <MASK> | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 32.<br><br><b>NOTE:</b> 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.<br><br><pre>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 prefix-len 16</pre> |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context         | Authority                                                                          |
|--------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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.

| Parameter                          | Description                                                                      |
|------------------------------------|----------------------------------------------------------------------------------|
| all-vrfs                           | Shows DHCPv4 server configuration settings for all VRFs.                         |
| leases {all-vrfs   vrf <VRF-NAME>} | Shows DHCPv4 server lease provided by the server for all VRFs or a specific VRF. |
| pool <POOL-NAME> [vrf <VRF-NAME>]  | Shows DHCPv4 server pool configuration settings for all VRFs or a specific VRF.  |

## Examples

Showing all DHCPv4 server configuration settings.

```
switch# show dhcp-server

VRF Name : default
DHCP Server : enabled
```

```

Operational State : operational
Authoritative Mode : false
Config_status : Applied

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

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
Config_status : Applied

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:a4
20.0.0.1 * 11:22:11:22:aa:dd

```

#### BOOTP Options

```

Boot-File-Name TFTP-Server-Name State TFTP-Server-Address

boot.txt * OPERATIONAL 10.0.0.10

```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context | Authority                                                                                                                                                              |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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. |

## 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.

| Parameter   | Description                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPV4-ADDR> | Specifies an IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. The IP address must be within the address range defined for the current pool. |

| Parameter       | Description                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------|
| mac <MAC-ADDR>  | Specifies a client station MAC address (xx:xx:xx:xx:xx:xx), where <b>x</b> is a hexadecimal number from 0 to F. |
| hostname <HOST> | Specifies the host name of the client station. Range: 1 to 255 printable ASCII characters                       |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context         | Authority                                                                          |
|--------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## 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**.

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

Removes DHCPv6 server authoritative mode on VRF **primary**.

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

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context      | Authority                                                                          |
|--------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter                  | Description                                                                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all-vrfs                   | Clears leases for all VRFs.                                                                                                                                        |
| <IPv6-ADDR> vrf <VRF-NAME> | Clears the lease for a specific client on a specific VRF. Specify the client address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a |

| Parameter      | Description                                                                                                                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | 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<br>2222:0000:3333:0000:0000:0000:4444:0055 becomes<br>2222:0:3333::4444:55. |
| vrf <VRF-NAME> | Clears leases for a specific VRF.                                                                                                                                                                                                                                                          |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                      | Command context | Authority                                                                                                                                                              |
|------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360 | 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. |

| Platforms              | Command context | Authority |
|------------------------|-----------------|-----------|
| 9300<br>9300S<br>10000 |                 |           |

## dhcpv6-server external-storage

```
dhcpv6-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
no dhcpv6-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.

| Parameter             | Description                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------|
| <VOLUME-NAME>         | Specifies the external storage volume name. Range: 1 to 64 printable ASCII characters.                            |
| file <LEASE-FILENAME> | Specifies the external storage filename. Range: 1 to 255 printable ASCII characters.                              |
| delay <DELAY>         | Specifies the interval in seconds between updates to the external storage file. Range: 15 to 86400. Default: 300. |

### Example

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

```
switch(config)# dhcpv6-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 dhcpv6-server external-storage Storage1 file LeaseFile delay 600
```

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms                                                                | Command context | Authority                                                                          |
|--------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter       | Description    |
|-----------------|----------------|
| <i>VRF-NAME</i> | Name of a VRF. |

### 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms                                      | Command context | Authority                                                                          |
|------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360 | config          | Administrators or local user group members with execution rights for this command. |

| Platforms              | Command context | Authority |
|------------------------|-----------------|-----------|
| 9300<br>9300S<br>10000 |                 |           |

## disable

disable

### Description

Disables the DHCPv6 server on the current VRF. The DHCPv6 server is disabled by default when configured on a VRF.

### Example

Disables the DHCPv6 server on VRF **primary**.

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

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms                                                                | Command context      | Authority                                                                          |
|--------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

## dns-server

```
dns-server <IPVv6-ADDR-LIST>
no dns-server <IPVv6-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.

| Parameter         | Description                                                  |
|-------------------|--------------------------------------------------------------|
| <IPVv6-ADDR-LIST> | Specifies the IP addresses of the DNS servers in IPv6 format |

| Parameter | Description                                                                                                                                                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | ( <b>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</b> ), where <b>x</b> is a hexadecimal number from 0 to F. Separate addresses with a space. A maximum of four IP addresses can be defined. |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context           | Authority                                                                          |
|--------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## enable

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)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# enable
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context      | Authority                                                                          |
|--------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

## lease

```
lease {<TIME> | infinite}
no 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.

```
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.

```
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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context           | Authority                                                                          |
|--------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

### option

```
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.

| Parameter           | Description                                                                                                                                                   |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <OPTION-NUM>        | Specifies a DHCPv6 option number. Range: 2 to 254.                                                                                                            |
| ascii <ASCII-STR>   | Specifies a value for the selected option as an ASCII string. Range: 1 to 255 ASCII characters.                                                               |
| hex <HEX-STR>       | Specifies a value for the selected option as a hexadecimal string. 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 <b>x</b> is a hexadecimal number from 0 to F. |

### Example

Defines DHCPv6 option **22** 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)# option 22 ipv6 2001::12
```

Deletes DHCPv6 option 22 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)# no option 22 ipv6 2001::12
```

Defines DHCPv6 option **18** for the server pool **mgmt-test** on VRF **mgmt**.

```
switch(config)# dhcpv6-server vrf mgmt
switch(config-dhcpv6-server)# pool mgmt-test
switch(config-dhcpv6-server-pool)# option 18 ascii "aswed"
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context           | Authority                                                                          |
|--------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## pool

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

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context      | Authority                                                                          |
|--------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter         | Description                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LOW-IPV6-ADDR>   | Specifies the lowest IP address in the pool in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F.  |
| <HIGH-IPV6-ADDR>  | Specifies the highest IP address in the pool in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. |
| prefix-len <MASK> | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 64 to 128.                           |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context           | Authority                                                                          |
|--------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter                          | Description                                                                      |
|------------------------------------|----------------------------------------------------------------------------------|
| all-vrfs                           | Shows DHCPv6 server configuration settings for all VRFs.                         |
| leases {all-vrfs   vrf <VRF-NAME>} | Shows DHCPv6 server lease provided by the server for all VRFs or a specific VRF. |
| pool <POOL-NAME> [vrf <VRF-NAME>]  | Shows DHCPv6 server pool configuration settings for all VRFs or a specific VRF.  |

## Examples

Showing all DHCPv6 server configuration settings.

```
switch# show dhcpv6-server

VRF Name : default
DHCPv6 Server : enabled
Operational State : operational
Authoritative Mode : true
Config_status : Applied

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

DHCPv6 dynamic IP allocation

Start-IPv6-Address End-IPv6-Address Prefix-Length

2001::2 2001::10 64

DHCPv6 Server options

Option-Number Option-Type Option-Value

7 ipv6 2001::15

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
Config_status : Applied

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

DHCPv6 dynamic IP allocation

Start-IPv6-Address End-IPv6-Address Prefix-Length

2000::1 2000::20 *
```

```

2001::20 2001::50 *
2001::2 2001::10 64
2010::20 2010::40 *

```

DHCPv6 Server options

```

Option-Number Option-Type Option-Value

7 ipv6 2001::15
23 ipv6 2001::30
30 ipv6 2001::10

```

DHCPv6 Server static IP allocation

DHCPv6 Server static host is not configured.

```

Pool Name : v6test
Lease Duration : 00:01:00

```

DHCPv6 dynamic IP allocation

```

Start-IPv6-Address End-IPv6-Address Prefix-Length

2001::1 2001::20 64
2010::10 2010::30 *
2020::20 2020::60 *

```

DHCPv6 Server options

```

Option-Number Option-Type Option-Value

7 ipv6 2001::20
23 ipv6 2001:0db8:85a3:0000:0000:8a2e:0370:7334
2001:0db8:85a3:0000:0000:8a2e:0370:7335
2001:0db8:85a3:0000:0000:8a2e:0370:7336
2001:0db8:85a3:0000:0000:8a2e:0370:7337

```

DHCPv6 Server static IP allocation

```

IPv6-Address Client-Hostname State Client-Id

2100::4 * OPERATIONAL 1:0:a0:24:ab:fb:9c

```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms    | Command context | Authority                                                                                                                                                              |
|--------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8320 | 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. |

| Platforms | Command context | Authority |
|-----------|-----------------|-----------|
| 8325      |                 |           |
| 8325H     |                 |           |
| 8325P     |                 |           |
| 8360      |                 |           |
| 9300      |                 |           |
| 9300S     |                 |           |
| 10000     |                 |           |

## static-bind

```
static-bind ipv6 <IPv6-ADDR> client-id <ID> [hostname <HOST>]
no static-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.

| Parameter       | Description                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv6-ADDR>     | Specifies the IP address to assign in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> 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. |
| client-id <ID>  | Specifies the client identifier or DUID.                                                                                                                                                                                                         |
| hostname <HOST> | Specifies the host name of the client station. Range: 1 to 255 printable ASCII characters                                                                                                                                                        |

## 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

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                                                | Command context                        | Authority                                                                          |
|--------------------------------------------------------------------------|----------------------------------------|------------------------------------------------------------------------------------|
| 8100<br>8320<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | <code>config-dhcpv6-server-pool</code> | Administrators or local user group members with execution rights for this command. |

## Troubleshooting

### Client not getting IP address

- CoPP drop

In case of excessive DHCP traffic, CoPP does the rate limit by dropping some of the packets.

Check if client packets are getting dropped by CoPP using `show copp statistics class dhcp-ipv4` or `show copp statistics class dhcp-ipv6` commands.

- Configuration issues

- IP range within the pool should match the client connected interface IP subnet.

```
dhcp-server vrf default
 pool pool1
 range 172.16.10.1 172.16.10.20
 exit
enable
```

Check the scale numbers supported on the platform. For example the maximum number of VRFs, and pools supported on the platform.

- Check if the DHCP Server is configured in client VRF and is in enabled state.
- Check for server pool exhaustion.

- DHCP Relay co-existence

From AOS-CX 10.07 onwards, you can configure DHCP Relay and DHCP Server simultaneously. If both are enabled for an earlier release, then either the DHCP relay or the DHCP server will fail to start.

### DHCP Server daemon taking up high CPU [`dhcp-server-adapter`]

- Due to architectural limitations, the DHCP Server on boot up the CPU utilization is high for about 2 minutes; this is expected behavior.

- In the VSX setup, when the number of clients in the lease table is more, the server daemon will have high CPU usage while syncing leases between primary and secondary VSX peers. Once syncing is complete, then the CPU utilization comes back to normal.

## Check point restore

DHCP-Server configuration changes are not allowed when it is enabled. However, through check-point restore or TFTP configuration download or REST, you can change the configuration in the management VRF. This configuration change gets applied when the server is disabled and enabled.

From 10.10 onwards, a configuration flag icon is displayed in `show dhcp-server` command to indicate if there is any configuration that is not applied.

## FAQ

### 1. What ports use DHCP for switch assignments?

You can set up a DHCP switch with a management VRF port; if the management VRF port is unavailable, use an IN-Band data port.

### 2. Is DHCP assignment available on boot up from the factory?

Yes, DHCP assignment is available on boot up from the factory. This assists Zero Touch depending on the platform; this can be a management VRF or an IN-Band data port on the default VLAN 1.

### 3. Is DHCP assignment available on both management VRF and IN-Band data ports simultaneously?

Yes, DHCP assignment is possible on both management VRF and IN Band data ports, but it depends on the platform.

If both ports can get a DHCP address, the DHCP address from the management VRF port is used for Zero Touch Provisioning instead of the one from the IN-Band data port. The data ports will wait 30 seconds before taking ownership of Zero Touch Provisioning (ZTP).

### 4. Which VLAN is assigned a DHCP address?

The factory default VLAN to which the DHCP address is assigned is VLAN1.

Users can configure the VLAN for DHCP allocation on platforms supporting multiple VLAN configurations. Only a single VLAN can support DHCP assignments.

### 5. Can DHCP assignments be disabled in an HPE Aruba Networking AOS-CX switch?

Use the `no ip dhcp` command on the required VLAN interface or management VRF port you can disable the DHCP assignments in an HPE Aruba Networking AOS-CX switch.

A static configuration option is available on both ports.

### 6. Can IP DHCP switch assignment be carried out on a Routed only Port (RoP)?

No, RoP is not supported. Only VLAN and OOBM ports can be allocated an address with DHCP.

### 7. Can an HPE Aruba Networking AOS-CX switch support DHCP IPv6 Allocation?

Yes, an HPE Aruba Networking AOS-CX switch can support DHCP IPv6 allocation. However, for Zero Touch Provisioning (ZTP), IPv4 is required.

### 8. Do HPE Aruba Networking AOS-CX switches support DHCP server?

Since the software release of AOS-CX 10.10, all platforms support DHCP server, except for 6100, 6000, and 4100i.

### **9. Can HPE Aruba Networking AOS-CX switches support DHCP address exclusion from a subnet?**

Not formally; however, you can use static bindings to unused MAC addresses as a workaround on a smaller scale.

### **10. Do all HPE Aruba Networking AOS-CX switches support DHCP helper?**

Since the software release of AOS-CX 10.10, all platforms support DHCP helper for IPv4 and IPv6.

### **11. Can DHCP Server and Relay simultaneously be supported on a switch?**

Yes, since the software release AOS-CX 10.08, the platforms that support DHCP Server and Relay both can be set up simultaneously.

### **12. How many helper addresses can be used?**

The Switched Virtual Interface can use up to eight helper addresses for IPv4 and IPv6.

### **13. Is DHCP Relay supported for multi-netted addresses?**

Yes, for both IPv4 and IPv6 DHCP Relay supports multi-netted addresses. The Gateway IP Address (GIADDR) used in the DHCP request will be the lowest IP address configured on the interface.

You can override the lowest IP address using the `bootp-gateway` command. IPV6 does not support `bootp`.

### **14. Can a multi-netted address support GIADDR from a different address?**

Yes, for IPv4 only. For more information, see [DHCP relay agent](#).

### **15. Can the binding of DHCP and IP remain after a switch reboot?**

Yes, the binding of DHCP and IP remains by using an external storage option `dhcpv4-snooping external-storage`.

### **16. If multiple 'ip-helper' IPs are configured for DHCP relay on an interface or SVI, which switch will forward the DHCP requests?**

In case of multiple 'ip-helper' IPs configured for DHCP relay on an interface or SVI, the client will receive multiple offers from different DHCP servers, and the client will choose which one to accept.

### **17. What happens when global *dhcp-smart-relay* is enabled in an interface or SVI with multiple IP addresses (multi-netting) that services DHCP clients in different subnets?**

On enabling global `dhcp-smart-relay` in an interface or SVI with multiple IP addresses (multi-netting) that services DHCP clients in different subnets, the AOS-CX device will first use the primary interface or SVI IP address as the unicast source to the DHCP server. If no response is received the AOS-CX device will use the secondary IPs from the lowest-numbered IP to the highest until a DHCP response is received.

### **18. What are the troubleshooting commands for DHCP relay agent?**

The initial troubleshooting for DHCP relay agent can be done using the following commands:

- `show dhcp-relay`
- `show dhcp-relay bootp-gateway`
- `show ip helper-address`

Next level of troubleshooting can be done by taking packets captured at the DHCP server side and AOS-CX side. For more information about AOS-CX packet capture, see *Mirroring* chapter of *AOS-CX Monitoring Guide*.

Perform additional AOS-CX side DHCP debugging using **`debug dhcprelay`** and **`debug dhcpv6relay`** commands. For more information, see *Debug logging* chapter of *AOS-CX Diagnostics and Supportability Guide*.



---

Applies only to the 8100, 8325, 8360 and 10000 Switch Series.

---

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.

---

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](#).

---



---

On 10000 series switches, DHCP snooping and PSM/Distributed Services (DSS) are mutually exclusive. If both features are enabled, unexpected behavior may occur.

---

### DHCPv6 guard

The DHCPv6 guard feature is an extension of DHCPv6 snooping. When the DHCPv6 snooping feature is configured globally and on the VLAN, the ports are configured as trusted and untrusted ports on the VLAN. DHCPv6 guard enhances this feature by creating a policy and applying it on a port and VLAN. This policy contains multiple attributes which are compared against the packet that is received on trusted ports. If the packet complies with the attributes of the policy, it is forwarded to the destination port; otherwise the packet is dropped.

## DHCP server interoperation

DHCP server can not be configured with DHCP snooping.

## DHCPv4 snooping conditions for dropping DHCPv4 packets

Applies only to DHCPv4 snooping.

| Packet types that are dropped | Conditions for dropping the packets                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCPOFFER, DHCPACK, DHCPNACK  | <ul style="list-style-type: none"><li>▪ A packet from a DHCP server is received on an untrusted port.</li><li>▪ The switch is configured with a list of authorized DHCP server addresses and a DHCP response received on a trusted port, but the source IP address is not an authorized DHCP server.</li></ul> |
| DHCPRELEASE, DHCPDECLINE      | <ul style="list-style-type: none"><li>▪ 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.</li></ul>                                                                                   |
| All DHCP packet types         | <ul style="list-style-type: none"><li>▪ 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.</li><li>▪ A DHCP packet containing DHCP relay information (option 82) is received on an untrusted port.</li></ul>       |

## Protocol details

1. In a VSX setup, the configured VSX Primary switch writes IP binding entries to an external storage file. If the VSX Primary switch reboots, the IP Binding entries will not be synced to the external storage file until the VSX Primary switch comes back up. Once the VSX Primary switch comes up, it will sync entries from the VSX secondary switch and write the consolidated bindings to external storage.
2. In a VSX setup, external storage should be configured only after the VSX role is configured.
3. In a VSX setup, once external storage is configured, the VSX switch role should not be changed. If there is a need to change the role, do so using these steps:
  - a. Remove DHCPv4-Snooping external storage.
  - b. Change the VSX role.
  - c. Configure DHCPv4-Snooping external storage
4. When a port is configured as a trusted port, all the dynamic IP binding entries learned on that port will be deleted.
5. When a client is connected on a trusted port, the dynamic IP binding entries will not be learned on the switch, even though the client gets an IP address.
6. If DHCPv4 snooping is enabled on two back-to-back access switches, DHCP packets will be dropped, Since by default option 82 is enabled on DHCPv4 snooping and the default policy is drop. The second switch with DHCPv4 snooping enabled drops the packets. In this scenario the user should enable DHCPv4 snooping option 82 on one switch, or else you can disable on both.
7. 8360 Switch Series: VXLAN is trusted by default for DHCPv4 and DHCPv6 snooping over VXLAN. VXLAN operational status must be in the forward state to forward the packets over VXLAN tunnel. DHCPv4 snooping is supported over VxLAN IPv4 and IPv6 underlay.

- 8100 Switch Series: DHCPv4 snooping, DHCPv6 snooping, and ND-snooping is supported over VxLAN IPv6 underlay.

## Supported platform and standards

The following table list the supported platforms for DHCP snooping.

**Table 1:** Support platforms for DHCP snooping

| Platform         | DHCP snooping |
|------------------|---------------|
| 8320             | No            |
| 8325/8325H/8326P | Yes           |
| 8360             | Yes           |
| 9300             | No            |
| 9300S            | No            |
| 1000             | Yes           |

**Table 2:** Scale

| Platform         | IP Bindings per port | IP Bindings per device |
|------------------|----------------------|------------------------|
| 8325/8325H/8325P | 2048                 | 2048                   |
| 8360             | 2048                 | 2048                   |
| 10000            | 2048                 | 2048                   |

## Configuring DHCPv4 and v6 snooping over VXLAN overlay

### Procedure

1. Configure VXLAN overlay setup to establish the VxLAN tunnel. For more information, see *AOS-CX VXLAN EVPN Guide*.
2. Validate whether the tunnel is established between the VTEPS (either static or EVPN) with the command `show interface vxlan vteps`.

The status of the tunnel should be operational in order to forward the packets.

3. Configure DHCPv4 and v6 snooping in the global and VLAN contexts with the commands `dhcpv4-snooping` and `dhcpv6-snooping`.
4. Configure the server connected port as trusted with the commands `dhcpv4-snooping trust` and `dhcpv6-snooping trust`.

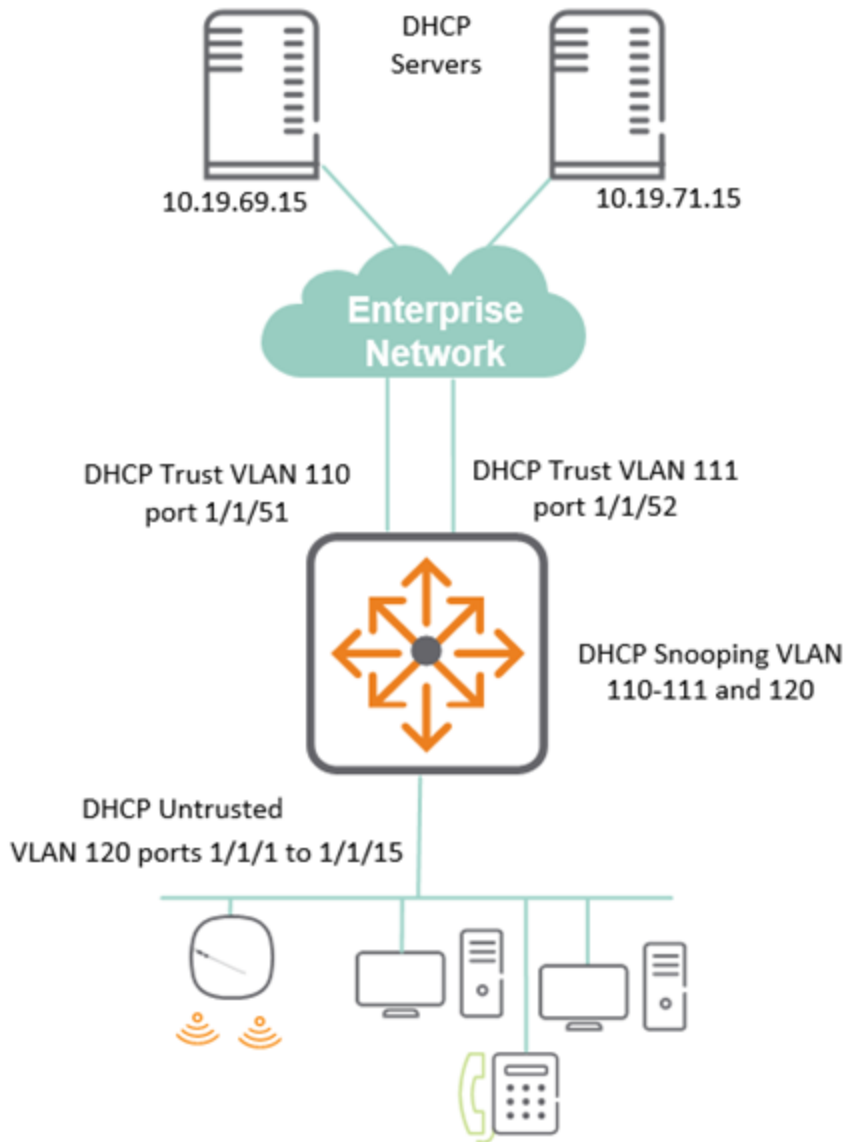
If the server is connected through the VXLAN tunnel, then this step can be ignored. This is because VXLAN is trusted by default for DHCPv4 and DHCPv6 snooping over VXLAN.

5. Validate the DHCPv4 and v6 snooping configuration with the commands `show dhcpv4-snooping` and `show dhcpv6-snooping`.

## DHCPv4 Snooping Use case

DHCP Snooping is used to protect from rogue or unwanted attacks from posing DHCP services. In the following use case:

- Set the switch for DHCPv4 snooping.
- Allow DHCP communication from the uplinks in the Enterprise network port 1/1/51 and 1/1/52.
- For communication to occur, identify the authorized DHCP servers 10.19.69.15 and 10.19.71.15.
- LAN facing user ports 1/1/1 to 1/1/15 is not configured as trusted.



Key configuration portion for above set up is shown with the relevant DHCPv4 snooping parameters:

```
dhcpv4-snooping <--enable DHCPv4 snooping
dhcpv4-snooping authorized-server 10.19.69.15 <--allow authorized servers
dhcpv4-snooping authorized-server 10.19.71.15
vlan 110
 description uplink
 dhcpv4-snooping <--enable DHCPv4 snooping
```

```

on required VLANs
vlan 111
 description uplink
 dhcpv4-snooping
vlan 120
 description User
 dhcpv4-snooping
interface 1/1/1
 no shutdown
 description User
 vlan access 120

...

interface 1/1/15
 no shutdown
 description User
 vlan access 120
interface 1/1/51 <--Unlinks on 1/1/51 and 52 trusted
 no shutdown
 vlan trunk native 1
 vlan trunk allowed 110
 dhcpv4-snooping trust
interface 1/1/52
 vlan trunk native 1
 vlan trunk allowed 111
 dhcpv4-snooping trust
interface vlan 110
 description uplink
 ip address 172.16.69.1/30
interface vlan 111
 description uplink
 ip address 172.16.71.1/30
interface vlan 120
 description User
 ip address 172.16.10.1/254
 ip helper-address 10.19.69.15
 ip helper-address 10.19.71.15
...
ip route 0.0.0.0/0 172.16.69.2 distance 10
ip route 0.0.0.0/0 172.16.71.2 distance 20
...

```

Using the show dhcpv4-snooping command, you can see some of the following DHCPv4 information:

- Applied VLANs for snooping, 110-112 and 120
- The untrusted policy is set to drop packets
- The list of authorized DHCP servers are set to 10.19.69.15 and 10,19.71.15
- Set the trusted or untrusted ports and any DHCP bindings for those ports. Port 1/1/1 and 1/1/2 offer DHCP.

```

show dhcpv4-snooping

DHCPv4-Snooping Information

DHCPv4-Snooping : Yes Verify MAC Address : Yes
Allow Overwrite Binding : No Enabled VLANs : 110-111,120
IP Binding Disabled VLANs :
Static Attributes : No

```

```

Client Event Logs : No

Option 82 Configurations

Untrusted Policy : drop Insertion : Yes
Option 82 Remote-id : mac

External Storage Information

Volume Name : --
File Name : --
Inactive Since : --
Error : --

Flash Storage Information

File Write Delay : --

Active Storage : --

Authorized Server Configurations

VRF Authorized Servers

default 10.19.69.15
default 10.19.71.15

Port Information

Port Trust Max Static Dynamic
----- -
1/1/51 Yes 0 0 0
1/1/52 Yes 0 0 0
1/1/1 No 1024 0 1
1/1/2 No 1024 0 1

!
!output omitted
!
1/1/14 No 1024 0 0
1/1/15 No 1024 0 0

```

## DHCP snooping commands

### clear dhcp-snooping binding

```
clear dhcp-snooping binding {all | ip <IP-ADDR> vlan <VLAN-ID> | port <PORT-NUM> | vlan <VLAN-ID>}
```

#### Description

Clears DHCP snooping binding entries.

| Parameter | Description                                                   |
|-----------|---------------------------------------------------------------|
| all       | Specifies that all DHCP binding information is to be cleared. |

| Parameter                                            | Description                                                                                |
|------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <code>ip &lt;IP-ADDR&gt; vlan &lt;VLAN-ID&gt;</code> | Specifies the IP address and VLAN for which all DHCP binding information is to be cleared. |
| <code>port &lt;PORT-NUM&gt;</code>                   | Specifies the port number for which all DHCP binding information is to be cleared.         |
| <code>vlan &lt;VLAN-ID&gt;</code>                    | Specifies the VLAN for which all DHCP binding information is to be cleared.                |

## Examples

Clearing all DHCP binding information for IP address 192.168.2.4 and VLAN 5:

```
switch(config)# clear dhcp-snooping binding ip 192.168.2.4 vlan 5
```

Clearing all DHCP binding information for port 1/1/1:

```
switch(config)# clear dhcp-snooping binding port 1/1/1
```

Clearing all DHCP binding information for VLAN 10:

```
switch(config)# clear dhcp-snooping binding vlan 10
```

Clearing all DHCP binding information:

```
switch(config)# clear dhcp-snooping binding all
```

## Command History

| Release          | Modification                                                                                                                                                    |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . The <b>ipv4</b> parameter is deprecated and replaced with <b>ip</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                                                                                        |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                                                                                                  |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                                                                                         |
| 10.07 or earlier |                                                                                                                                                                 |

## Command Information

| Platforms    | Command context             | Authority                                                                                                                  |
|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325 | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this |

| Platforms                       | Command context | Authority                                   |
|---------------------------------|-----------------|---------------------------------------------|
| 8325H<br>8325P<br>8360<br>10000 |                 | command from the operator context (>) only. |

## clear dhcp-snooping statistics

```
clear dhcp-snooping statistics
```

### Description

Clears all DHCP snooping statistics.

### Examples

Clear all DHCP snooping statistics:

```
switch# clear dhcp-snooping statistics
```

### Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

### Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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. |

## dhcp-snooping

```
dhcp-snooping
no dhcp-snooping
```

### Description

Enables DHCP snooping. DHCP snooping is disabled by default. DHCP snooping is not supported on the management interface.

The **no** form of the command disables DHCP snooping, flushing all the IP bindings learned since DHCP snooping was enabled.

## Examples

Enabling DHCP snooping:

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

Disabling DHCP snooping:

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

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping (in config-vlan context)

```
dhcp-snooping
no dhcp-snooping
```

### Description

Enables DHCP snooping for the specified VLAN in the **config-vlan** context. DHCP snooping is disabled by default for all VLANs.

The no form of the command disables DHCP snooping on the specified VLAN, flushing all the IP bindings learned for this VLAN since DHCP snooping was enabled for this VLAN.

### Examples

Enabling DHCP snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# dhcp-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Disabling DHCP snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no dhcp-snooping
switch(config-vlan-100)# exit
switch(config)#
```

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config-vlan     | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping allow-overwrite-binding

```
dhcp-snooping allow-overwrite-binding
no dhcp-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 DHCP snooping overwrite binding.

### Examples

Enabling DHCP snooping overwrite binding:

```
switch(config) # dhcp-snooping allow-overwrite-binding
```

Disabling DHCP snooping overwrite binding:

```
switch(config) # no dhcp-snooping allow-overwrite-binding
```

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping authorized-server

```
dhcp-snooping authorized-server <IP-ADDR> [vrf <VRF-NAME>]
no dhcp-snooping authorized-server <IP-ADDR> [vrf <VRF-NAME>]
```

### Description

Adds an authorized (trusted) DHCP server to a list of authorized servers for use by DHCP 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 DHCP 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                                          |
|----------------|------------------------------------------------------|
| <IP-ADDR>      | Specifies the IP address of the trusted DHCP server. |
| vrf <VRF-NAME> | Specifies the VRF name.                              |

## 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)# dhcp-snooping authorized-server 192.168.2.2
switch(config)# dhcp-snooping authorized-server 192.168.2.3 vrf default
switch(config)# dhcp-snooping authorized-server 192.168.2.10 vrf default
```

Removing DHCP server 192.168.2.3 from the authorized server list:

```
switch(config)# no dhcp-snooping authorized-server 192.168.2.3 vrf default
```

## Command History

| Release    | Modification                                                                              |
|------------|-------------------------------------------------------------------------------------------|
| 10.14      | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11      | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000 | Command introduced for the 8360 Switch Series.                                            |

## Command Information

| Platforms                                       | Command context     | Authority                                                                          |
|-------------------------------------------------|---------------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | <code>config</code> | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping event-log client

```
dhcp-snooping event-log client
no dhcp-snooping event-log client
```

### Description

This command enables or disables dhcp-snooping client level event logs that help with client telemetry on a remote management station such as HPE Aruba Networking Central. By default, client level event logs are disabled. The **no** form of this command disables client-level event logs for DHCP snooping after they are enabled. View these logged DHCP snooping events by issuing the command **show events -c dhcp-snooping**.



For additional information on DHCP-related event logging, please refer to the Event Log Message Reference Guide.

## Examples

Enabling DHCP client level event logs:

```
switch(config)# dhcp-snooping event-log client
```

Disabling external storage:

```
switch(config)# no dhcp-snooping event-log client
```

## Command History

| Release | Modification                                                                              |
|---------|-------------------------------------------------------------------------------------------|
| 10.14   | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.12   | Command introduced for the 8100 and 8360 Switch Series.                                   |
| 10.11   | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.10   | Command introduced.                                                                       |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping external-storage

```
dhcp-snooping external-storage volume <VOL-NAME> file <FILE-NAME>
no dhcp-snooping external-storage volume <VOL-NAME> file <FILE-NAME>
```

### Description

Configures external storage to be used for backing up IP bindings (used by DHCP 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.



| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| volume <VOL-NAME> | Specifies the name of the existing external storage volume where the IP bindings file will be saved. Before running the <b>dhcp-snooping external-storage volume</b> command, first create the external storage volume using command <b>external-storage &lt;VOLUME-NAME&gt;</b> . See <i>External storage commands</i> in the <i>Command-Line Interface Guide</i> . |
| file <FILE-NAME>  | Specifies the file name to use for storing IP bindings. Maximum 255 characters.                                                                                                                                                                                                                                                                                      |

Configuring IP bindings storage in file **dsnoop\_ipbindings** on existing volume **dhcp\_snoop**:

```
switch(config)# dhcp-snooping external-storage volume dhcp_snoop file dsnoop_ipbindings
```

Disabling external storage:

```
switch(config)# no dhcp-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 dhcp-snooping external-storage volume dhcp_snoop
dhcp-snooping will use flash storage to store IP Binding database
switch(config)#
```

## Command History

| Release    | Modification                                                                              |
|------------|-------------------------------------------------------------------------------------------|
| 10.14      | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11      | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000 | Command introduced for the 8360 Switch Series.                                            |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping flash-storage

```
dhcp-snooping flash-storage [delay <DELAY>]
```

```
no dhcp-snooping flash-storage [delay <DELAY>]
```

## Description

Configures switch flash storage to be used for backing up client IP bindings (used by DHCP 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 **dhcp-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     | Description                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------|
| delay <DELAY> | Specifies the delay in seconds between writes (when necessary) to the flash storage, Default: 900. Range: 300 to 86400. |

---

## Examples

Configuring switch flash storage for DHCP snooping IP binding storage with a write delay of 1200 seconds:

```
switch(config)# dhcp-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 dhcp-snooping flash-storage
```

## Command History

| Release    | Modification                                                                              |
|------------|-------------------------------------------------------------------------------------------|
| 10.14      | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11      | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000 | Command introduced for the 8360 Switch Series.                                            |
| 10.09      | Command introduced for the 6000 and 6100 Switch Series.                                   |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping max-bindings

```
dhcp-snooping max-bindings <MAX-BINDINGS>
no dhcp-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 binding is the maximum value of the range.

The no form of the command reverts max bindings for the selected interface to its default.

| Parameter      | Description                                                                     |
|----------------|---------------------------------------------------------------------------------|
| <MAX-BINDINGS> | Specifies the maximum number of DHCP bindings. Range: 1 to 2000.Range 1 to 2048 |

### Examples

Set the DHCP max bindings to 256 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# dhcp-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

Revert DHCP max bindings to its default on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no dhcp-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

### Command History

| Release    | Modification                                                                              |
|------------|-------------------------------------------------------------------------------------------|
| 10.14      | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11      | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000 | Command introduced for the 8360 Switch Series.                                            |
| 10.09      | Command introduced for the 6000 and 6100 Switch Series.                                   |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config-if       | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping option 82

```
dhcp-snooping option 82 [remote-id {mac | subnet-ip | mgmt-ip}][untrusted-policy {drop | keep | replace}]
no dhcp-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 (**dhcp-snooping option 82**), this default configuration is used:

```
dhcp-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 DHCP snooping option 82.

| Parameter        | Description                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| remote-id        | 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: |
| mac              | The default. Uses the switch MAC address as the remote ID.                                                                                                |
| subnet-ip        | Uses the IP address of the client VLAN as the remote ID.                                                                                                  |
| untrusted-policy | Specifies what action to take for DHCP packets (with option 82) that are received on untrusted ports. Specify one of these actions:                       |
| drop             | The default. Drop DHCP packets (with option 82) without forwarding them.                                                                                  |

| Parameter | Description                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| keep      | Forward DHCP packets (with option 82).                                                                                                                                                |
| replace   | Replace the option 82 information in the DHCP packets with whatever is set for <b>remote-id</b> (one of: <b>mac</b> , <b>subnet-ip</b> , or <b>mgmt-ip</b> ) and forward the packets. |

## Examples

Configuring DHCP snooping option 82 with the keep action:

```
switch(config)# dhcp-snooping option 82 untrusted-policy keep
```

Configuring DHCP snooping option 82 with `mgmt-ip` as the `remote-id` and the `replace` action:

```
switch(config)# dhcp-snooping option 82 remote-id mgmt-ip untrusted-policy replace
```

Disabling DHCP snooping option 82:

```
switch(config)# no dhcp-snooping option 82 untrusted-policy keep
```

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier | Command introduced                                                                        |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping static-attributes

```
dhcp-snooping static-attributes
no dhcp-snooping static-attributes
```

## Description

Enables storage of static attributes provided to the DHCP client by DHCP server during DHCP packet exchange. Disabled by default. When enabled, the following attributes are stored in OVSDDB along with the client IP binding entry:

1. Name server IP addresses: DNS server IPs provided by the DHCP server to the client. Maximum: 3 per client.
2. Default gateway IP address: Router IP addresses provided by DHCP server to the client. Maximum: 3 per client.
3. Server IP address: IP address of the DHCP server that leased the IP to the client.

The **no** form of the command disables storing of client static attributes. After disabling, existing client static attributes will be flushed.

## Examples

Enabling the storage of DHCP snooping static attributes:

```
switch(config)# dhcp-snooping static-attributes
```

Disabling the storage of DHCP snooping static attributes:

```
switch(config)# no dhcp-snooping static-attributes
```

## Command History

| Release | Modification                                                                              |
|---------|-------------------------------------------------------------------------------------------|
| 10.14   | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11   | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.10   | Command introduced.                                                                       |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping trust

```
dhcp-snooping trust
no dhcp-snooping trust
```

## Description

Enables DHCP 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 DHCP snooping trust on the selected port.

## Examples

Enabling DHCP snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# dhcp-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling DHCP snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no dhcp-snooping trust
switch(config-if)# exit
switch(config)#
```

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config-if       | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping tunnel vxlan trust

```
dhcp-snooping tunnel vxlan trust
no dhcp-snooping tunnel vxlan trust
```

### Description

Enables dhcp-snooping trust on all VxLAN tunnels.

The no form of the command to marks all VxLAN tunnels as untrusted.

By default, all VxLAN tunnel interfaces are trusted. When trust is disabled on VxLAN tunnel interfaces:

- DHCP broadcast packets are not forwarded on VxLAN tunnels.
- DHCP server packets received on VxLAN tunnel interfaces are discarded.

## Examples

Enabling trust on all VxLAN tunnel interfaces:

```
switch(config)# dhcp-snooping tunnel vxlan trust
```

Disabling trust on all VxLAN tunnel interfaces:

```
switch(config)# no dhcp-snooping tunnel vxlan trust
```

## Command History

| Release    | Modification                                                                              |
|------------|-------------------------------------------------------------------------------------------|
| 10.14      | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11.1000 | Command introduced.                                                                       |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-snooping verify mac

```
dhcp-snooping verify mac
no dhcp-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 DHCP snooping MAC verification.

### Examples

Enabling DHCP snooping MAC verification:

```
switch(config)# dhcp-snooping verify mac
```

Disabling DHCP snooping MAC verification:

```
switch(config)# no dhcp-snooping verify mac
```

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## show dhcp-snooping

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

### Description

Shows the DHCP 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

Showing the DHCP snooping configuration:

```
switch# show dhcp-snooping

dhcp-snooping Information

dhcp-snooping : Yes Verify MAC Address : Yes
```

```

Allow Overwrite Binding : No Enabled VLANs : 1-100
Static Attributes : Yes
Client Event Logs : Yes

```

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

| VRF     | Authorized Servers |
|---------|--------------------|
| default | 1.1.10.3           |
| default | 10.10.10.1         |
| default | 10.10.10.56        |
| default | 200.10.10.3        |
| green   | 1.1.10.3           |
| green   | 1.10.10.3          |
| green   | 10.10.100.3        |
| red     | 192.168.122.53     |
| red     | 192.168.122.121    |

Port Information

| Port     | Trust | Max Bindings | Static Bindings | Dynamic Bindings |
|----------|-------|--------------|-----------------|------------------|
| 1/1/2    | Yes   | 5000         | 50              | 0                |
| 1/1/3    | Yes   | 8192         | 0               | 0                |
| 1/1/5    | Yes   | 8192         | 0               | 22               |
| 1/1/16   | No    | 100          | 0               | 0                |
| 10/10/10 | No    | 8100         | 320             | 200              |
| lag120   | No    | 512          | 0               | 0                |

## Command History

| Release    | Modification                                                                              |
|------------|-------------------------------------------------------------------------------------------|
| 10.14      | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11      | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000 | Command introduced for the 8360 Switch Series.                                            |
| 10.09      | Command introduced for the 6000 and 6100 Switch Series.                                   |

| Release          | Modification                                    |
|------------------|-------------------------------------------------|
| 10.08            | Updated example with flash storage information. |
| 10.07 or earlier |                                                 |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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 dhcp-snooping binding

```
show dhcp-snooping binding [vsx-peer][detail]
```

### Description

Shows the DHCP snooping binding 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. |
| detail    | Shows detailed information for active IP bindings on the system.                                                                                                                                                                 |

### Examples

Showing the DHCP snooping binding configuration:

```
switch(config)# show dhcp-snooping binding

 MacAddress IP VLAN Interface Time-Left

aa:b1:c1:dd:ee:ff 10.2.3.4 1 1/1/2 582
aa:b2:c2:dd:ee:ff 10.2.3.5 1 1/1/2 584
```

Showing detailed information for active IP bindings:

```
switch(config)# show dhcp-snooping binding detail

VLAN Id : 2, MAC : 00:50:56:96:74:46

 IP Interface Time-Left

100.1.2.100 1/1/23 194
```

```

Static Attributes:
Default Router : 100.1.2.1, 192.1.1.1, 1.1.1.2
Server IP : 10.1.84.2
Name Servers : 192.1.1.2, 2.2.2.2, 1.1.1.1

```

VLAN Id : 3, MAC : 00:50:56:96:e5:8e

```

IP Interface Time-Left

100.1.3.100 2/1/22 145

```

```

Static Attributes:
Default Router : 100.1.3.1, 192.1.1.1, 1.1.1.2
Server IP : 10.1.84.2
Name Servers : 192.1.1.2, 2.2.2.2, 1.1.1.1

```

VLAN Id : 3, MAC : 00:11:01:00:00:03

```

IP Interface Time-Left

100.1.3.99 2/1/24 137

```

```

Static Attributes:
Default Router : 100.1.3.1, 192.1.1.1, 1.1.1.2
Server IP : 10.1.84.2
Name Servers : 192.168.0.1, 192.168.1.1, 192.168.2.1

```

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.10            | Detail parameter added.                                                                   |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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 dhcp-snooping statistics

```
show dhcp-snooping statistics [vsx-peer]
```

## Description

Shows the DHCP snooping statistics.

| 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

Showing the DHCP snooping statistics:

```
switch(config)# show dhcp-snooping statistics
```

| Packet-Type | Action  | Reason                        | Count |
|-------------|---------|-------------------------------|-------|
| server      | forward | from trusted port             | 5425  |
| client      | forward | to trusted port               | 3895  |
| server      | drop    | received on untrusted port    | 117   |
| server      | drop    | unauthorized server           | 214   |
| client      | drop    | destination on untrusted port | 78    |
| client      | drop    | untrusted option 82 field     | 85    |
| client      | drop    | bad DHCP release request      | 0     |
| client      | drop    | failed verify MAC check       | 5     |
| client      | drop    | failed on max-binding limit   | 15    |

## Command History

| Release          | Modification                                                                              |
|------------------|-------------------------------------------------------------------------------------------|
| 10.14            | The <b>dhcpv4-snooping</b> keyword is deprecated and replaced with <b>dhcp-snooping</b> . |
| 10.11            | Command introduced for the 8325 and 10000 Switch Series.                                  |
| 10.09.1000       | Command introduced for the 8360 Switch Series.                                            |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.                                   |
| 10.07 or earlier |                                                                                           |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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. |

# 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.

| Parameter                     | Description                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------|
| all                           | Specifies that all DHCPv6 binding information is to be cleared.                                 |
| ip <IPV6-ADDR> vlan <VLAN-ID> | Specifies the IPv6 address and VLAN for which all DHCPv6 binding information is to be cleared.  |
| interface <IFNAME>            | Specifies the interface for which all DHCPv6 binding information is to be cleared.              |
| vlan <VLAN-ID>                | Specifies the VLAN for which all DHCPv6 binding information is to be cleared. Range: 1 to 4094. |

### Examples

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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000       | Command introduced for the 8360 Switch Series.           |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.  |
| 10.07 or earlier |                                                          |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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. |

## clear dhcpv6-snooping guard-policy statistics

```
clear dhcpv6-snooping guard-policy statistics [vlan <VLAN-ID> | interface <INTERFACE-NAME>]
```

### Description

Clears all DHCPv6 snooping guard policy statistics from the specified VLAN or interface.

| Parameter        | Description                           |
|------------------|---------------------------------------|
| <VLAN-ID>        | Specifies the VLAN ID. Range: 1-4094. |
| <INTERFACE-NAME> | Specifies the interface name.         |

### Examples

Clearing all DHCPv6 snooping guard policy statistics from VLAN 100:

```
switch# clear dhcpv6-snooping guard-policy statistics vlan 100
```

Clearing all DHCPv6 snooping guard policy statistics from interface 1/1/10:

```
switch# clear dhcpv6-snooping guard-policy statistics interface 1/1/10
```

### Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms             | Command context             | Authority                                                                                                                                                              |
|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H | 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. |

| Platforms              | Command context | Authority |
|------------------------|-----------------|-----------|
| 8325P<br>8360<br>10000 |                 |           |

## 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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000       | Command introduced for the 8360 Switch Series.           |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.  |
| 10.07 or earlier |                                                          |

### Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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. |

## 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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000       | Command introduced for the 8360 Switch Series.           |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.  |
| 10.07 or earlier |                                                          |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000       | Command introduced for the 8360 Switch Series.           |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.  |
| 10.07 or earlier |                                                          |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config-vlan     | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter                         | Description                                              |
|-----------------------------------|----------------------------------------------------------|
| <code>&lt;IPV6-ADDR&gt;</code>    | Specifies the IPv6 address of the trusted DHCPv6 server. |
| <code>vrf &lt;VRF-NAME&gt;</code> | Specifies the VRF name.                                  |

## 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

| Release    | Modification                                             |
|------------|----------------------------------------------------------|
| 10.11      | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000 | Command introduced for the 8360 Switch Series.           |

## Command Information

| Platforms                                       | Command context     | Authority                                                                          |
|-------------------------------------------------|---------------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | <code>config</code> | Administrators or local user group members with execution rights for this command. |

## dhcpv6-snooping event-log client

```
dhcpv6-snooping event-log client
no dhcpv6-snooping event-log client
```

### Description

This command enables or disables DHCPv6 snooping client level event logs that help with client telemetry on a remote management station such as HPE Aruba Networking Central. By default, client level event logs are disabled. The **no** form of this command disables client-level event logs for DHCPv6 snooping after they are enabled. View these logged DHCPv6 snooping events by issuing the command `show events -c dhcpv6-snooping`.



For additional information on DHCP-related event logging, please refer to the Event Log Message Reference Guide.

## Examples

Enabling DHCPv6 client level event logs:

```
switch(config)# # dhcpv6-snooping event-log client
```

Disabling external storage:

```
witch(config)# # no dhcpv6-snooping event-log client
```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.12   | Command introduced for the 8100 and 8360 Switch Series.  |
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| volume <VOL-NAME> | Specifies the name of the existing external storage volume where the IPv6 bindings file will be saved. Before running the <code>dhcpv6-snooping external-storage volume</code> command, first create the external storage volume using command <code>external-storage &lt;VOLUME-NAME&gt;</code> . See <i>External storage commands</i> in the <i>Command-Line Interface Guide</i> . |
| file <FILE-NAME>  | Specifies the file name to use for storing IPv6 bindings. Maximum 255 characters.                                                                                                                                                                                                                                                                                                    |

## 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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.08            | Updated example with flash storage information.          |
| 10.07 or earlier | Command introduced                                       |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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                        | Description                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <code>delay &lt;DELAY&gt;</code> | Specifies the delay in seconds between writes (when necessary) to the flash storage, Default: 900. Range: 300 to 86400. |

---

## 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

| Release    | Modification                                             |
|------------|----------------------------------------------------------|
| 10.11      | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000 | Command introduced for the 8360 Switch Series.           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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 binding is the maximum value of the range.

The no form of the command reverts max bindings for the selected interface to its default.

| Parameter      | Description                                                      |
|----------------|------------------------------------------------------------------|
| <MAX-BINDINGS> | Specifies the maximum number of DHCP bindings. Range: 1 to 2000. |

### Examples

Set the DHCPv6 max bindings to 256 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# dhcpv6-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

Revert DHCPv6 max bindings to its default on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no dhcpv6-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

### Command History

| Release    | Modification                                             |
|------------|----------------------------------------------------------|
| 10.11      | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000 | Command introduced for the 8360 Switch Series.           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config-if       | Administrators or local user group members with execution rights for this command. |

## 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

Enabling DHCPv6 snooping trust on interface 2/2/1:

```
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:

```
switch(config)# interface 2/2/1
switch(config-if)# no dhcpv6-snooping trust
switch(config-if)# exit
switch(config)#
```

## Command History

| Release    | Modification                                             |
|------------|----------------------------------------------------------|
| 10.11      | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000 | Command introduced for the 8360 Switch Series.           |

## Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## dhcpv6-snooping tunnel vxlan trust

```
dhcpv6-snooping tunnel vxlan trust
no dhcpv6-snooping tunnel vxlan trust
```

### Description

Enables DHCPv6-snooping trust on all VxLAN tunnels.

The no form of the command to marks all VxLAN tunnels as untrusted.

By default, all VxLAN tunnel interfaces are trusted. When trust is disabled on VxLAN tunnel interfaces:

- DHCP broadcast packets are not forwarded on VxLAN tunnels.
- DHCP server packets received on VxLAN tunnel interfaces are discarded.

### Examples

Enabling trust on all VxLAN tunnel interfaces:

```
switch(config)# dhcpv6-snooping tunnel vxlan trust
```

Disabling trust on all VxLAN tunnel interfaces:

```
switch(config)# no dhcpv6-snooping tunnel vxlan trust
```

### Command History

| Release    | Modification        |
|------------|---------------------|
| 10.11.1000 | Command introduced. |

### Command Information

| Platforms                                       | Command context | Authority                                                                          |
|-------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## match server access-list

```
match server access-list <ACL-NAME>
no match server access-list <ACL-NAME>
```

## Description

Configures an access list to a DHCPv6 snooping guard policy, enabling the DHCPv6 snooping guard policy to allow or deny the specific DHCP server to assign an IPv6 address. If no filters are applied, DHCP server traffic from any source IP address is allowed in the trusted port.

The **no** form of the command removes the specified access list from the DHCPv6 snooping guard policy.

| Parameter                     | Description                                               |
|-------------------------------|-----------------------------------------------------------|
| <code>&lt;ACL-NAME&gt;</code> | Specifies the name of the IPv6 access list to be matched. |

## Examples

Creating an access-list acl1 on DHCPv6 snooping guard policy pol1 :

```
switch(config)# dhcpv6-snooping guard-policy pol1
switch(config-dhcpv6-guard-policy)# match server access-list acl1
```

Deleting the access list acl1 from the DHCPv6 snooping guard policy pol1:

```
switch(config)# dhcpv6-snooping guard-policy pol1
switch(config-dhcpv6-guard-policy)# no match server access-list acl1
```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms                                       | Command context            | Authority                                                                          |
|-------------------------------------------------|----------------------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config-dhcpv6-guard-policy | Administrators or local user group members with execution rights for this command. |

## match client prefix-list

```
match client prefix-list <PREFIX-LIST-NAME>
no match client prefix-list <PREFIX-LIST-NAME>
```

## Description

Configures a prefix-list for the DHCPv6 snooping guard policy enabling the policy to allow the assigned IPv6 addresses within a specific prefix range.

The **no** form of the command removes a prefix list from the DHCPv6 snooping guard policy.

| Parameter                             | Description                                 |
|---------------------------------------|---------------------------------------------|
| <code>&lt;PREFIX-LIST-NAME&gt;</code> | Specifies the name of the IPv6 prefix list. |

## Examples

Adding a prefix list named `pref1` to the `pol1` DHCPv6 snooping guard policy:

```
switch(config)# ipv6 prefix-list pref1 permit 2001:db8::/64 le 128
switch(config)# dhcpv6-snooping guard-policy pol1
switch(config-dhcpv6-guard-policy)# match client prefix-list pref1
```

Deleting the prefix list named `prf1` from the `pol1` DHCPv6 snooping guard policy:

```
switch(config)# dhcpv6-snooping guard-policy pol1
switch(config-dhcpv6-guard-policy)# no match client prefix-list <ipv6-prefix-list-name>
```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms                                       | Command context                         | Authority                                                                          |
|-------------------------------------------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | <code>config-dhcpv6-guard-policy</code> | Administrators or local user group members with execution rights for this command. |

## preference

```
preference [minimum | maximum] <VALUE>
no preference
```

### Description

Enables a DHCPv6 snooping guard policy to allow or deny the DHCPv6 servers in the specified server preference range. If not configured the minimum preference is set to 0 and maximum preference is set to 255.

The **no** form of the command removes the server preference limits on the specified DHCPv6 snooping guard policy.

| Parameter       | Description                                                                |
|-----------------|----------------------------------------------------------------------------|
| minimum <VALUE> | Specifies the minimum value for the server preference range. Range: 1-255. |
| maximum <VALUE> | Specifies the maximum value for the server preference range. Range: 1-255. |

## Examples

Setting the minimum and maximum server preference range to 6-250 on DHCPv6 snooping guard policy pol1:

```
switch(config)# dhcpv6-snooping guard-policy pol1
switch(config-dhcpv6-guard-policy)# preference min 6
switch(config-dhcpv6-guard-policy)# preference max 250
```

Disabling the server preference range on DHCPv6 snooping guard policy pol1:

```
switch(config)# dhcpv6-snooping guard-policy pol1
switch(config-dhcpv6-guard-policy)# no preference
```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms                                       | Command context            | Authority                                                                          |
|-------------------------------------------------|----------------------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | config-dhcpv6-guard-policy | Administrators or local user group members with execution rights for this command. |

## 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 |

## Parameter

## Description

VSX peer switch is not displayed. This parameter is available on switches that support VSX.

## Examples

Showing the DHCPv6 snooping configuration:

```
switch# show dhcpv6-snooping

DHCPv6-Snooping Information

DHCPv6-Snooping : Yes Enabled VLANs : 1,5,7,100-110
Trusted Port Bindings Enabled VLANs :
Client Event Logs : Yes

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
VRF Authorized Servers

default
2001:0db8:85a3:0000:0000:8a2e:0370:7334
default 2002::2
default 2004::1
red 2002::1
red 2002::2
red 2002::9
green 5000::1
green 5000::2
green 5000::3
green 5000::7
green 5000::8

Port Information

Port Trust Max Static Dynamic
----- Trust Bindings Bindings Bindings
1/1/2 Yes 0 0 0
1/1/3 Yes 0 3 0
1/1/5 Yes 0 22 0
1/1/16 No 256 0 20
10/10/10 No 256 12 7
lag120 No 256 3 0
```

## Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.08            | Updated example with flash storage information.          |
| 10.07 or earlier | Command introduced                                       |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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 dhcpv6-snooping binding

```
show dhcpv6-snooping binding [vsx-peer]
```

### Description

Shows the DHCPv6 snooping binding 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

Showing the DHCPv6 snooping binding configuration:

```
switch# show dhcpv6-snooping binding

IP Binding Information
=====
MAC-ADDRESS IPV6-ADDRESS VLAN INTERFACE
TIME-LEFT

00:50:56:96:e4:cf aaaa:bbbb:cccc:dddd:eeee:1234:5678:abcd 1 1/1/1
584
00:50:56:96:04:4d 1000::3 134 1/1/2
435
00:50:56:96:d8:3d 2000:1000::4 2002 lag123
21234
```

### Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000       | Command introduced for the 8360 Switch Series.           |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.  |
| 10.07 or earlier |                                                          |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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. |

## dhcpv6-snooping guard-policy

```
dhcpv6-snooping guard-policy <POLICY-NAME>
no dhcpv6-snooping guard-policy <POLICY-NAME>
```

### Description

Configures a DHCPv6 snooping guard policy with the given name and enters the guard policy configuration context.

The no form of the command disables the specified guard policy.

| Parameter     | Description                                                                    |
|---------------|--------------------------------------------------------------------------------|
| <POLICY-NAME> | Specifies the name of the DHCPv6 snooping guard policy.<br>Maximum length: 64. |

### Examples

Creating the DHCPv6 snooping guard policy name pol1:

```
switch(config)# dhcpv6-snooping guard-policy pol1
switch(config-guard-policy-pol1)#
```

Deleting the DHCPv6 snooping guard policy named pol1:

```
switch(config)# no dhcpv6-snooping guard-policy pol1
```

Creating the DHCPv6 snooping guard policy name pol1 on interface 1/1/1:



The DHCPv6 snooping guard policy applied on the port takes priority over the policy applied over VLAN.

```
switch(config)# interface 1/1/1
switch(config-if)# dhcpv6-snooping guard-policy pol1
```

Creating the DHCPv6 snooping guard policy name pol1 on a VLAN:

```
switch(config)# vlan 100
switch(config-vlan-100)# dhcpv6-snooping guard-policy pol1
```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms | Command context                     | Authority                                                                          |
|-----------|-------------------------------------|------------------------------------------------------------------------------------|
| 8100      | config                              | Administrators or local user group members with execution rights for this command. |
| 8325      | config-if                           |                                                                                    |
| 8325H     | config-dhcpv6-guard-policy          |                                                                                    |
| 8325P     | config-vlan- <i>&lt;VLAN-ID&gt;</i> |                                                                                    |
| 8360      |                                     |                                                                                    |
| 10000     |                                     |                                                                                    |

## show dhcpv6-snooping guard-policy

```
show dhcpv6-snooping guard-policy[<POLICY_NAME>] [vsx-peer]
```

### Description

Shows the DHCPv6 snooping guard policy configuration.

| Parameter                  | Description                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;POLICY-NAME&gt;</i> | Specifies the DHCPv6 snooping guard policy for which the information is displayed.                                                                                                                                               |
| 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 the DHCPv6 snooping guard policy configuration:

```
switch# show dhcpv6-snooping guard-policy
DHCPv6-Snooping guard-policy Information
```

```

DHCPV6 Guard Policy name : POL1
Attached Access List : ACL1
Attached Prefix List : PRF1
Preference Range : 0-255
Applied on VLAN : 5,7
Applied on Port

DHCPV6 Guard Policy name : POL2
Attached Access List : ACL2
Attached Prefix List : PRF2
Preference Range : 2-20
Applied on VLAN
Applied on Port : 1/1/1, 1/1/2

DHCPV6 Guard Policy name : POL3
Attached Access List : ACL3
Attached Prefix List : PRF3
Preference Range : 3-60
Applied on VLAN : 4,6
Applied on Port

```

Showing the DHCPv6 snooping guard policy configuration for the policy named POLICY\_NAME1:

```

switch# show dhcpv6-snooping guard-policy POLICY_NAME1

DHCPv6-Snooping guard-policy Information
=====
DHCPV6 Guard Policy name : POLICY_NAME1
Attached Access List : ACL1
Attached Prefix List : PRF1
Preference Range : 0-255
vsx-sync
Applied on VLAN : 5,7
Applied on Port : 1/1/1, 1/1/2

```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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 dhcpv6-snooping guard-policy interface

```
show dhcpv6-snooping guard-policy [interface <INTERFACE-NAME>] [vsx-peer]
```

## Description

Shows the DHCPv6 snooping guard policy configuration and statistics for the specified interface.

| Parameter                     | Description                                                                                                                                                                                                                      |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;INTERFACE-NAME&gt;</i> | Specifies the interface name for which the DHCPv6 guard counter information is displayed.                                                                                                                                        |
| <code>vsx-peer</code>         | 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 the DHCPv6 snooping guard policy configuration and statistics for interface 1/1/1:

```
switch# show dhcpv6-snooping guard-policy int 1/1/1
DHCPv6 Guard Policy Applied : poll
DHCPv6 Guard Policy Counters
=====
DHCPv6 Packets Received : 20
DHCPv6 Packets Forwarded : 5
DHCPv6 Packets Dropped : 15 [Total]
Access list error [7]
Prefix list error [8]
Server preference error [0]
```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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 dhcpv6-snooping guard-policy vlan

```
show dhcpv6-snooping guard-policy [vlan <VLAN-ID>] [vsx-peer]
```

## Description

Shows the DHCPv6 snooping guard policy configuration and statistics for the specified VLAN.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <VLAN-ID> | Specifies the VLAN ID for which the DHCPv6 guard counter information is displayed.                                                                                                                                               |
| 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 the DHCPv6 snooping guard policy configuration and statistics for VLAN 100:

```
switch# show dhcpv6-snooping guard-policy vlan 2
DHCPv6 Guard Policy Applied : poll
DHCPv6 Guard Policy Counters
=====

DHCPv6 Packets Received : 20
DHCPv6 Packets Forwarded : 5
DHCPv6 Packets Dropped : 15 [Total]
Access list error [0]
Prefix list error [8]
Server preference error [7]
```

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.11   | Command introduced for the 8325 and 10000 Switch Series. |
| 10.10   | Command introduced.                                      |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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 dhcpv6-snooping statistics

```
show dhcpv6-snooping statistics [vsx-peer]
```

### Description

Shows the DHCPv6 snooping statistics.

| 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

Showing the DHCPv6 snooping statistics:

```
switch(config) # show dhcpv6-snooping statistics
```

| Packet-Type | Action  | Reason                        | Count |
|-------------|---------|-------------------------------|-------|
| server      | forward | from trusted port             | 12    |
| client      | forward | to trusted port               | 20    |
| server      | drop    | received on untrusted port    | 5     |
| server      | drop    | unauthorized server           | 4     |
| client      | drop    | destination on untrusted port | 2     |
| client      | drop    | bad DHCP release request      | 5     |
| server      | drop    | relay reply on untrusted port | 2     |
| client      | drop    | failed on max-binding limit   | 5     |

## Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.11            | Command introduced for the 8325 and 10000 Switch Series. |
| 10.09.1000       | Command introduced for the 8360 Switch Series.           |
| 10.09            | Command introduced for the 6000 and 6100 Switch Series.  |
| 10.07 or earlier |                                                          |

## Command Information

| Platforms                                       | Command context             | Authority                                                                                                                                                              |
|-------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>10000 | 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. |

## Troubleshooting

### DHCP client not receiving IP

1. Trusted port configuration: check if the server reachable port is configured as trusted.
2. Validate Packet drop counters: use **show dhcpv4-snooping statistics** and **show dhcpv6-snooping statistics** commands to view the packet drop counters. This helps to identify a possible

reason for the termination of DHCP packet exchange between client and server. A few possible reasons are listed below:

- Maximum binding limit reached
    - System-wide limit—The maximum binding limit is shared between DHCPv4-Snooping, DHCPv6-Snooping, ND-Snooping, and IP-Source-Bindings. On reaching the limit, DHCP client requests get dropped. To check the limit, use the **show capacities ip-bindings** command.
    - Per port limit: This is a per port configurable value for a protocol. On reaching the limit, the subsequent client requests are dropped.
  - Conflicts with IP-Source-Bindings—User-configured IP-Source-Bindings are given priority over dynamically learned bindings. Validate if the dynamic client is conflicting with any of the existing IP-Source-Binding.
  - Authorized server check failures—Authorized server configuration is global. When one or more authorized servers are set up, all server replies should come from one of the authorized server IP addresses.
  - CoPP packet drops—If the rate of the DHCP packets entering is higher than the configured value, excessive packets are dropped by CoPP. Check CoPP statistics for the DHCP class and configure the value accordingly. Higher CoPP values could cause other protocols to misbehave depending on the platform.
3. Server configuration and reachability: validate the following to ensure that the DHCP Server is reachable and configured correctly.
    - a. Check that the server is reachable over one of the trusted ports.
    - b. Check the server logs to understand the DHCP exchange status between client and server.
    - c. Check if DHCP Server pools are exhausted.
  4. Option-82 configuration issues (Specific to DHCP Snooping IPv4)
    - a. This configuration usually arises when DHCP Snooping and Relay are configured on the same VLAN. Option 82 at DHCP Snooping IPv4 should be disabled when configured for Inter-VRF DHCP-Relay. Use **no dhcpv4-snooping option 82** command to disable the functionality.
    - b. Option 82 is enabled by default, and the drop policy is set. If client packets are received with option 82, then they are dropped with this configuration.
  5. Server and client are connected to same the VLAN
    - a. Check if the server is reachable on the same VLAN as the client.
    - b. If the server is on a different L3 network, configure DHCP-Relay to forward the packets between the client and server.
  6. Authorized server configurations—When configured, the server assigning IP address should be one of the IP addresses from the authorized server list.

In DHCP snooping IPv6, if DHCP Relay is between a test device and a server, the authorised server configuration should include a link to the local IP address of the relay interface. This is because, while forwarding the server's response to the client, it will stamp a link to the local IP address as the source IP of the packet.

## IP-Binding mismatch in VSX topologies

1. Both primary and secondary VSX peers should have the same clock value. If not, there is a possibility of inconsistent ip-bindings that could result in ip-binding sync in a loop. There is no straight-forward way to check the inconsistencies but by looking at the number of bindings and

debug log analysis

2. Ensure the ISL state is up and operational.

### **DHCP client IP traffic is dropped at data path**

1. This can happen when IP-Source-Lockdown is used along with DHCP snooping. Ensure IP-Bindings are learned for clients that are experiencing traffic failure issues
2. Check the hardware programming state of the IP-Binding entry by IP-Source-Lockdown. Use **show ipv4 source-lockdown bindings** or **show ipv6 source-lockdown bindings** commands.

A number of deployments provide access to WAN or public network only through a proxy server for the network security. This section provides information about the various methods of HTTP proxy configuration on the switch. The HTTP proxy configured is used to connect to HPE Aruba Networking Central as per the zero-touch provisioning requirement.

HTTP proxy location can be configured using the CLI or 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 VRF 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 VRF 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.
  - A port number may need to be specified at the end of the IP address for FQDN to connect via HTTP proxy. For example, if 8088 is the TCP port number, use the command **http-proxy 192.168.248.248:8088**.
- 

## DHCP options commands

### http-proxy

```
http-proxy {<FQDN | IPV4-ADDR> | IPV6-ADDR[:PORT]} [vrf <VRF-NAME>]
no http-proxy [<FQDN | IPV4-ADDR>] [vrf <VRF-NAME>]
```

#### Description

Specifies HTTP proxy location and VRF.

When HTTP proxy location and VRF are configured on the switch, it overrides any existing HTTP proxy location and VRF as this has the highest priority over the values obtained from other sources.

Following locations can be used for the HTTP proxy location:

- A fully qualified domain name (FQDN).
- An IPv4 address with colon separated port number
- An IPv6 address with colon separated port number



When configuring an IPv6 address with a port number, the address must be specified inside square brackets. An example - [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:8080.

If the command is entered without the VRF parameter, then the VRF used will be 'default' VRF. The **no** form of this command removes a specified HTTP proxy location.

| Parameter   | Description                                     |
|-------------|-------------------------------------------------|
| <FQDN>      | Specifies FQDN for HTTP proxy location.         |
| <IPV4-ADDR> | Specifies IPV4 address for HTTP proxy location. |
| <IPV6-ADDR> | Specifies IPV6 address for HTTP proxy location. |
| <VRF-NAME>  | Specifies VRF for HTTP proxy.                   |



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

## Examples

Specifying a FQDN for HTTP proxy location and **MGMT** VRF with an IPv6 address:

```
switch(config)# http-proxy http-proxy.example.com vrf mgmt
switch(config)# http-proxy [2000::100]:8080 vrf mgmt
```

Specifying a FQDN for HTTP proxy location and **MGMT** VRF with an IPv4 address:

```
switch(config)# http-proxy http-proxy.example.com vrf mgmt
switch(config)# http-proxy 192.168.1.3:8080 vrf mgmt
```

Removing HTTP proxy location

```
switch(config)# no http-proxy
```

## Command History

| Release          | Modification                             |
|------------------|------------------------------------------|
| 10.13.1000       | Command updated to reflect OTP scenario. |
| 10.07 or earlier | --                                       |

## Command Information

| <b>Platforms</b> | <b>Command context</b> | <b>Authority</b>                                                                   |
|------------------|------------------------|------------------------------------------------------------------------------------|
| All platforms    | <code>config</code>    | Administrators or local user group members with execution rights for this command. |



---

ND snooping is not supported on the 8320 Switch Series.

---



---

ND snooping is supported over VxLAN with IPv4 or IPv6 underlay for the following platforms: 6300, 6400, 8100, and 8360.

---

## Overview (applies to the 8325/8325H/8325P, 9300/9300S, and 10000 Switch Series)

ND (Neighbor Discovery) snooping is used in Layer 2 switching networks and prevents ND attacks. RA (Router Advertisement) guard is a sub-feature of ND snooping and manages RA and RR (Router Redirect) packets on configured VLANs. RA and RR packets received on trusted ports are allowed. RA and RR packets are dropped in the following cases:

- 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 a packet is received on an untrusted port of a RA guard enabled VLAN.



---

On the 8325, 9300/9300S, and 10000 Switch Series, only the RA guard portion of ND snooping is supported. The following are not supported: RA guard policy, ND guard, RA drop.

---

## Overview (applies to the 6300, 6400, 8100, and 8360 Switch Series)

ND snooping is used in Layer 2 switching networks and 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 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 DHCPv6 snooping table and DHCPv6 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.

When RA guard policy is enabled (with `ipv6 nd-snooping ra-guard policy`), RA packets received on trusted ports are validated against a set of parameters configured on the policy and assigned to a port or VLAN.



---

For more information on RA guard including RA guard policies, see this related video on the HPE Aruba Networking [AirHeads Broadcasting Channel](#).

---

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.



---

Statically-configured IP binding information supersedes any information collected dynamically by ND snooping for the same client.

---

## Configuring ND snooping over VxLAN with IPv4 and IPv6 underlay

### Procedure

1. Configure VXLAN overlay setup to establish the VxLAN tunnel. For more information, see *AOS-CX VXLAN EVPN Guide*.
2. Validate whether the tunnel is established between the VTEPS (either static or EVPN) with the command `show interface vxlan vteps`.



---

The status of the tunnel should be operational in order to forward the packets.

---

3. Configure or enable Nd-snooping at the global and VLAN contexts with the commands `Nd-snooping enable` and `nd-snooping`, respectively.
4. Configure the server connected port as trusted with the command `Nd-snooping trust`.



---

If the server is connected through the VXLAN tunnel, then this step can be ignored. This is because VXLAN is trusted by default for ND snooping over VXLAN.

---

5. Validate the Nd-snooping configuration with the command `show Nd-snooping`.

## ND snooping commands

### clear nd-snooping binding

```
clear nd-snooping bindings {all | ipv6 <IPV6-ADDR> vlan <VLAN-ID> |
 port <PORT-NUM> | vlan <VLAN-ID>}
```

## Description

Clears ND snooping binding entries.

## Command context

| Parameter                     | Description                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------|
| all                           | Specifies that all ND binding information is to be cleared.                                 |
| ip <IPV6-ADDR> vlan <VLAN-ID> | Specifies the IPv6 address and VLAN for which all ND binding information is to be cleared.  |
| port <PORT-NUM>               | Specifies the port (interface) for which all ND binding information is to be cleared.       |
| vlan <VLAN-ID>                | Specifies the VLAN for which all ND binding information is to be cleared. Range: 1 to 4094. |

## Examples

Clearing all ND binding information for 5000::1 vlan 1:

```
switch(config)# clear nd-snooping bindings ipv6 5000::1 vlan 1
```

Clearing all ND binding information for port 1/1/10:

```
switch(config)# clear nd-snooping bindings port 1/1/10
```

Clearing all ND binding information for VLAN 10:

```
switch(config)# clear nd-snooping bindings vlan 10
```

Clearing all ND binding information:

```
switch(config)# clear nd-snooping bindings all
```

## Command History

| Release          | Modification                |
|------------------|-----------------------------|
| 10.10            | Added support for the 8360. |
| 10.07 or earlier | --                          |

## Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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. |

## clear nd-snooping ra-guard-policy statistics

```
clear nd-snooping ra-guard-policy statistics [vlan <VLAN-ID>][interface <IFNAME>]
```

### Description

Clear all RA Guard policy statistics from the specified interface or VLAN.

### Command context

| Parameter          | Description                                                      |
|--------------------|------------------------------------------------------------------|
| vlan <VLAN-ID>     | Clear all RA Guard policy information on the specified VLAN      |
| interface <IFNAME> | Clear all RA Guard policy information on the specified interface |

### Examples

Clear all RA Guard policy statistics for VLAN 10:

```
switch# clear nd-snooping ra-guard-policy statistics vlan 10
```

Clear all RA Guard policy statistics for interface 1/1/10

```
switch# clear nd-snooping ra-guard-policy statistics interface 1/1/10
```

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

### Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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. |

## clear nd-snooping statistics

```
clear nd-snooping statistics
```

### Description

Clears all ND snooping statistics.

## Examples

Clear all ND snooping statistics:

```
switch# clear nd-snooping statistics
```

## Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms                                                        | Command context             | Authority                                                                                                                                                              |
|------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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. |

## diag-dump nd-snooping basic

```
diag-dump nd-snooping basic
```

### Description

This command displays information about the ND-Snooping configuration and runtime context.

### Examples

The following example displays sample output for this command.

```
switch# diag-dump nd-snooping basic
=====
[Start] Feature nd-snooping Time : Tue Mar 29 02:53:59 2022
=====
[Start] Daemon ipsavd

Feature nd-snooping:

 Global ND snoop = ENABLED
 ND snoop MAC check = ENABLED

VLAN ND-Snooping ND-Guard RA-Guard RA-Guard-Log RA-Drop
---- -
1 ENABLED ENABLED ENABLED DISABLED DISABLED
```

```

Statistics
Counter Name Count

ra_recd_on_trusted_port 0
ra_drop_on_trusted_port 0
ra_recd_on_untrusted_port 0
rr_recd_on_trusted_port 0
rr_recd_on_untrusted_port 0
ns_recd_on_trusted_port 0
ns_recd_on_untrusted_port 0
ns_failed_mac_check 0
ns_failed_prefix_check 0
ns_failed_binding_limit 0
ns_failed_nd_snoop_validation 0
na_recd_on_trusted_port 0
na_recd_on_untrusted_port 0
na_failed_mac_check 0
na_failed_prefix_check 0
na_failed_binding_limit 0
na_failed_nd_snoop_validation 0
nd_invalid_packet_received 0
total_nd_packets_dropped 0
Pkts_to_refilter_interface 0
Pkts_on_vxlan_tunnels_received 0
Pkts_on_vxlan_tunnels_sent 0
Pkts_on_vxlan_tunnels_dropped 0

```

```

Feature ipsavvxlan:
Source IP = 2.2.2.2
VXLAN Socket = 29

```

```

Feature remote-ipbinding:

```

```

Feature ipbinding:
Storage = DISABLED

```

```

Total count of lockdown entries = 0
Total count of IPv6 lockdown entries = 0

```

```

Displaying lease entries with (vid,mac) as key.

```

```

Total number of entries: 0

```

| Leased IPv6 addr  | MAC               | Vid | Switch port | Lease time | Server IPv6 |
|-------------------|-------------------|-----|-------------|------------|-------------|
| address IS_STATIC | Lockdown          |     |             |            |             |
| 2000::2           | 11:22:32:44:55:66 | 1   | 1/1/1       | 195        | 0           |
| 0                 | Yes               |     |             |            |             |
| 2000::1           | 11:22:33:44:55:66 | 1   | 1/1/1       | 211        | 0           |
| 0                 | Yes               |     |             |            |             |

```

Displaying lease entries with (vid,ip) as key.

```

```

Total number of entries: 0

```

| Leased IPv6 addr  | MAC               | Vid | Switch port | Lease time | Server IPv6 |
|-------------------|-------------------|-----|-------------|------------|-------------|
| address IS_STATIC | Lockdown          |     |             |            |             |
| 2000::2           | 11:22:32:44:55:66 | 1   | 1/1/1       | 195        | 0           |
| 0                 | Yes               |     |             |            |             |
| 2000::1           | 11:22:33:44:55:66 | 1   | 1/1/1       | 211        | 0           |
| 0                 | Yes               |     |             |            |             |

Feature ipsavmac:

Feature ipsavvlan:

| Vlan ID | State  | VNI | Port map |
|---------|--------|-----|----------|
| 1       | ENABLE | -   | 1 420    |
| 7       | ENABLE | 100 | 3,4      |
| 100     | ENABLE | -   | 1        |

Feature ipsavport:

ISL Port Name =  
Index = 0  
Egress blocked port map = None  
IPv6 Lockdown vidmap =

| Port Name | Index | Socket | Trusted | Max Binding | Lockdown | VID map |
|-----------|-------|--------|---------|-------------|----------|---------|
| 1/1/10    | 10    | 26     | No      | 16384       | No       | 1       |
| 1/1/8     | 8     | 30     | No      | 16384       | No       | 1       |
| 1/1/26    | 26    | 22     | No      | 16384       | No       | 1       |
| 1/1/27    | 27    | 23     | No      | 16384       | No       | 1       |
| 1/1/14    | 14    | 19     | No      | 16384       | No       | 1       |
| 1/1/25    | 25    | 32     | No      | 16384       | No       | 1       |
| 1/1/17    | 17    | 43     | No      | 16384       | No       | 1       |
| 1/1/18    | 18    | 42     | No      | 16384       | No       | 1       |
| 1/1/28    | 28    | 16     | No      | 16384       | No       | 1       |
| 1/1/23    | 23    | 28     | No      | 16384       | No       | 1       |
| 1/1/24    | 24    | 18     | No      | 16384       | No       | 1       |
| 1/1/11    | 11    | 34     | No      | 16384       | No       | 1       |
| 1/1/13    | 13    | 25     | No      | 16384       | No       | 1       |
| 1/1/16    | 16    | 36     | No      | 16384       | No       | 1       |
| 1/1/22    | 22    | 35     | No      | 16384       | No       | 1       |
| 1/1/5     | 5     | 40     | No      | 16384       | No       | 1       |
| 1/1/9     | 9     | 20     | No      | 16384       | No       | 1       |
| 1/1/12    | 12    | 38     | No      | 16384       | No       | 1       |
| 1/1/15    | 15    | 39     | No      | 16384       | No       | 1       |
| 1/1/20    | 20    | 29     | No      | 16384       | No       | 1       |
| 1/1/4     | 4     | 41     | No      | 16384       | No       | 1       |
| 1/1/7     | 7     | 37     | No      | 16384       | No       | 1       |
| 1/1/21    | 21    | 33     | No      | 16384       | No       | 1       |
| 1/1/1     | 1     | 17     | No      | 16384       | No       | 1       |
| 1/1/6     | 6     | 27     | No      | 16384       | No       | 1       |
| 1/1/19    | 19    | 24     | No      | 16384       | No       | 1       |
| 1/1/2     | 2     | 31     | Yes     | 16384       | No       | 1       |
| 1/1/3     | 3     | 21     | No      | 16384       | No       | 1       |

Feature ipsav:

\* nd-snooping \*  
VID map = 1  
Global Config = ENABLED  
State = ENABLED

-----  
[End] Daemon ipsavd  
-----

```

=====
[End] Feature nd-snooping
=====
Diagnostic-dump captured for feature nd-snooping

```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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. |

## 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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms                                                        | Command context | Authority                                                                          |
|------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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.

### 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)#
```

### Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

### Command Information

| Platforms             | Command context | Authority                                                                          |
|-----------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H | config-vlan     | Administrators or local user group members with execution rights for this command. |

| Platforms                               | Command context | Authority |
|-----------------------------------------|-----------------|-----------|
| 8325P<br>8360<br>9300<br>9300S<br>10000 |                 |           |

## 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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

### Command Information

| Platforms                                                        | Command context | Authority                                                                          |
|------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config          | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter   | Description                 |
|-------------|-----------------------------|
| <IPV6-ADDR> | Specifies the IPv6 address. |

### Examples

Configuring ND snooping prefix-list on VLAN 1:

```
switch(config)# vlan 1
switch(config-vlan-1)# nd-snooping prefix-list 2001::1/64
switch(config-vlan-1)# exit
switch(config)#
```

Remove configuration of ND snooping prefix-list on VLAN 100:

```
switch(config)# vlan 1
switch(config-vlan-1)# no nd-snooping prefix-list 2001::1/64
switch(config-vlan-1)# exit
switch(config)#
```

### Command History

| Release          | Modification                |
|------------------|-----------------------------|
| 10.10            | Added support for the 8360. |
| 10.07 or earlier | --                          |

### Command Information

| Platforms    | Command context       | Authority                                                                                                                                                              |
|--------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | config-vlan-<VLAN-ID> | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## 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.

| Parameter                         | Description                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;MAX-BINDINGS&gt;</code> | Specifies the maximum number of ND bindings. You can use the <b>show capacities</b> command to see the maximum available for your switch model. |

## Examples

Set the ND max bindings to 768 on interface 2/2/1:

```
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

| Release          | Modification                |
|------------------|-----------------------------|
| 10.10            | Added support for the 8360. |
| 10.07 or earlier | --                          |

## Command Information

| Platforms    | Command context | Authority                                                                          |
|--------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-if       | Administrators or local user group members with execution rights for this command. |

## 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 History

| Release          | Modification                |
|------------------|-----------------------------|
| 10.10            | Added support for the 8360. |
| 10.07 or earlier | --                          |

## Command Information

| Platforms    | Command context | Authority                                                                          |
|--------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-vlan     | Administrators or local user group members with execution rights for this command. |

## 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:

```
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:

```
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:

```
switch(config)# vlan 100
switch(config-vlan-100)# no nd-snooping ra-guard
switch(config-vlan-100)# exit
switch(config)#
```

## Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms                                                        | Command context       | Authority                                                                          |
|------------------------------------------------------------------|-----------------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-vlan-<VLAN-ID> | Administrators or local user group members with execution rights for this command. |

## 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)#
```

## Command History

| Release          | Modification                |
|------------------|-----------------------------|
| 10.10            | Added support for the 8360. |
| 10.07 or earlier | --                          |

## Command Information

| Platforms    | Command context       | Authority                                                                          |
|--------------|-----------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-vlan-<VLAN-ID> | Administrators or local user group members with execution rights for this command. |

## nd-snooping trust

```
nd-snooping trust
no nd-snooping trust
```

## Description

Enables ND snooping trust on the selected interface (port) allowing RA and RR packets to be received. RA and RR packets received on untrusted ports are discarded, all ports are untrusted by default.

The no form of the command disables ND snooping trust on the selected port.

## Examples

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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms                                                        | Command context | Authority                                                                          |
|------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | config-if       | Administrators or local user group members with execution rights for this command. |

## 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.

| Parameter      | Description                                                                         |
|----------------|-------------------------------------------------------------------------------------|
| vlan <VLAN-ID> | Specifies the VLAN for which the ND configuration is to be shown. Range: 1 to 4094. |

| 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

(Applies to the HPE Aruba Networking 5420, 6200, 6300, 6400, 8100, and 8360 Switch series.) Showing all ND snooping configuration:

```
switch(config)# show nd-snooping

ND Snooping Information
=====

ND Snooping : Enabled
ND Snooping Enabled VLANs : 10
Trusted Port Bindings Enabled VLANs : 10
ND Guard Enabled VLANs : 10
RA Guard Enabled VLANs : 10
RA Drop Enabled VLANs :
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
```

(Applies to the HPE Aruba Networking 5420, 6200, 6300, 6400, 8100, 8360 Switch series.) Showing ND snooping configuration for VLAN 2:

```
switch(config)# show nd-snooping vlan 2

ND Snooping Information
=====

ND Snooping : Enabled
MAC Address Check : Disabled
Trusted Port Bindings : Enabled
ND Guard : Enabled
RA Guard : Disabled
RA Drop : Disabled

PORT TRUST MAX-BINDINGS CURRENT-BINDINGS
----- -
1/1/1 Yes
1/1/2 Yes
1/1/3 No 100 10
```

(Applies to the HPE Aruba Networking 8325, 9300/9300S, 10000 Switch series.) Showing all ND snooping configuration:

```

switch(config)# show nd-snooping

ND Snooping Information
=====

ND Snooping : Enabled
ND Snooping Enabled VLANs : 10
RA Guard Enabled VLANs : 10
MAC Address Check : Disabled

PORT TRUST
----- -----
1/1/1 Yes
1/1/2 Yes
1/1/3 No
1/1/4 No
1/1/5 No

```

(Applies to the HPE Aruba Networking 8325, 9300/9300S, 10000 Switch series.) Showing ND snooping configuration for VLAN 2:

```

switch(config)# show nd-snooping vlan 2

ND Snooping Information
=====

ND Snooping : Enabled
MAC Address Check : Disabled
RA Guard : Disabled

PORT TRUST
----- -----
1/1/1 Yes
1/1/2 Yes
1/1/3 No

```

## Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms                                                        | Command context             | Authority                                                                                                                                                              |
|------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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 nd-snooping binding

```
show nd-snooping bindings [vsx-peer]
```

### Description

Shows the ND snooping binding 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

Showing the ND snooping binding configuration:

```
switch# show nd-snooping binding

 PORT IPV6-ADDRESS MAC-ADDRESS VLAN TIME-
LEFT STATE

1/1/1 2001::1 00:00:0A:01:02:03 1 600
Valid
1/1/2 fe80::250:56ff:fe9a:143c 00:00:0B:01:02:03 2 -
Tentative
1/1/3 2001:1111:2222:3333:4444:5555:6666:7777 00:00:0C:01:02:03 4094 -
Testing
```

### Command History

| Release          | Modification                |
|------------------|-----------------------------|
| 10.10            | Added support for the 8360. |
| 10.07 or earlier | --                          |

### Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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 nd-snooping prefix-list

```
show nd-snooping prefix-list [vsx-peer]
```

### Description

Shows the ND snooping prefix list information.

| 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

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

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms                                                        | Command context             | Authority                                                                                                                                                              |
|------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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 nd-snooping statistics

```
show nd-snooping statistics [vsx-peer]
```

### Description

Shows the global ND snooping statistics.

| 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

(Applies to the HPE Aruba Networking 5420, 6200, 6300, 6400, 8100, 8360.) Showing global ND snooping statistics:

```
switch(config)# show nd-snooping statistics
```

| PACKET-TYPE | ACTION  | REASON                                          | COUNT |
|-------------|---------|-------------------------------------------------|-------|
| RA          | forward | RA packets received on trusted port             | 20    |
| RA          | drop    | RA packets received on untrusted port           | 45    |
| NS          | forward | NS packets received on trusted port             | 52    |
| NS          | forward | NS packets received on untrusted port           | 95    |
| NS          | drop    | NS packets failed MAC check                     | 14    |
| NS          | drop    | NS packets failed Prefix check                  | 12    |
| NS          | drop    | NS packets failed on max-binding limit          | 0     |
| NS          | drop    | NS packets failed ND snooping validation checks | 20    |
| NA          | forward | NA packets received on trusted port             | 17    |
| NA          | forward | NA packets received on untrusted port           | 30    |
| NA          | drop    | NA packets failed Prefix check                  | 15    |
| NA          | drop    | NA packets failed on max-binding limit          | 2     |
| NA          | drop    | NA packets failed ND snooping validation checks | 5     |

(Applies to the HPE Aruba Networking 8325, 9300/9300S, 10000 Switch series.) Showing global ND snooping statistics:

```
switch(config)# show nd-snooping statistics
```

| PACKET-TYPE | ACTION  | REASON                                | COUNT |
|-------------|---------|---------------------------------------|-------|
| RA          | forward | RA packets received on trusted port   | 20    |
| RA          | drop    | RA packets received on untrusted port | 45    |
| RR          | forward | RR packets received on trusted port   | 20    |
| RR          | drop    | RR packets received on untrusted port | 45    |

## Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.10            | Added support for the 8360.                              |
| 10.09            | Added support for the 8325. Added support for the 10000. |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms                                                        | Command context             | Authority                                                                                                                                                              |
|------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8325<br>8325H<br>8325P<br>8360<br>9300<br>9300S<br>10000 | 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. |

# RA guard policy commands

## hop limit

```
hop limit [minimum | maximum] <HOP-LIMIT>
no hop limit [minimum | maximum] <HOP-LIMIT>
```

### Description

Enables verification of the advertised hop count limit if the RA guard policy is applied on a VLAN or interface. RA packets with the hop limit within the specified minimum and maximum values are processed. If none of the values are specified for hop limit, the default range is 1-255. If hop limit is not enabled, packets are not validated for hop limit.

The **no** form of the command disables the hop limit on the specified RA guard policy.



---

ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

---

| Parameter   | Description                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <HOP-LIMIT> | Specifies the hop-limit value. Range: 1-255.                                                                                                    |
| minimum     | Specifies the minimum value for the hop-limit range. Default: 1, Range 1-255.<br>The range is minimum-255 if only a minimum value is specified. |
| maximum     | Specifies the maximum value for the hop-limit range. Default: 255, Range 1-255.<br>The range is 1-maximum if only a maximum value is specified. |

### Examples

Enabling the hop limit on the RA guard policy and adding minimum and maximum values for hop limit on the policy:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-raguard-policy)# hop-limit enable
switch(config-raguard-policy)# hop-limit maximum 150
switch(config-raguard-policy)# hop-limit minimum 50
```

Disabling the hop limit on the RA guard policy:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-raguard-policy)# no hop-limit enable
```

Removing minimum and maximum values for the hop limit on the RA guard policy:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-raguard-policy)# no hop-limit maximum 150
switch(config-raguard-policy)# no hop-limit minimum 50
switch(config-raguard-policy)# no hop-limit maximum
switch(config-raguard-policy)# no hop-limit minimum
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context       | Authority                                                                          |
|--------------|-----------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-raguard-policy | Administrators or local user group members with execution rights for this command. |

## ipv6 nd-snooping ra-guard policy

```
ipv6 nd-snooping ra-guard policy <POLICY-NAME>
no ipv6 nd-snooping ra-guard policy <POLICY-NAME>
```

### Description

Creates the Router Advertisement (RA) guard policy with the given name and enters the RA guard policy configuration context.

The **no** form of the command removes the specified RA guard policy from the switch.



ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

| Parameter     | Description                                                    |
|---------------|----------------------------------------------------------------|
| <POLICY-NAME> | Specifies the name of the RA guard policy. Maximum length: 64. |

### Examples

Creating the RA guard policy globally with a specified name:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-raguard-policy)#
```

Deleting the specified RA guard policy:

```
switch(config)# no ipv6 nd-snooping ra-guard policy <POLICY-NAME>
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context | Authority                                                                          |
|--------------|-----------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config          | Administrators or local user group members with execution rights for this command. |

## managed-config-flag

```
managed-config-flag [on | off]
no managed-config-flag [on | off]
```

### Description

Enables the verification of the advertised manage configuration flag. Verifies that the advertised managed address configuration flag is On or Off based on the configured value.

The **no** form of the command disables the manage configuration flag verification.



ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

| Parameter | Description                                                             |
|-----------|-------------------------------------------------------------------------|
| on        | Verifies that the advertised managed address configuration flag is On.  |
| off       | Verifies that the advertised managed address configuration flag is Off. |

### Examples

Enabling managed configuration flag verification:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-ra-guard-policy)# managed-config-flag off
switch(config-ra-guard-policy)# managed-config-flag on
```

Disabling managed configuration flag verification:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-ra-guard-policy)# no managed-config-flag
switch(config-ra-guard-policy)# no managed-config-flag off
switch(config-ra-guard-policy)# no managed-config-flag on
```

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

### Command Information

| Platforms    | Command context       | Authority                                                                          |
|--------------|-----------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-raguard-policy | Administrators or local user group members with execution rights for this command. |

## match access-list

```
match access-list <ACL-NAME>
no match access-list <ACL-NAME>
```

### Description

Configures the access list to an RA guard policy. The access list has to be created with the desired match criteria before adding it into RA guard policy. Advertised packets are verified for the match criteria when an RA guard policy with matched access list is enabled on a trusted port or VLANs.

The **no** form of the command removes the access list from the RA guard policy.



ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

| Parameter  | Description                                          |
|------------|------------------------------------------------------|
| <ACL-NAME> | Specifies the name of the access list to be matched. |

### Examples

Adding an access list named Example\_ACL to the RA guard policy POL1:

```
switch(config)# ipv6 nd-snooping ra-guard policy POL1
switch(config-raguard-policy)# match access-list Example_ACL
```

Deleting the access list named Example\_ACL from the RA guard policy POL1:

```
switch(config)# ipv6 nd-snooping ra-guard policy POL1
switch(config-raguard-policy)# no match access-list Example_ACL
```

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

### Command Information

| Platforms    | Command context       | Authority                                                                          |
|--------------|-----------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-raguard-policy | Administrators or local user group members with execution rights for this command. |

## match prefix-list

```
match prefix-list <PREFIX-LIST-NAME>
no match prefix-list <PREFIX-LIST-NAME>
```

### Description

Configures a prefix-list for the RA guard policy. Advertised prefixes in RA packets are compared against the configured prefix-list and if there is no match, the RA packets are dropped. If the RA prefix list is not configured, this check is not performed.

The **no** form of the command removes the prefix list from the RA guard policy.



ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

| Parameter          | Description                                          |
|--------------------|------------------------------------------------------|
| <PREFIX-LIST-NAME> | Specifies the name of the prefix list to be matched. |

### Examples

Adding a prefix list named PREFIX\_LIST\_EXAMPLE to the POLICY1 RA guard policy:

```
switch(config)# ipv6 nd-snooping ra-guard policy POLICY1
switch(config-raguard-policy)# match prefix-list PREFIX_LIST_EXAMPLE
```

Deleting the prefix list named PREFIX\_LIST\_EXAMPLE from the POLICY1 RA guard policy:

```
switch(config)# ipv6 nd-snooping ra-guard policy POLICY1
switch(config-raguard-policy)# no match pefix-list PREFIX_LIST_EXAMPLE
```

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

### Command Information

| Platforms    | Command context       | Authority                                                                          |
|--------------|-----------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-raguard-policy | Administrators or local user group members with execution rights for this command. |

## nd-snooping ra-guard attach-policy

```
nd-snooping ra-guard attach-policy <POLICY-NAME>
no nd-snooping ra-guard attach-policy <POLICY-NAME>
```

### Description

Applies the created RA guard policy to a specific L2 port or VLAN.

The **no** form of the command detaches the specified RA guard policy from the L2 port or VLAN.

| Parameter                        | Description                                |
|----------------------------------|--------------------------------------------|
| <code>&lt;POLICY-NAME&gt;</code> | Specifies the name of the RA guard policy. |

## Usage

In the interface configuration (config-if) context:

- RA guard must be enabled on member VLANs of the port for which RA packets need to be inspected using the policy.

In the interface configuration (config-if) and VLAN configuration (config-vlan) contexts:

- RA packets received on untrusted ports are dropped without any inspection.
- RA packets received on trusted ports are validated against the policy.
- The applied policy takes effect only if ND snooping is enabled globally and both ND snooping and RA guard are enabled under the VLAN context.

Policy precedence between VLAN and port:

- If the policy is attached to both VLAN and port, the port policy takes precedence over the VLAN policy.
- Only one policy can be attached per VLAN or port.
- If the port belongs to a different VLAN (for example, in the case of a trunk port) the tagged VLAN takes priority. If the packets are untagged, the native VLAN policy takes precedence.

## Examples

Attaching the RA guard policy to an L2 port:

```
switch(config)# interface 1/1/10
switch(config-if)# nd-snooping ra-guard attach-policy POLICY_NAME
```

Attempting to attach the RA guard policy to a port where routing is enabled, the policy is not configured, or it is an untrusted port:

(When prompted, enter "Y" to create the policy and attach it to the interface. )

```
switch(config)# interface 1/1/10
switch(config-if)# nd-snooping ra-guard attach-policy POLICY_NAME
RA Guard policy can't be attached to an interface with routing enabled.

switch(config-if)# no routing
switch(config-if)# nd-snooping trust
switch(config-if)# nd-snooping ra-guard attach-policy POLICY_NAME
switch(config-if)#6300(config-if)# nd-snooping ra-guard attach-policy POLICY_NOT_
CREATED
RA guard policy does not exist.
Do you want to create (y/n)?

switch(config)# interface 1/1/10
```

```
switch(config-if)# nd-snooping ra-guard attach-policy AA
RA Guard policy is ineffective, as 1/1/10 is configured as untrusted port.
```

Attaching the RA guard policy to a VLAN:

```
switch(config)# vlan 10
switch(config-vlan-10)# nd-snooping ra-guard attach-policy POLICY_NAME
```

Detaching the RA guard policy:

```
switch(config)# interface 1/1/10
switch(config-if)# no nd-snooping ra-guard attach-policy POLICY_NAME
```

Attempting to detach a RA guard policy which is not applied on the port or VLAN:

```
switch(config)# interface 1/1/10
switch(config-if)# no nd-snooping ra-guard attach-policy POLICY_NAME
RA Guard Policy POLICY_NAME is not applied on this port.
```

Attempting to detach a non-existent RA guard policy:

```
switch(config-if)# no nd-snooping ra-guard attach-policy POLICY_NOT_CREATED
Could not find the policy POLICY_NOT_CREATED.
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms | Command context       | Authority                                                                          |
|-----------|-----------------------|------------------------------------------------------------------------------------|
| 8100      | config-if             | Administrators or local user group members with execution rights for this command. |
| 8360      | config-vlan-<VLAN-ID> |                                                                                    |

## other-config-flag

```
other-config-flag [on | off]
no other-config-flag [on | off]
```

### Description

Enables the verification of the advertised other configuration flag. Verifies that the advertised Other Stateful Configuration flag is On or Off based on the configured value.

The **no** form of the command disables other configuration flag verification.



---

ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

---

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| on        | Verifies that the advertised Other Stateful Configuration flag is On.  |
| off       | Verifies that the advertised Other Stateful Configuration flag is Off. |

## Examples

Enabling other configuration flag verification:

```
switch(config) # ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-raguard-policy) # other-config-flag off
switch(config-raguard-policy) # other-config-flag on
```

Disabling other configuration flag verification:

```
switch(config) # ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-raguard-policy) # no other-config-flag
switch(config-raguard-policy) # no other-config-flag off
switch(config-raguard-policy) # no other-config-flag on
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context       | Authority                                                                          |
|--------------|-----------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-raguard-policy | Administrators or local user group members with execution rights for this command. |

## router-preference

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

### Description

Enables the router preference verification on the RA guard policy for advertised packets and processes the packets only if the router preference is lower than the configured value. If the router preference is not configured, this validation is bypassed.

The **no** form of this command disables router preference verification on the RA guard policy.

| Parameter | Description                                 |
|-----------|---------------------------------------------|
| high      | Sets the maximum router preference to high. |

| Parameter | Description                                   |
|-----------|-----------------------------------------------|
| medium    | Sets the maximum router preference to medium. |
| low       | Sets the maximum router preference to low.    |

## Examples

Enabling router preference verification with the maximum router preference set to high:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-ra-guard-policy)# router-preference high
```

Disabling router preference verification:

```
switch(config)# ipv6 nd-snooping ra-guard policy <POLICY-NAME>
switch(config-ra-guard-policy)# no router-preference
```

## Command History

| Release          | Modification        |
|------------------|---------------------|
| 10.10 or earlier | Command introduced. |

## Command Information

| Platforms    | Command context        | Authority                                                                          |
|--------------|------------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-ra-guard-policy | Administrators or local user group members with execution rights for this command. |

## show nd-snooping ra-guard interface

```
show nd-snooping ra-guard interface <INTERFACE-ID>
```

### Description

Shows RA guard counters for the specified interface. Counters are cleared once the RA guard policy is detached from the interface.

| Parameter      | Description                                                            |
|----------------|------------------------------------------------------------------------|
| <INTERFACE-ID> | Specifies the interface for which the RA guard counters are displayed. |

## Examples

Showing RA guard counters for interface 1/1/1:

```
switch# show nd-snooping ra-guard interface 1/1/1
```

```

RA Guard Policy Counters
=====

RA Guard Policy Applied : POLICY_2
RA Packets Received : 10
RA Packets Forwarded : 5
RA Packets Dropped : 5 [Total]

 reason : Managed flag error [0]
 Other flag error [0]
 Access list error [0]
 Prefix list error [0]
 Router preference error [0]
 Hop limit error [5]

```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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 nd-snooping ra-guard policy

show nd-snooping ra-guard policy [<POLICY-NAME>]

### Description

Shows the RA guard policy configuration.

| Parameter     | Description                                                |
|---------------|------------------------------------------------------------|
| <POLICY-NAME> | Specifies the name of the RA guard policy to be displayed. |

### Examples

Showing RA guard configuration:

```

switch# show nd-snooping ra-guard policy
RA Guard Policy Applied Ports Applied VLANs

POLICY_NAME1 1/1/25,1/1/27,1/1/29-1/1/44,1/1/46 10,20,50-100
POLICY_NAME2 1/1/1-1/1/24

```

```

switch# show nd-snooping ra-guard policy POLICY_NAME1

```

```

RA Guard policy Information
=====
Policy name : POLICY_NAME1
Policy Applied Ports : 1/1/25,1/1/27,1/1/29-1/1/44,1/1/46
Policy Applied VLANs : 10,20,50-100
Hop Limit : enabled
 minimum : 50
 maximum : 150
Managed config flag : On
Other config flag : On
Access List : ACL1
Prefix List : PREFIX_LIST_NAME
Router Preference : high

```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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 nd-snooping ra-guard vlan

show nd-snooping ra-guard vlan <VLAN-ID>]

### Description

Shows RA guard counters for the specified VLAN. Counters are cleared once the RA guard policy is detached from the VLAN.

| Parameter | Description                                                                          |
|-----------|--------------------------------------------------------------------------------------|
| <VLAN-ID> | Specifies a VLAN ID for which the RA guard counters are displayed. Range: 1 to 4094. |

## Examples

Showing RA guard counters for VLAN 2:

```

switch# show nd-snooping ra-guard vlan 2

RA Guard Policy Counters
=====

RA Guard Policy Applied : POLICY_1
RA Packets Received : 20
RA Packets Forwarded : 5

```

```

RA Packets Dropped : 15 [Total]
 reason : Managed flag error [1]
 Other flag error [4]
 Access list error [1]
 Prefix list error [4]
 Router preference error [0]
 Hop limit error [5]

```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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. |

Enabling IPv6 destination guard on a switch prevents ND cache depletion issues and helps in minimizing Denial-of-Service (DoS) attacks. When IPv6 destination guard is enabled address resolution is performed only for the destination addresses that are active on the link.

This feature requires the binding table to be populated with the help of DHCPv6 snooping, ND snooping, or static-ip-bindings. Destination guard enables the destination address based filtering of IPv6 traffic and blocks the Neighbor Discovery (ND) protocol resolution for destination addresses that are not found in the binding table.

## IPv6 destination guard commands

### clear ipv6 destination-guard statistics vlan

```
clear ipv6 destination-guard statistics vlan <VLAN-ID>
```

#### Description

Clears IPv6 destination guard statistics from the specified VLAN.

#### Command context

| Parameter      | Description                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------|
| vlan <VLAN-ID> | Specifies the VLAN for which all destination guard statistics are to be cleared. Range: 1 to 4094. |

#### Examples

Clearing all ipv6 destination-guard statistics for VLAN 10:

```
switch# clear ipv6 destination-guard statistics vlan 10
```

#### Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

#### Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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. |

# ipv6 destination guard

```
ipv6 destination-guard
no ipv6 destination-guard
```

## Description

Enables IPv6 destination guard on a VLAN.

The **no** form of the command removes the IPv6 destination guard from a VLAN.



---

To avoid dropping valid packets when destination guard is enabled, it is recommended to configure DHCPv6 snooping and ND snooping to populate the binding database.

---

## Examples

Enabling IPv6 destination guard policy on a VLAN:

```
switch(config)# vlan 10
switch(config-vlan-10)# ipv6 destination-guard
```

Disabling IPv6 destination guard policy on a VLAN:

```
switch(config-vlan-10)# no ipv6 destination-guard
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context                     | Authority                                                                          |
|--------------|-------------------------------------|------------------------------------------------------------------------------------|
| 8100<br>8360 | config-vlan- <i>&lt;VLAN-ID&gt;</i> | Administrators or local user group members with execution rights for this command. |

## show ipv6 destination-guard statistics vlan

```
show ipv6 destination-guard statistics {vlan <VLAN-ID>}
```

## Description

Shows IPv6 destination guard statistics for the specified VLAN.

## Command context

| Parameter                   | Description                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------|
| vlan <i>&lt;VLAN-ID&gt;</i> | Specifies the VLAN for which all destination guard statistics are to be displayed. Range: 1 to 4094. |

## Examples

Showing IPv6 destination-guard statistics for VLAN 10:

```
switch# show ipv6 destination-guard statistics vlan 10
Packets dropped for VLAN 10 : 25467
```

Showing IPv6 destination-guard statistics for all VLANs:

```
switch# show ipv6 destination-guard statistics
Packets dropped for VLAN 10 : 25467
Packets dropped for VLAN 30 : 434
Packets dropped for VLAN 50 : 8767
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms    | Command context             | Authority                                                                                                                                                              |
|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360 | 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 destination-guard

```
show ipv6 destination-guard
```

### Description

Shows the ipv6 destination-guard configuration.

### Examples

Showing the IPv6 destination-guard configuration:

```
switch# show ipv6 destination-guard
IPv6 Destination-Guard information
Enabled VLANs : 10,20,31-35
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| <b>Platforms</b> | <b>Command context</b>      | <b>Authority</b>                                                                                                                                                       |
|------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8100<br>8360     | 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. |

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: GRE, IPv6 in IPv4, and IPv6 in IPv6.
- A maximum of 16 source IP addresses are supported. Tunnels can have the same source IP address and different destination IP addresses. The source IP, destination IP, and VRF combine to uniquely identify a tunnel.

### 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.

## VRF Aware GRE support




---

VRF-aware GRE is only supported on the 6300, 6400, 8325, 8325H, 8360, and 10000 Switch Series. This feature is supported on the 8325H Switch Series starting from 10.17.0001.

---

The VRF attachments of GRE tunnels in the existing implementation does not let the GRE underlay and GRE overlay to be placed on different VRFs. VRF-aware GRE allows the GRE tunnel underlay and GRE overlay to be placed on different VRFs. With the VRF-aware GRE feature, the tenant and tunnel (overlay) can be in one VRF and the tunnel underlay can be in another VRF. Tunnels are configured in an overlay VRF but the tunnel destination is reachable via the underlay VRF. The underlay VRF for the encapsulated packets needs to be configured on the tunnel using the command **transport vrf**.

A configuration example of VRF-aware GRE tunneling is as follows:

```
switch# configure terminal
switch(config)# interface loopback 1
switch(config-loopback-if)# vrf attach red
switch(config-loopback-if)# ip address 1.1.1.1/24
switch(config-loopback-if)# ip ospf 1 area 0.0.0.0

switch(config)# interface loopback 2
switch(config-loopback-if)# vrf attach blue
switch(config-loopback-if)# ip address 1.1.1.1/32

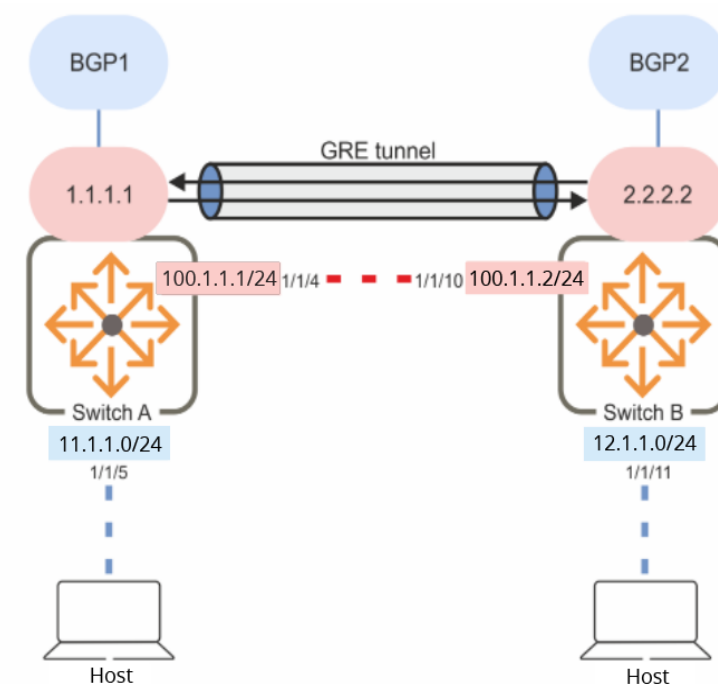
switch(config)# interface tunnel 1 mode gre ipv4
switch(config-gre-if)# vrf attach blue
switch(config-gre-if)# source ip 1.1.1.1
switch(config-gre-if)# destination ip 2.2.2.2
switch(config-gre-if)# transport vrf red
switch(config-gre-if)# ip address 100.1.1.1/24
switch(config-gre-if)# no shutdown
```

Notes regarding the configuration example:

1. *Blue* is an overlay VRF of the tunnel.
2. *Interface tunnel 1* is a routable interface with an IP 100.1.1.1/24 attached to VRF *blue*.
3. Tunnel source IP (the outer SIP (Source IP address) of the outgoing GRE packet) is 1.1.1.1. The source IP can be the IP of any routable interface (e.g. loopback/SVI) on underlay VRF *red*. The interface IP must also be present in overlay VRF *blue*.
4. The destination IP (the outer DIP (Destination IP address) of the outgoing GRE packet) is 2.2.2.2. This is the source-IP of the remote tunnel.
5. *Transport-vrf red* is the underlay VRF of the tunnel. The IP 2.2.2.2 is reachable on this VRF.

- The destination IP must be reachable on the overlay VRF *blue* and requires route leaking. The route leak can be done via static or dynamic IVRL. An example command would be: **ip route 12.1.1.1/24 tunnel1 vrf blue**

## Example of VRF-aware GRE topology



In the topology figure, the tunnel is between Switch A (Endpoint 1.1.1.1) and Switch B (endpoint 2.2.2.2). The tunnel is configured in the overlay VRF *blue*. The connected hosts are in VRF *blue* and the BGP session is established in the same overlay VRF *blue*.

These endpoints are reachable via underlay ports 1/1/1 and 1/1/10 respectively in the underlay VRF *red*. Note the following points:

- The tunnel is configured in the overlay VRF *blue*.
- The loopback interface with the tunnel source IP is in the overlay VRF *blue* in order to bring up the tunnel which is configured in the *blue* VRF.
- The loopback interface is configured in the underlay VRF *red* and has the same tunnel source IP. It is a reachable tunnel endpoint in the underlay.
- Route leaking is occurring via IVRL from underlay VRF *red* to overlay VRF *blue*. This route leak can be done via static IVRL or Dynamic IVRL using BGP e.g. running the command **ip route 12.1.1.1/24 tunnel1 vrf blue**.

## IVRL using Static Route leaking

Route leaking with port:

```
ip route 2.2.2.0/24 1/1/1 vrf blue
```

Route leaking with port and next hop:

```
ip route 2.2.2.0/24 1/1/1 10.1.1.2 vrf blue
ip route 10.1.1.0/24 1/1/1 vrf blue
```

## IVRL using Dynamic Route leaking via BGP

We leak only the remote endpoint and the underlay route from the underlay VRF red into the overlay VRF blue using BGP OSPF redistribute with route-map.

To prevent remote endpoints being learned twice via IBGP as well as IVRL, we need to block the advertisement of these neighbor IPs back to the neighbor by setting community no-advertise in the route maps.

Example configuration of IVRL using Dynamic Route leaking via BGP:

```
vrf blue
 rd 4:100
 address-family ipv4 unicast
 route-target import 3:100
 exit-address-family
vrf red
 rd 3:100
 address-family ipv4 unicast
 route-target export 3:100
 route-target export route-map LEAK_DEST_TEP
 exit-address-family
!
ip prefix-list DEST_TEP_RULE seq 5 permit 2.2.2.2/32
ip prefix-list DEST_TEP_RULE seq 6 permit 10.1.1.0/24
!
route-map LEAK_DEST_TEP permit seq 10
 match ip address prefix-list DEST_TEP_RULE
 set community no-advertise

router bgp 1
!
 vrf blue
 bgp router-id 111.1.1.1
 neighbor 100.1.1.2 remote-as 1
 neighbor 100.1.1.2 update-source 100.1.1.1
 address-family ipv4 unicast
 neighbor 100.1.1.2 activate
 redistribute connected
 exit-address-family
!
 vrf red
 address-family ipv4 unicast
 redistribute ospf route-map LEAK_DEST_TEP
 exit-address-family
```

## 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

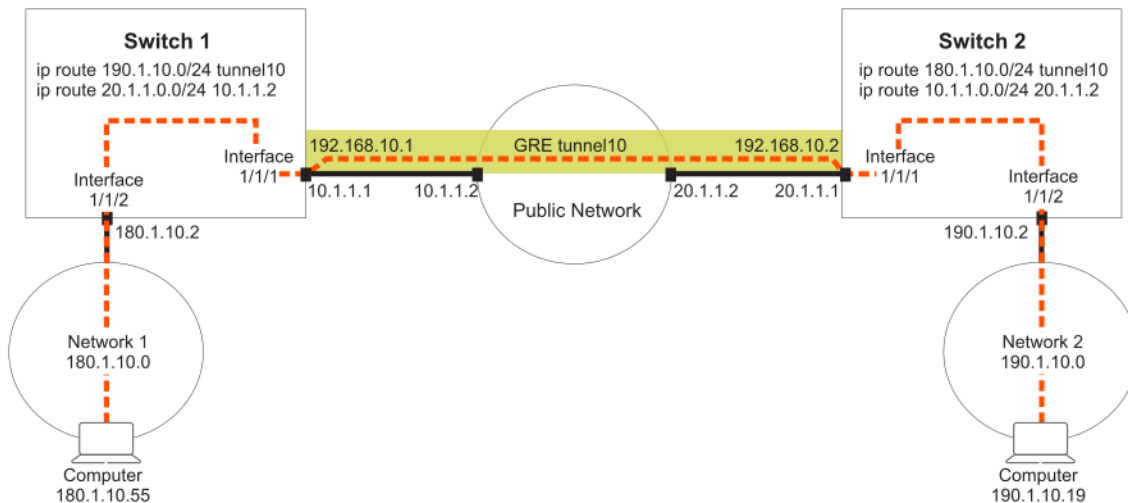
This example creates the following configuration:

- Creates GRE tunnel **33**.
- Set the tunnel IP address to **10.10.20.209/24**.
- 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.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ip address 10.10.20.209/24
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.



## 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)# 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)# ip address 180.1.10.2/24
switch(config-if)# no shutdown
switch(config-if)# exit
```
- 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
switch(config-gre-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)# 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)# 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.  

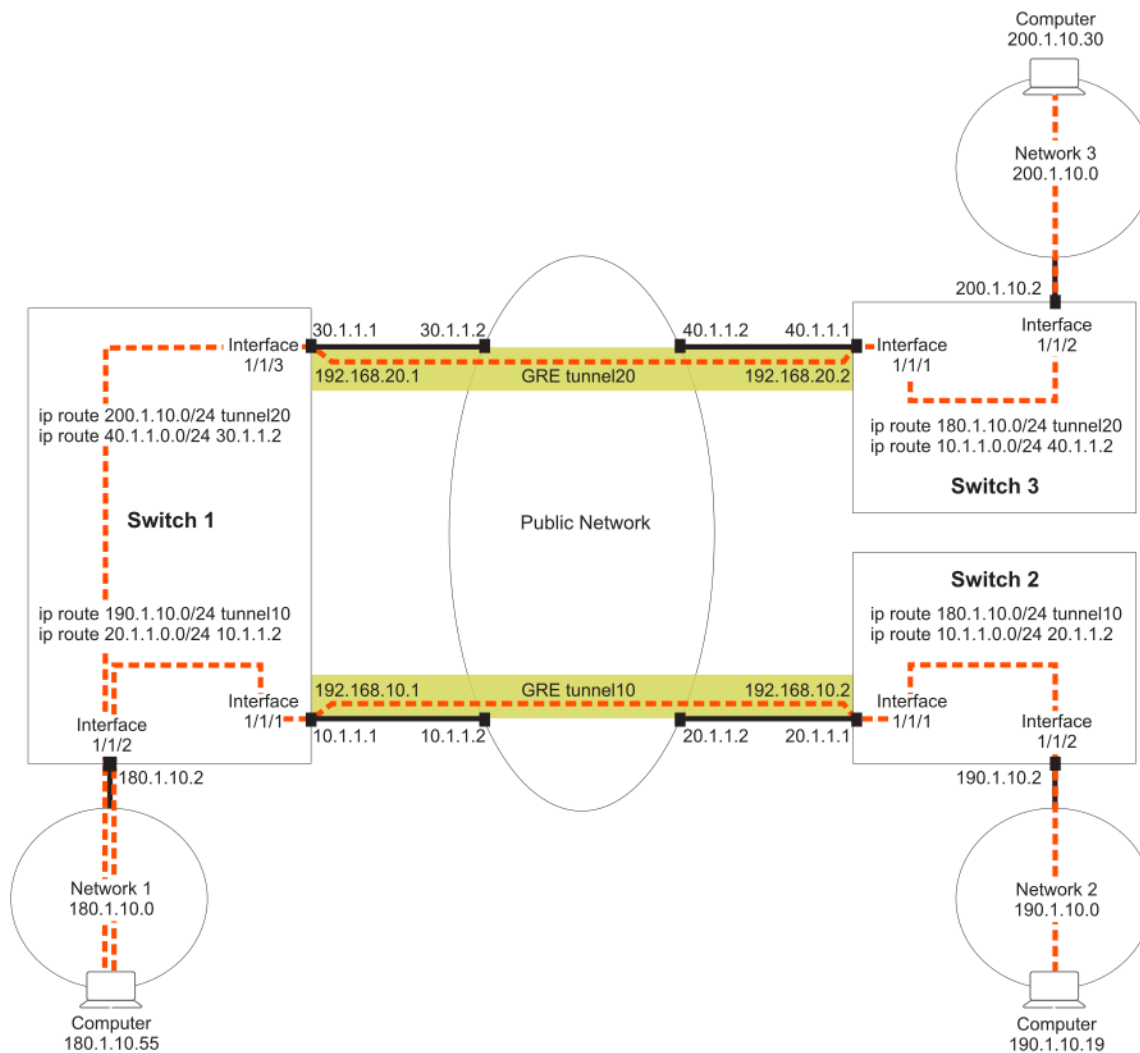
```
switch(config)# interface 1/1/2
switch(config-if)# ip address 190.1.10.2/24
switch(config-if)# no shutdown
switch(config-if)# exit
```
- c. Create GRE tunnel **10** and assign the IP address **192.168.10.2/24**, source address **20.1.1.1**, and destination address **10.1.1.1** to it.  

```
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 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.



## 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)# 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)# ip address 180.1.10.2/24
switch(config-if)# no shutdown
switch(config-if)# exit
```
  - 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)# 30.1.1.1/24
switch(config-if)# no shutdown
switch(config-if)# exit
```
  - 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
switch(config-gre-if)# exit

```

- 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
switch(config-gre-if)# exit

```

- 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
switch(config)# ip route 190.1.10.0/24 tunnel10

```

- 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
switch(config)# ip route 200.1.10.0/24 tunnel20

```

## 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)# 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)# ip address 190.1.10.2/24
switch(config-if)# no shutdown
switch(config-if)# exit

```

- 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)# 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)# 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.

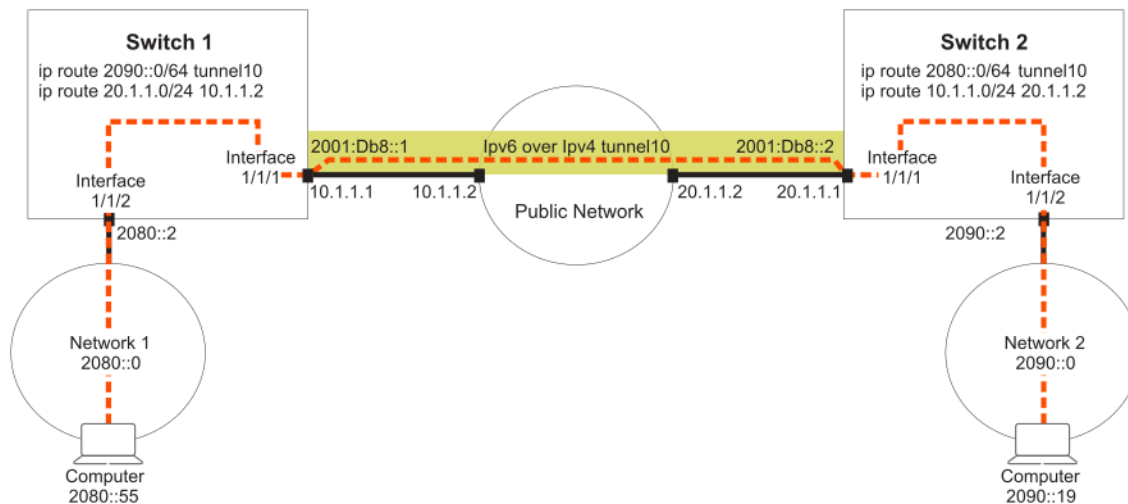
```

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.



### 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)# 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)# 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)# 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)# ipv6 address 2090::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::2/32**, source address **10.1.1.1**, and destination address **20.1.1.1** to it.

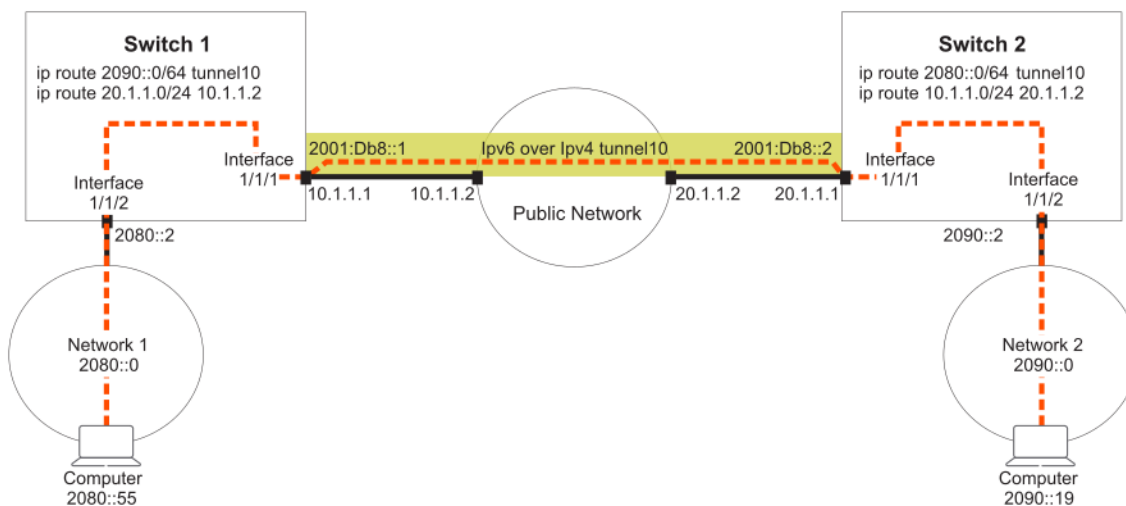
```
switch(config)# interface tunnel 10 mode ip 6in4
switch(config-ip-if)# ipv6 address 2001:DB8::2/62
switch(config-ip-if)# source ip 20.1.1.1
switch(config-ip-if)# destination ip 10.1.1.1
switch(config-ip-if)# no shutdown
switch(config-ip-if)# exit
```

- 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.



### 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)# 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)# 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 2090::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)# 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)# 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.

Parameter	Description
<DESC>	Specifies the descriptive text to associate with the IP tunnel. Range: 1 to 64 printable ASCII characters.

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100	config-gre-if	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8320 8325 8325H 8360 9300 9300S 10000	config-ip-if	

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.

Parameter	Description
<IPV4-ADDR>	Specifies the destination IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

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 mode gre ipv4
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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

destination ipv6

```
destination ipv6 <IPVv6-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.

Parameter	Description
<IPV6-ADDR>	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.

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-ip-if	Administrators or local user group members with execution rights for this command.

interface tunnel

```
interface tunnel <TUNNEL-NUMBER> mode {gre ip | ip 6in4 | ip 6in6 | ipsec ipv4}
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.



The option **ipv4** is deprecated and it is advised to use **ip** instead. Execute **show deprecated-commands** to view a list of deprecated commands.

Parameter	Description
mode {gre ip ip 6in4 ip 6in6}	<p>Creates an IP tunnel. Choose one of the following options:</p> <ul style="list-style-type: none">▪ gre ip: Creates a GRE tunnel.▪ ip 6in4: Creates an IPv4 tunnel for IPv6 traffic.▪ ip 6in6: Creates an IPv6 tunnel for IPv6 traffic.▪ ipsec ipv4: Creates an IPsec tunnel for IPv4. After this command is executed, command-line interface enters the IPsec Tunnel interface context <p>This is optional in the no form, unless a mode has already been entered.</p>
<TUNNEL-NUMBER>	<p>Specifies the number for a new tunnel. Range for 8100, 8320, 8325, 8325H, 8360, 9300, and 9300S switches: 1-255. Range for 10000 switch series: 1-1279. Numbering is shared between all tunnels, so the same tunnel number cannot be used for an IPv6 in IPv4 tunnel and a GRE tunnel. Maximum number of GRE, 6in4 or 6in6 tunnels supported simultaneously for the 8100 switch is 64. Maximum number of GRE, 6in4 or 6in6 tunnels supported</p>

Parameter	Description
	simultaneously for the 8320, 8325, 8325H, 8360, 9300, 9300S, and 10000 switch is 127. IPSec tunnels are only supported on 10000 switch series.
<code><EXISTING-TUNNEL-NUMBER></code>	Specifies the number for an existing IP tunnel. Range for 8100, 8320, 8325, 8325H, 8360, 9300, and 9300S switches: 1-255. Range for 10000 switch series: 1-1279. Numbering is shared between all tunnels, so the same tunnel number cannot be used for an IPv6 in IPv4 tunnel and a GRE tunnel. Maximum number of GRE, 6in4 or 6in6 tunnels supported simultaneously for the 8100 switch is 64. Maximum number of GRE, 6in4 or 6in6 tunnels supported simultaneously for the 8320, 8325, 8325H, 8360, 9300, 9300S, and 10000 switch is 127. IPSec tunnels are only supported on 10000 switch series.

Examples

Defines a new GRE tunnel with number **27**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)#
```

Switches to the **config-gre-if** context for existing tunnel **33**.

```
switch(config)# interface tunnel 33
switch(config-gre-if)#
```

Deletes GRE tunnel **33**.

```
switch(config)# no interface tunnel 33
```

Defines a new IPv6 in IPv4 tunnel with number **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)#
```

Switches to the `config-ip-if` context for existing tunnel **27**.

```
switch(config)# interface tunnel 27
switch(config-ip-if)#
```

Deletes IPv6 in IPv4 tunnel **27**.

```
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-if)#
```

Deletes IPv6 in IPv6 tunnel with number **3**.

```
switch(config)# no interface tunnel 33 mode gre ipv4
```

Command History

Release	Modification
10.16.1000	GRE support added for 8325H switch series.
10.14	The ipv4 parameter is deprecated and replaced with ip .
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-gre-if config-ip-if config	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
<IPV4-ADDR>	Specifies the tunnel IP 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 .
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-gre-if	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
<IPV6-ADDR>	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.
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.

Examples

Defines the local IP address **2001:DB8:5::1/64** for tunnel **8** for an IPv6 to IPv6 tunnel.

```
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**.

```
switch(config)# interface tunnel 8
switch(config-ip-if)# no ipv6 address 2001:DB8:5::1/64
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-ip-if config-if	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
<VALUE>	Specifies the MTU in bytes. Range: 1,280 bytes to 9,192 bytes.

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 ip 6in4
switch(config-ip-if)# mtu 1000
```

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)# ip mtu
```

Sets the MTU on IPv6 in IPv6 tunnel **8** to **900** bytes.

```
switch(config)# interface tunnel 8 mode ip 6in6
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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100	config-gre-if	Administrators or local user group members with execution rights for this command.
8320	config-ip-if	
8325		
8325H		
8360		
9300		
9300S		
10000		

show interface tunnel

show interface tunnel[<TUNNEL-NUMBER>] [vsx-peer]

Description

Shows configuration settings for all IP tunnels, or a specific tunnel.

Parameter	Description
<TUNNEL-NUMBER>	Specifies the number of an IP tunnel. Range: 1 to 127.
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.



Note: Subinterfaces are supported as IP 6in4, 6in6 and GRE tunnel underlays on 6300, 6400, 8100 and 8360 Switch Series.

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 IP
tunnel interface IP address 192.0.2.0/24
tunnel source IP address 1.1.1.1
tunnel destination IP address 2.2.2.2
tunnel ttl 60
tunnel transport vrf red
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
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	RX	TX	Total
L3 Packets	0	0	0

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 IP
tunnel interface IP address 192.0.2.0/24
tunnel source IP address 1.1.1.1
tunnel destination IP address 2.2.2.2
tunnel ttl 60
tunnel transport vrf BBlue
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
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	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0

```
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	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0

Command History

Release	Modification
10.17	Added support for subinterfaces as IP 6in4, 6in6 and GRE tunnel underlays on 6300, 6400, 8100 and 8360 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	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 running-config interface tunnel

show running-config interface tunnel<TUNNEL-NUMBER> [vsx-peer]

Description

Shows the commands used to configure a tunnel.

Parameter	Description
<TUNNEL-NUMBER>	Specifies the number of an IP tunnel. Range: 1 to 127.
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.



VRF Route Leaking is needed for **VRF Aware GRE** to work when **transport vrf** is configured.

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 tunnel1
interface tunnel 1 mode ip 6in6
description Network2 Tunnel
source ipv6 2::1
destination ipv6 2::2
ipv6 address 4::1/64
ttl 60
```

Shows the configuration for an IPsec tunnel:

```
switch# show running-config interface tunnel 1
interface tunnel 1 mode ipsec ipv4
description Network1-Tunnel
source ip 1.1.1.1
destination ip 2.2.2.2
```

Shows the configuration of interface tunnel transport:

```
switch#(config-gre-if)# show running-config interface tunnel2
interface tunnel 2 mode gre ipv4
source ip 10.10.20.11
destination ip 10.20.1.2
transport vrf VRF1
ip address 10.10.10.1/24
ttl 60
```

Command History

Release	Modification
10.17	Added support for subinterfaces as IP 6in4, 6in6 and GRE tunnel underlays on 6300, 6400, 8100 and 8360 Switch Series.
10.12.1000	Command updated to display the IPsec configuration.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	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.

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**.

```
switch(config)# interface tunnel 33 mode gre ipv4  
switch(config-gre-if)# no shutdown
```

Disables GRE interface **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4  
switch(config-gre-if)# shutdown
```

Enables IPv6 in IPv4 interface **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4  
switch(config-ip-if)# no shutdown
```

Disables IPv6 in IPv4 interface **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4  
switch(config-ip-if)# shutdown
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
<code><IPv4-ADDR></code>	Specifies the source IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
<IPV6-ADDR>	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.

Examples

Defines the source IPv6 address to be **2001:DB8::1** for IPv6 in IPv6 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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 9300S 10000	config-ip-if	Administrators or local user group members with execution rights for this command.

tll

```
tll <COUNT>
no tll
```

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.

Parameter	Description
<COUNT>	Specifies the hop count. Range: 1 to 255. Default: 64.

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100	config-gre-if	Administrators or local user group members with execution rights for this command.
8320	config-ip-if	
8325		
8325H		
8360		
9300		
9300S		
10000		

transport vrf

```
transport vrf <VRF-NAME>  
no transport vrf <VRF-NAME>
```

Description

Indicates the transport VRF of the tunnel. This VRF is the same as the VRF associated with the underlay interface over which the tunnel sends or receives encapsulated packets. If not configured, VRF Aware feature is not enabled.

The **no** form of this command removes the transport VRF from the tunnel.

Parameter	Description
<VRF-NAME>	Specifies the transport VRF of the tunnel.

Usage

- Transport VRF must be different from the tunnel VRF that is already configured.
- Only meant for usage on VRF-aware GRE tunnels.

Examples

Example of adding VRF *VRF1* transport to a tunnel:

```
switch# configure terminal  
switch(config)# interface tunnel 1 mode gre ip  
switch(config-gre-if)# transport vrf VRF1
```

Example of removing the transport VRF *VRF1* from the tunnel:

```
switch# configure terminal  
switch(config)# interface tunnel 1  
switch(config-gre-if)# no transport vrf VRF1
```

Command History

Release	Modification
10.14.1000	Command introduced on 8325 and 10000 Switch series.

Command Information

Platforms	Command context	Authority
6300 8325 8325H 10000	config-gre-if	Administrators or local user group members with execution rights for this command.

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**).

Parameter	Description
<VRF-NAME>	Specifies the VRF name to which to assign the tunnel.

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 gre ipv4
switch(config-ip-if)# vrf attach vrf2
```

Reassigns IPv6 in IPv4 tunnel **27** to the default VRF.

```
switch(config)# interface tunnel 27
switch(config-ip-if)# no 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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100	<code>config-gre-if</code>	Administrators or local user group members with execution rights for this command.
8320	<code>config-ip-if</code>	
8325		
8325H		
8360		
9300		
9300S		
10000		



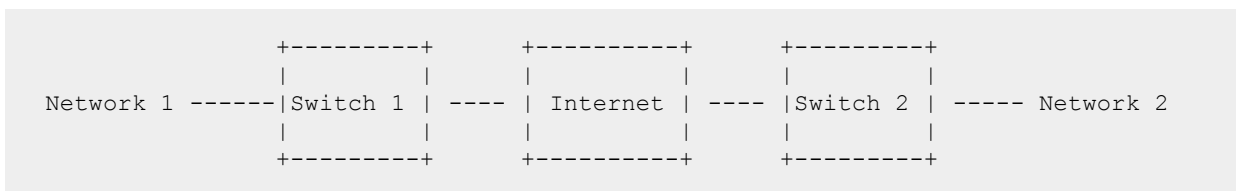
IPsec tunnel is supported only on 10000 switch series.

An IPsec tunnel is a secure tunneling protocol that creates virtual point-to-point links over an IP network. IPsec provides secure communication over a network by encrypting packets. It encapsulates the entire IP packet and adds an outer IP header.

IPsec tunneling protocol

IPsec creates a virtual point-to-point link between two devices by encrypting and encapsulating various protocols within an IP network. For example, the following diagram shows an IPsec tunnel created between Switch 1 and Switch 2. Even if Network 1 and Network 2 are separated by multiple network devices, IPsec creates a virtual point-to-point link that makes it appear as if they are directly connected to each other. When a packet is sent from Network 1 to Network 2 (and vice versa), it is transmitted through various network devices in between, as indicated by the cloud. However, since the packets are encrypted and encapsulated, the intermediate network devices are unaware of Network 1 and Network 2.

Figure 1 IPsec tunnel between two networks



To establish an IPsec tunnel, you need to configure Pensando Policy and Services Manager (PSM). For complete information on the Pensando Policy and Services Manager, refer to the Pensando Policy and Services Manager for Distributed Services Switches: User Guide.

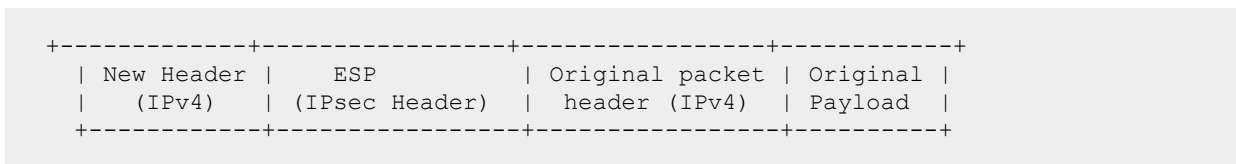


IPsec tunnels can only be established if the switch is running with either the L3-core or spine profiles. If you are using the L3-agg or leaf profiles, IPsec tunnels are not supported.

IPsec Tunnel encapsulation and decapsulation

The following diagram shows the example of an IPsec encapsulated packet:

Figure 2 IPsec encapsulated packet



When a packet is sent from switch 1 to switch 2 using an IPsec tunnel between two networks:

1. Switch 1 receives an incoming packets from Network 1.
2. If the packet is not intended for the switch (destination MAC), it will be forwarded.
3. If the switch receives the packet, it will check the destination IP address to determine whether the packet needs to be processed by the CPU or forwarded using the next-hop in the routing table.
4. Once the switch receives the next-hop information, it encrypts and encapsulates the packet if the egress interface is a tunnel interface, and then sends it to the next-hop.
5. Once the packet is routed in the network and received by switch 2, the packet is decrypted and decapsulated.
6. The inner packet (actual payload) will be routed to Network 2.

BGP over an IPsec tunnel interface

BGP over an IPsec tunnel can be configured by defining the BGP peer as the IPsec tunnel overlay IP. The IP address of an IPsec interface is reachable over the IPsec tunnel. For more information, see the *Configuring BGP over an IPsec tunnel interface* section in the IP Routing Guide.

Limitations

- IPsec tunnels must not be configured under the default VRF. Since the Distributed Service Module (DSM) to IPsec tunnel is a VRF-based mapping, tunnels need to be configured under a non-default VRF only.
- IPsec tunnels are not supported with ROP or loopback as an underlay.
- IPsec tunnels are supported with only SVI as an underlay, and the source IP of the tunnel must be derived from the underlay SVI.
- IPsec tunnels exceeding 1024 per VRF will be dropped.

Unsupported features

- IPsec tunnel endpoint as ipv6
- TTL on IPsec tunnel
- VRF change or delete on IPsec tunnel
- Source IP change or delete on IPsec tunnel
- Destination IP change or delete on IPsec tunnel
- IPVRL on IPsec tunnels with a static route
- Underlay on different VRF
- ECMP of IPsec tunnels in the route
- Multicast over IPsec tunnel
- ACL on IPsec tunnels
- IPsec over L3 Tunnels (GRE/6in4/6in6)
- ACL/PBR on VXLAN tunnels which will be sent over IPsec
- L3-agg and leaf profiles
- BGP over IPsec is not supported in IPsec Active-Standby mode
- Dynamic BGP peering is not supported over IPsec.
- BGP-peer Groups are not supported over IPsec.
- Route Reflectors are not supported.
- IP unnumbered IP as BGP source IP is not supported.
- Routes exceeding 1024 IPsec routes per VRF will be dropped. The ordering of preferred routes cannot be guaranteed when more routes are learned than supported.

- Backup routing between Static and BGP for the same prefix is not supported.
- BFD failover for IPsec BGP is not supported.

IPsec tunnels commands

description

```
description <DESC>
no description
```

Description

Adds descriptive information to help administrators and operators understand the purpose or role of an IPsec tunnel interface.

The **no** form of this command removes the description from a tunnel.

Parameter	Description
<DESC>	Specifies the descriptive text to associate with the IPsec tunnel. Range: 1 to 64 printable ASCII characters.

Examples

Adding a description for the IPsec tunnel **1**:

```
switch(config)# interface tunnel 1 mode ipsec ipv4
switch(config-ipsec-if)# description Network1 Tunnel
```

Removing the description for IPsec tunnel **3**:

```
switch(config)# interface tunnel 3
switch(config-ipsec-if)# no description
```

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
10000	config-ipsec-if	Administrators or local user group members with execution rights for this command.

destination ip

```
destination ip <IPV4-ADDR>
no destination ip <IPV4-ADDR>
```

Description

Adds or updates the destination IP address used in encapsulation. You cannot modify or delete the destination IP address . To delete or modify the IP address, you must first remove the old values and configure the new values.

The **no** form of this command removes the destination IP address from an IPsec tunnel.

Parameter	Description
<code><IPV4-ADDR></code>	Specifies the destination IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Adding the destination IP address to be **2.2.2.2** for IPsec tunnel:

```
switch(config-ipsec-if) # destination ip 2.2.2.2
```

Deleting the destination IP address **4.4.4.1**:

```
switch(config-ipsec-if) # no destination ip 4.4.4.1
```

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
10000	config-ipsec-if	Administrators or local user group members with execution rights for this command.

interface tunnel

```
interface tunnel <TUNNEL-NUMBER> [mode ipsec ipv4]  
no interface tunnel <TUNNEL-NUMBER> [mode ipsec ipv4]
```

Description

Creates or updates an IPsec tunnel. After you enter the command, the firmware switches to the configuration context for the IPsec tunnel.

The **no** form of this command deletes the IPsec tunnel.

Parameter	Description
<code>mode ipsec ipv4</code>	Specifies the IPsec tunnel mode for the interface.
<code><TUNNEL-NUMBER></code>	Specifies the number for a new tunnel. Range: 1 to 1279.

Examples

Creating a new IPsec tunnel with number 1.

```
switch(config)# interface tunnel 1 mode ipsec ipv4  
switch(config-ipsec-if)#
```

Deleting the IPsec tunnel with number 3.

```
switch(config)# no interface tunnel 3 mode ipsec ipv4
```

Command History

Release	Modification
10.12.1000	Command Introduced.

Command Information

Platforms	Command context	Authority
10000	config	Administrators or local user group members with execution rights for this command.

ip address

```
ip address <IPV4-ADDR>/<MASK>  
no ip address <IPV4-ADDR>/<MASK>
```

Description

Configures or updates the ip address of the IPsec interface. Each IPsec tunnel interface can have 1 primary address.

The **no** form of this command deletes the local IP address assigned to the IPsec interface. The tunnels need to be shutdown before removing the IP address as it is restricted when the IPsec tunnel is up.

Parameter	Description
<IPV4-ADDR>	Specifies the tunnel IP 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 .
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.

Examples

Defines the local IP address **10.10.10.1** for the IPsec tunnel.

```
switch(config)# interface tunnel 1 mode ipsec ipv4  
switch(config-ipsec-if)# ip address 10.10.10.1/24
```

Deletes the local IP address **10.10.10.1** for IPsec tunnel.

```
switch(config)# interface tunnel 1 mode ipsec ipv4
switch(config-ipsec-if)# no ip address 10.10.10.1/24
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config-ipsec-if	Administrators or local user group members with execution rights for this command.

ip mtu

ip mtu <VALUE>

Description

Sets the MTU (maximum transmission unit) for an IPsec interface. The default value is 1500 bytes.

Parameter	Description
<VALUE>	Specifies the MTU in bytes. Range: 1,280 bytes to 9,198 bytes.

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. This is an optional command. If the command is not configured, the default value of 1500 will be used.

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 MTU of the underlying interface that the tunnel is using.

Examples

Setting the MTU on IPv4 tunnel **1** to **9000** bytes.

```
switch(config)# interface tunnel 1 mode ipsec ipv4
switch(config-ipsec-if)# ip mtu 9000
```

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
10000	config-ipsec-if config	Administrators or local user group members with execution rights for this command.

IPsec Tunnel backup route support



IPsec tunnel is supported only on 10000 switch series.

With this feature, backup static routes can now be added via CLI with IPsec tunnel interface as nexthop. Multiple IPsec tunnel interface as nexthop with different distance can be added for a prefix now.

Lowest distance routes are preferred as the active route. Once the active route goes-down, the next lowest distance route is considered as the active route.

This feature provides backup route path for routes pointing IPsec tunnel interface as ECMP of IPsec tunnel interface is not supported.

Examples

Configuring route support:

```
switch(config)# ip route 10.1.1.0/24 tunnel10 vrf red distance 10
switch(config)# ip route 10.1.1.0/24 tunnel20 vrf red distance 5
```



Same route prefix for different IPsec tunnels as nexthop with same distance cannot be configured.

Configuring route support for distance 10 on tunnel10:

```
switch(config)# ip route 10.1.1.0/24 tunnel10 vrf red distance 10
switch(config)# ip route 10.1.1.0/24 tunnel20 vrf red distance 10
Failed to configure static route. Route already exists with same distance 10 on
tunnel10.
```



Static back route is supported only for IPsec tunnel interface as nexthop and not supported for other types of nexthops.

show capacities-status

```
show capacities-status
```

Description

Showing system capacities status and their values at the system level

Examples

Showing capacities status of IPsec tunnels:

```
switch# show capacities-status

System Capacities Status
Capacities Status Name                               Value Maximum
-----
.....
Number of IPsec tunnels currently configured          5    1024
^^^
```

Command History

Release	Modification
10.12.1000	Updated to display the IPsec related information.

Command Information

Platforms	Command context	Authority
10000	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 capacities-status tunneling

```
show capacities-status tunneling
```

Description

Showing system capacities status and their values for IPsec IPv4, GRE IPv4, IPv6 in IPv4, and IPv6 in IPv6 features.

Examples

Showing capacities status of IPsec tunnels:

```
switch# show capacities-status
System Capacities Status: Filter Tunneling
Capacities Status Name                               Value Maximum
-----
-----
Number of GRE IPv4, "IPv6 in IPv4" and "IPv6 in IPv6" Tunnels currently configured
                                                0    127
Number of IPsec tunnels currently configured
                                                0    1024
Number of unique GRE IPv4, "IPv6 in IPv4" and "IPv6 in IPv6" tunnel local IPs
currently configured                               0    16
Number of unique GRE IPv4, "IPv6 in IPv4" and "IPv6 in IPv6" tunnel TTLs currently
configured                                         0    4
^^^
```

Command History

Release	Modification
10.12.1000	Updated to display the IPsec related information.

Command Information

Platforms	Command context	Authority
8325H 10000	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 interface tunnel

show interface tunnel [<TUNNEL-NUMBER>]

Description

Shows configuration settings for all IPsec tunnels. If the tunnel number is specified, then the command shows the configuration settings of the specified IPsec tunnel.

Parameter	Description
<TUNNEL-NUMBER>	Specifies the number of an IP tunnel. Range: 1 to 127.

Examples

Showing configuration settings for all tunnels:

```
switch# show interface tunnel

Interface tunnel1 is down
Admin state is up
tunnel type IPsec IPv4
tunnel source IPv4 address 1.1.1.1
tunnel destination IPv4 address 2.2.2.2
tunnel ip address 100.1.1.12/24
Description: Network1-Tunnel
Interface tunnel2 is down
Admin state is up
tunnel type IPsec IPv4
tunnel source IPv4 address 3.3.3.3
tunnel destination IPv4 address 4.4.4.4
tunnel ip address 200.1.1.12/24
Description: Network2-Tunnel
```

Showing configuration settings for the IPsec tunnel [1]:

```
switch# show interface tunnel 1

Interface tunnel1 is down
Admin state is up
State information:
Description: Network1-Tunnel
tunnel type IPsec IPv4
tunnel source IPv4 address 1.1.1.1
tunnel destination IPv4 address 2.2.2.2
```

Command History

Release	Modification
10.15	Displays the IP address as a parameter
10.12.1000	Updated to display the IPsec related information.

Command Information

Platforms	Command context	Authority
10000	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 interface tunnel brief

```
show interface tunnel [<TUNNEL-NUMBER>] brief
```

Description

Shows the brief tunnel information such as tunnel interface names and link state.

Parameter	Description
<TUNNEL-NUMBER>	Specifies the number of an IP tunnel. Range: 1 to 127.

Examples

Showing the brief tunnel information of all tunnels:

```
switch# show interface tunnel 1 brief
-----
Tunnel name          IP Address          Status
-----
tunnel1              100.1.1.12/24      down
tunnel2              200.1.1.12/24      down
```

Showing the brief tunnel information of the IPsec tunnel 1:

```
switch# show interface tunnel brief
-----
---
Port      Native Mode  Type  Enabled Status Reason  Speed  Description
         VLAN
-----
tunnel1  --   routed --   yes   down   --     --
```

Command History

Release	Modification
10.15	Displays the IP address as a parameter.
10.12.1000	Updated to display the IPsec related information.

Command Information

Platforms	Command context	Authority
10000	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 running-config interface tunnel

show running-config interface tunnel [<TUNNEL-NUMBER>]

Description

Shows the configuration of an IPsec tunnel.

Parameter	Description
<TUNNEL-NUMBER>	Specifies the number of an IP tunnel. Range: 1 to 127.

Examples

Showing the configuration for an IPsec tunnel:

```
switch# show running-config interface tunnel 1
interface tunnel 1 mode ipsec ipv4
description Network1-Tunnel
source ip 1.1.1.1
destination ip 2.2.2.2
ip address 100.1.1.12/24
```

Command History

Release	Modification
10.15	Displays the IP address as a parameter.
10.12.1000	Updated to display the IPsec related information.

Command Information

Platforms	Command context	Authority
10000	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 running-config current-context

```
show running-config current-context
```

Description

Shows the IPsec tunnel configuration under the current context.

Examples

Showing the IPsec tunnel configuration under the current context:

```
switch(config-ipsec-if)# show running-config current-context
interface tunnel 1 mode ipsec ipv4
  description Network1-Tunnel
  source ip 1.1.1.1
  destination ip 2.2.2.2
  ip address 100.1.1.12/24
```

Showing the the IPsec tunnel configuration under the current context(Removing or modifying the destination IP):

```
Switch(config-ipsec-if)# show run current-context
interface tunnel 1 mode ipsec ipv4
  vrf attach c001
  source ip 144.0.1.1
  destination ip 144.0.1.2
  no shutdown
10000-24(config-ipsec-if)# no destination ip
Destination IP deletion not allowed for IPsec tunnel1
10000-24(config-ipsec-if)# destination ip 144.0.1.3
Destination IP modification not allowed for IPsec tunnel1
```

Command History

Release	Modification
10.15	Displays the IP address as a parameter.
10.12.1000	Updated to display the IPsec related information.

Command Information

Platforms	Command context	Authority
10000	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.

source ip

```
source ip <IPV4-ADDR>
```

Description

Adds the source IP address to be used for IPsec encapsulation. Note that an existing tunnel cannot be modified or deleted. To change an existing tunnel, that tunnel must be removed and configured with the new values.

Parameter	Description
<IPv4-ADDR>	Specifies the source IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Adding the source IP address to be **1.2.3.4** for IPsec tunnel **1**:

```
switch(config)# interface tunnel 1 mode ipsec ipv4
switch(config-ipsec-if)# source ip 1.2.3.4
```

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
10000	config-ipsec-if	Administrators or local user group members with execution rights for this command.

vrf attach

vrf attach <VRF-NAME>

Description

Assigns an IPsec tunnel to a VRF. By default, all tunnels are automatically assigned to the default VRF when they are created. This is an optional command.

The **no** form of this command assigns a tunnel to the default VRF (*default*).

Parameter	Description
<VRF-NAME>	Specifies the name of the VRF to which the tunnel will be assigned.

Examples

Assigning IPsec tunnel **1** to **vrf1**.

```
switch(config)# interface tunnel 1 mode ipsec ipv4
switch(config-ipsec-if)# vrf attach vrf1
```

Command History

Release**Modification**

10.12.1000

Command introduced.

Command Information**Platforms****Command context****Authority**

10000

`config`
`config-ipsec-if`

Administrators or local user group members with execution rights for this command.

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.



On 10000 series switches, IP Source Lockdown and PSM / Distributed Services (DSS) are mutually exclusive. If both features are enabled, unexpected behavior may occur.

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
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPv4-ADDR>	Specifies the client IPv4 unicast address.
<MAC-ADDR>	Specifies the client MAC address.
<IFNAME>	Specifies the interface on which the client is connected.

Examples

Adding a static IPv4 binding:

```
switch(config)# ipv4 source-binding 1 10.2.1.4 00:50:56:96:e4:cf 1/1/1
```

Removing a IPv4 binding:

```
switch(config)# no ipv4 source-binding 1 10.2.1.4 00:50:56:96:e4:cf 1/1/1
```

Command History

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

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).



This configuration will disable flow tracking statistics collection.

Examples

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

Release	Modification
10.14	Added information related to role based IPFIX.
10.12	Command enabled on 8325 and 10000 series switches.
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 10000	config-if	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPv4-ADDR>	Specifies the client IPv4 unicast address.

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 History

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

show ipv4 source-binding

```
show ipv4 source-binding [vsx-peer]
```

Description

Shows all IPv4 static source binding information irrespective of source lockdown 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

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

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	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 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.

Parameter	Description
binding	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 .
interface <IFNAME>	Specifies the client interface (port). When entered without the binding parameter, the summary status information is displayed for the specified interface.
ip <IPV4-ADDR>	Specifies the client IPv4 unicast address.
mac <MAC-ADDR>	Specifies the client MAC address.
vlan <VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
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 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 : --

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

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

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 : --
```

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

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
```

Command History

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	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.

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.

Parameter	Description
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPv6-ADDR>	Specifies the client IPv6 address.
<MAC-ADDR>	Specifies the client MAC address.
<IFNAME>	Specifies the interface on which the client is connected.

Examples

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

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

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).



This configuration will disable flow tracking statistics collection.

Examples

Enabling IPv6 source lockdown on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 source-lockdown
```

Enabling IPv6 source lockdown on interface lag112:

```
switch(config)# interface lag112
switch(config-if)# ipv6 source-lockdown
```

Disabling IPv6 source lockdown on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 source-lockdown
```

Command History

Release	Modification
10.14	Added information related to role based IPFIX.
10.12	Command enabled on 8325 and 10000 series switches.
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8325 8360 10000	config-if	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPV6-ADDR>	Specifies the client IPv6 address.

Example

Configure IPv6 source lockdown hardware retry for the client on VLAN 1.

```
switch(config)# ipv6 source-lockdown hardware retry 1 2000::2
```

Command History

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

show ipv6 source-binding

```
show ipv6 source-binding [vsx-peer]
```

Description

Shows all IPv6 static source binding information irrespective of source lockdown 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

Showing all IPv6 source binding information:

```
switch# show ipv6 source-binding
```

PORT	VLAN	MAC-ADDRESS	HW-STATUS	FROM	IPv6-ADDRESS
1/1/1	1234	00:50:56:96:e4:cf	Yes/No	static	3000::1
1/1/1	1	00:50:56:96:04:4d	Yes/No	static	3000::2
1/1/24	1	00:01:01:00:00:01	Yes	static	1001::1

Command History

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	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 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.

Parameter	Description
binding	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 .
interface <IFNAME>	Specifies the client interface (port). When entered without the binding parameter, the summary status information is displayed for the specified interface.
ip <IPV6-ADDR>	Specifies the client IPv6 address.
mac <MAC-ADDR>	Specifies the client MAC address.
vlan <VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
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 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       Yes
```

Showing the summary status information for the specified interface in the binding database:

```
switch# show ipv6 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 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    : Yes
Hardware Error Reason : --

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    : Yes
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

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    : 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 ipv6 source-lockdown binding mac 00:50:56:96:e4:cf

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 : --
```

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

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   : Yes
Hardware Error Reason : --
```

Command History

Release	Modification
10.10	Command enabled on 8360 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	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.

Internet Control Message Protocol

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.

Type	ICMP messages
0	Echo Reply (Ping Reply, used with Type 8, Ping Request)
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request (Ping Request, used with Type 0, Ping Reply)
9	Router Advertisement (Used with Type 9)
10	Router Solicitation (Used with Type 10)
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request (Used with Type 14)
14	Timestamp Reply (Used with Type 13)
15	Information Request (obsolete) (Used with Type 16)
16	Information Reply (obsolete) (Used with Type 15)
17	Address Mask Request (Used with Type 17)
18	Address Mask Reply (Used with Type 18)

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

Release	Modification
10.07 or earlier	--

Command Information

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

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	Description
<PACKET-INTERVAL>	Specifies the ICMPv4/v6 packet interval in seconds. Default: 1 second. Range: 1-86400.

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

Release	Modification
10.8	Added the optional <PACKET-INTERVAL> parameter to the no form of the command.
10.07 or earlier	--

Command Information

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

ip icmp unreachable

```
ip icmp unreachable
no 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 packet. 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

Release	Modification
10.07 or earlier	--

Command Information

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

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 myhost1 3.3.3.3
switch(config)# exit
switch# show ip dns

```

```

VRF Name : default
Mode : static
Domain Name : switch.com
Name Server(s) : 1.1.1.1

```

Host configuration: Active

Host Name	Address
myhost1	3.3.3.3

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 vrf mainvrf
switch(config)# ip dns host myhost 3.3.3.3 vrf mainvrf
switch(config)# quit
switch# show ip dns vrf mainvrf

```

```

VRF Name : mainvrf
Mode : static
DNS Domain list : domain1.com, domain2.com, domain3.com
Name Server(s) : c::13

```

Host Name	Address
myhost	3.3.3.3

Fully Qualified Domain Name Resolver

The FQDN (Fully Qualified Domain Name) resolver is a subsystem within the DNS client that enables dynamic resolution of domain names to their corresponding IP addresses (IPv4 and/or IPv6). The task of name resolutions can be offloaded to **FQDN Resolver** by the applications. **FQDN Resolver** performs the name resolution and updates the status back to the interested applications. Periodic refresh for name resolution will be carried by this service.

With the command line interface it's possible to configure refresh Interval and force refresh for FQDN resolver entries. The following show commands are also available:

Show FQDN Resolver

Field	Description
Total FQDN	Total count of FQDN resolver entries in the database.
Refresh Time.	Refresh interval for FQDN resolver entries in seconds.
Source	Source of the resolution requests.
VRF	Virtual Routing and Forwarding instance.
FQDN	Fully Qualified Domain Name being resolved.
Status	Resolution status (resolved, unresolved or stale).
Addr-Family	Address family requested for resolution (IPv4, IPv6, or both).
ip-address	Resolved IP addresses.

Show FQDN Resolver Detail

Field	Description
Source	Source of the resolution requests.
VRF	Virtual Routing and Forwarding instance.
FQDN	Fully Qualified Domain Name being resolved.
Status	Resolution status (resolved, unresolved or stale).
Requested Address Family	Address family requested for resolution (IPv4, IPv6, or both).
IPv4 Addresses	Resolved IPv4 addresses.
IPv6 Addresses	Resolved IPv6 addresses.

Show FQDN Resolver Refresh Interval

Field	Description
Refresh Interval	Current refresh interval for FQDN resolvers in seconds.

DNS client commands

ip dns domain-list

```
ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
no ip 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.

Parameter	Description
<code>list <DOMAIN-NAME></code>	Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.
<code>vrf <VRF-NAME></code>	Specifies a VRF name. Default: default.

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

Release	Modification
10.07 or earlier	--

Command Information

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

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.

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

Release	Modification
10.07 or earlier	--

Command Information

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

ip dns fqdn-resolver force-refresh

```
ip dns fqdn-resolver force-refresh { fqdn WORD | source port-access | vrf WORD | status (resolved | stale | unresolved) }
```

Description

This command initiates a force refresh for FQDN resolver entry/entries. It can refresh all FQDN entries, or entries filtered by FQDN, source, VRF or status. If no FQDN is specified, all entries are refreshed.

Parameter	Description
fqdn	Refresh entries associated with specific FQDN. <i>Optional</i>
source	Refresh entries based on the source of the resolution request. <i>Optional</i>
vrf	Refresh entries associated with a specific VRF. <i>Optional</i>
status	Refresh entries associated with a specific resolution status. <i>Optional</i>



The **source** parameter is not supported in 8320, 8400 or 9300 switch series.

Examples

Refreshing all FQDN entries:

```
switch(config)# ip dns fqdn-resolver force-refresh
```

Refreshing a specific FQDN:

```
switch(config)# ip dns fqdn-resolver force-refresh fqdn www.example.com
```

Refreshing all FQDNs from specific source:

```
switch(config)# ip dns fqdn-resolver force-refresh source port-access
```

Refreshing FQDN in a specific VRF:

```
switch(config)# ip dns fqdn-resolver force-refresh fqdn www.example.com vrf red
```

Refreshing FQDN for a specific source and vrf:

```
switch(config)# ip dns fqdn-resolver force-refresh source classifier vrf red
```

When a FQDN entry is not found:

```
switch(config)# ip dns fqdn-resolver force-refresh fqdn www.nonexistent.com  
No FQDN entries matching the given criteria.
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

ip dns fqdn-resolver refresh-interval

```
[no] ip dns fqdn-resolver refresh-interval <3600-86400>
```

Description

Sets the refresh interval for FQDN resolvers. The interval specifies the time in seconds after which the FQDN resolver entries are refreshed. The valid range for the interval is between 3600 seconds (1 hour) to 86400 seconds (1 day). For each FQDN entry refresh timer is applicable from the time entry is installed.

The **no** form of this command removes the refresh interval and sets it back to default value which is 1 day.

Parameter	Description
<3600-86400>	Refresh interval in seconds (default: 86400 seconds). <i>Required</i>

Examples

This example sets a custom refresh interval.

```
switch(config)# ip dns fqdn-resolver refresh-interval 6000
switch(config)# ip dns fqdn-resolver refresh-interval 85400
```

Resetting the refresh interval to the default value.

```
switch(config)# no ip dns fqdn-resolver refresh-interval
```

Attempting to set an invalid interval:

```
switch(config)# ip dns fqdn-resolver refresh-interval 20
Invalid interval. Valid range: 3600-86400 seconds.
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

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

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.

Parameter	Description
host <HOST-NAME>	Specifies the name of a host. Length: 1 to 256 characters.
<IP-ADDR>	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.
vrf <VRF-NAME>	Specifies a VRF name. Default: default.

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

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
<IP-ADDR>	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.
vrf <VRF-NAME>	Specifies a VRF name. Default: default.

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

Release	Modification
10.07 or earlier	--

Command Information

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

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.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF for which to show information. If no VRF is defined, the default VRF is used.
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

Parameter

Description

VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

DNS client arbitration on the MGMT interface on a MGMT VRF can be updated via three different methods.

1. Using the **domain-name <name>** or **nameservers <servers>** commands in the command-line interface.
2. Using the **ip dns domain-name <DOMAIN-NAME> vrf MGMT** or **ip dns server-address <SERVER> vrf MGMT** commands in the command-line interface.
3. Using the **ip dhcp** command in the command-line interface (dynamic entries).

AOS-CX gives the following priority levels to the these three update methods.

- Priority 1 - standalone CLI configuration
- Priority 2 - static ip dns configuration
- Priority 3 - Dynamic config

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

Host Name      Address
-----
host2          2.2.2.2
host3          5.5.5.5
host3          c::12
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

```

```

Host Name      Address
-----
host2          2.2.2.3
host3          5.5.5.6
host3          c::13

```

```

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

```

```

Host Name      Address
-----
host3          5.5.5.5
host3          c::12

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	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 ip dns fqdn-resolver

```
show ip dns fqdn-resolver
```

Description

This command displays a summary table of all FQDN resolver entries, including the total count of FQDN entries, refresh time, source information, and a tabular display of all entries.

Examples

Show unresolved FQDN entries with ipv4 requested:

```
switch# show ip dns fqdn-resolver
Total FQDN: 1
Refresh Time: 86400 seconds

Source: port-access
VRF      FQDN                               Status      Addr-Family  ip-address
-----
--
default  host1.search.com                       unresolved  ipv4         -
```

Show resolved FQDN entries:

```
switch# show ip dns fqdn-resolver
Total FQDN: 2
Refresh Time: 7200 seconds

Source: port-access
VRF      FQDN                               Status      Addr-Family  ip-
address
-----
-----
default  www.example.com                       resolved    ipv4
192.168.1.1, 192.168.1.2
default  api.test.com                           resolved    ipv4         10.0.0.1
2001:db8::1, 2001:db8::2
long_vrf_na  a_very_long_fqdn_name                 resolved    ipv4         10.0.0.2
```

When no FQDN entries exist:

```
switch(config)# show ip dns fqdn-resolver
No FQDN resolver entries found.
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ip dns fqdn-resolver detail

```
show ip dns fqdn-resolver detail
```

```
{fqdn WORD | source port-access | vrf WORD | requested-address-family (ipv4 | ipv6 | both)}
```

Description

Displays detailed hierarchical information for FQDN resolver entries, including the FQDN, VRF, requested address family, resolved IPv4 and IPv6 addresses, resolution status, and remaining refresh timer. The command supports filtering by FQDN, source, VRF, and address family. If no filters are provided, all entries are displayed.

Examples

Show detailed view with unresolved entry:

```
switch# show ip dns fqdn-resolver detail
-----
Source: port-access
-----
FQDN: host1.search.com
VRF: default
Requested Address Family: ipv4
Status: unresolved
-----
```

Show detailed view with resolved entries:

```
switch# show ip dns fqdn-resolver detail
Source: port-access
  FQDN: www.example.com
  VRF: default
  Status: resolved
  Requested Address Family: both
    IPv4 Addresses:
      192.168.1.1
    IPv6 Addresses:
      2001:db8::1
      2001:db8::2
-----
FQDN: www.hpe.com
VRF: default
Status: resolved
Requested Address Family: ipv4
  IPv4 Addresses:
    10.0.0.1
-----
```

Show detailed view with filter:

```
switch# show ip dns fqdn-resolver detail fqdn www.example.com
Source: port-access
  FQDN: www.example.com
  VRF: default
  Status: resolved
  Requested Address Family: both
    IPv4 Addresses:
      192.168.1.1
      192.168.1.2
    IPv6 Addresses:
```

```
2001:db8::1
2001:db8::2
-----
```

Show detailed view when no entries exist:

```
switch# show ip dns fqdn-resolver detail
No FQDN resolver entries found
```



The **source** parameter is not supported in 8320, 8400 or 9300 switch series.



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ip dns fqdn-resolver refresh-interval

```
show ip dns fqdn-resolver refresh-interval
```

Description

Displays the current refresh interval for FQDN resolvers.

Examples

Show current refresh interval (default):

```
switch# show ip dns fqdn-resolver refresh-interval
Refresh Interval: 86400 seconds
```

Show refresh interval after configuration change:

```
switch(config)# ip dns fqdn-resolver refresh-interval 7200
switch(config)# exit
switch# show ip dns fqdn-resolver refresh-interval
Refresh Interval: 7200 seconds
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

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.

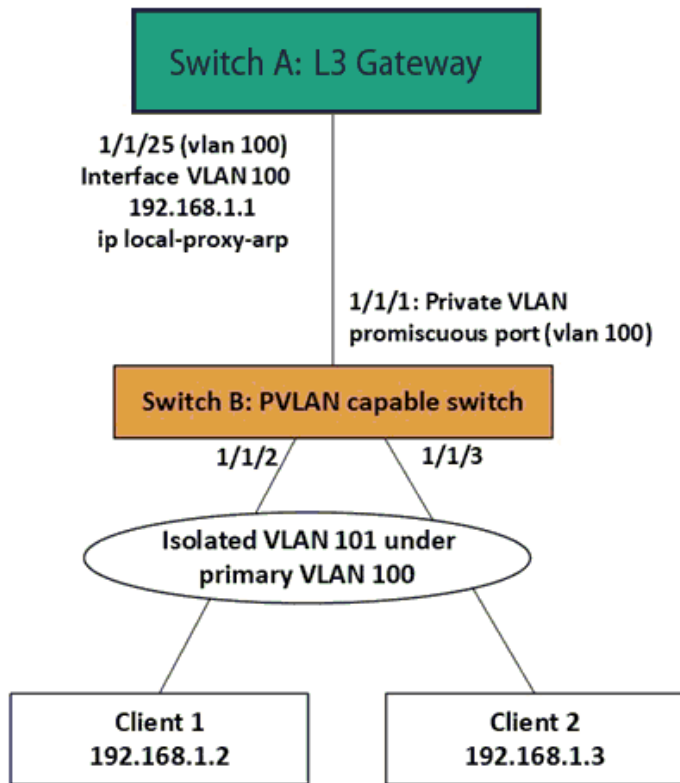
Proxy ARP is supported on L3 physical and VLAN interfaces. It is disabled by default. To enable proxy ARP, routing must be enabled on the interface.

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 and is disabled by default. Routing must be enabled on the interface to enable local proxy ARP.

Local proxy ARP can be used along with private VLAN deployments to allow layer 3 communication where clients are isolated at layer 2.

Figure 1 Local Proxy ARP Use Case Example



The local proxy ARP feature is to be configured only if there is a need for the clients to communicate while still maintaining layer 2 isolation.

The following steps configure the local ARP proxy deployment shown in [Figure 1, Local Proxy ARP Use Case Example](#).

Step 1: Configuring private VLAN in switch B

- A. Configure the primary and isolated VLAN first

```
PVLAN-Switch(config)# vlan 100
PVLAN-Switch(config-vlan-100)# private-vlan primary
PVLAN-Switch(config-vlan-100)# vlan 101
PVLAN-Switch(config-vlan-101)# private-vlan isolated primary-vlan 100
```

- B. Configure the PVLAN secondary ports to which clients are connected

```
PVLAN-Switch(config)# interface 1/1/2,1/1/3
PVLAN-Switch(config-if-<1/1/1,1/1/2>)# vlan trunk allowed 101
PVLAN-Switch(config-if-<1/1/1,1/1/2>)# private-vlan port-type secondary
```

- C. Configure the PVLAN promiscuous port on the uplink which connects to the L3 gateway

```
PVLAN-Switch(config)# interface 1/1/1
PVLAN-Switch(config-if)# vlan trunk allowed 100
```

```
PVLAN-Switch(config-if) # private-vlan port-type promiscuous
PVLAN-Switch(config-if) # no shutdown
```

For details about private VLAN configuration, refer to the *AOS-CX Layer-2 Bridging guide*.

Step 2: Configuring L3 gateway in switch A

```
L3-GW(config) # vlan 100
L3-GW(config-vlan-100) # exit
L3-GW(config) # interface 1/1/25
L3-GW(config-if) # vlan trunk allowed 100
L3-GW(config-if) # no shutdown
L3-GW(config-if) # exit
L3-GW(config) # interface vlan 100
L3-GW(config-if-vlan) # ip address 192.168.1.1/24
```

Now the clients will be able to ping the gateway IP; but will not be able to communicate with each other due to the isolation enforced with private VLAN. As expected, the ping from client 1 to client 2 will fail in the above example, although the clients are in the same subnet.

Step 3: Configuring local proxy ARP in switch A

If local proxy ARP is enabled in the L3 gateway, the L3 gateway responds to ARP requests for addresses in the same subnet. In other words, the L3 gateway will be doing proxy for ARP resolution.

```
L3-GW(config) # no ip icmp redirect
L3-GW(config) # interface vlan 100
L3-GW(config-if-vlan) # ip local-proxy-arp
```

With this, the L3 communication will be enabled between client 1 and client 2. Now the ping from client 1 to client 2 will be successful in the above example. The ARP table in client 1 will be populated with the MAC of L3 gateway; not the MAC of client 2. Similar ARP table entry for client 2 as well. In other words, the L3 gateway is doing proxy for ARP resolution for the local network where clients are isolated at layer 2.

Dynamic ARP inspection

Dynamic arp inspection is provided as a mechanism for making ARP more secure.



Dynamic ARP inspection is available on the 8325/8325H/8325P and 10000 Switch Series.



On the 10000 Switch Series, Dynamic ARP Inspection and PSM / Distributed Services (DSS) are mutually exclusive. If both features are enabled, unexpected behavior may occur.



-
- Dynamic ARP inspection over VXLAN is supported on the HPE Aruba Networking 8325 and 10000 Switch Series.
 - ARP suppression and Dynamic ARP inspection are mutually exclusive at the device level, only one of the features can be configured on a device.
 - VXLAN tunnel is considered as trusted for Dynamic ARP inspection by default.
-

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.

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 and the DHCP snooping table is 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

This example configures proxy ARP on interface **1/1/2**

```
switch# config
switch(config)# interface 1/1/2
switch(config-if)# ip proxy-arp
```

This example configures proxy ARP on interface VLAN **30**.

```
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

This example configures local proxy ARP on interface **1/1/2**

```
switch# config
switch(config)# interface 1/1/2
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
```

Configuring dynamic ARP inspection over VXLAN overlay

Applicable to the 8100, 8325, 8360, 10000 Switch Series

Procedure

1. Configure VXLAN overlay setup to establish the VxLAN tunnel. For more information, see *AOS-CX VXLAN EVPN Guide*.
2. Validate whether the tunnel is established between the VTEPS (either static or EVPN) with the command **show interface vxlan vteps**. The status of the tunnel should be operational in order to forward the packets.
3. Configure ARP inspection in the VLAN context with the command **arp inspection**.

4. Configure the port as trusted or untrusted with the command **arp inspection trust**. If the connected port is VXLAN tunnel, then this step can be ignored. This is because the VXLAN tunnel is always considered as trusted.
5. Validate the ARP inspection configuration with the command **show arp inspection**.

ARP commands

arp inspection

arp inspection

Description

Enables Dynamic ARP inspection on the current VLAN, which means that ARP packets received from untrusted interfaces are discarded if they have an Invalid IP-to-MAC address binding.

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

Release	Modification
10.12	Command introduced on the 8100 and 8360 Switch Series
10.11.1000	Command introduced on the 8325 Switch Series
10.11.1000	Command introduced on the 10000 Switch Series

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 10000	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

arp inspection trust

```
arp inspection trust
no arp inspection trust
```

Description

Configures 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

Release	Modification
10.11.1000	Command introduced on the 8325 Switch Series
10.11.1000	Command introduced on the 10000 Switch Series

Command Information

Platforms	Command context	Authority
8325 8325H 8325P 10000	config-if	Administrators or local user group members with execution rights for this command.

arp ip

```
arp ip <IP_ADDR> mac <MAC_ADDR>
no arp ip <IP_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.

Parameter	Description
ip <IP-ADDR>	Specifies the IP address of the neighbor or the virtual IP address of the cluster in IP format (x.x.x.x), where x is a decimal number from 0 to 255. . Range: 4096 to 131072. Default: 131072.
mac <MAC-ADDR>	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.

Example

Configuring a static ARP entry on a interface VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# arp ip 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 ip 2.2.2.2 mac 01:00:5e:00:00:01
```

Command History

Release	Modification
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4 parameter is deprecated.
10.07 or earlier	--

Command Information

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

arp process-grat-arp

```
arp process-grat-arp
no arp process-grat-arp
```

Description

Enables the processing of gratuitous ARP packets on the individual port or group of L3 ports together. By default, the gratuitous ARP processing is enabled. When gratuitous ARP (GARP) processing is enabled, a switch that is advertising any changes in its MAC through the GARP will reflect in the neighbor table of the switch. However, the switch will not be able to learn the neighbor through the GARP. This configuration is applicable only on L3 interfaces such as ROPs, subinterfaces, and SVIs. The **no** form of this command disables the processing of gratuitous ARP packets.

Example

Enabling the processing of gratuitous ARP packets on the interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# arp process-grat-arp
```

Enabling the processing of gratuitous ARP packets on interfaces **1/1/1** to **1/1/5**:

```
switch(config)# interface 1/1/1-1/1/5
switch(config-if<1/1/1-1/1/5>)# no shutdown
switch(config-if<1/1/1-1/1/5>)# arp process-grat-arp
```

Enabling the processing of gratuitous ARP packets on sub-interface **1/1/1.10**:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# no shutdown
switch(config-subif)# arp process-grat-arp
```

Disabling the processing of gratuitous ARP packets on VLANs **2 to 100**:

```
switch(config)# interface vlan 2-100
switch(config-if-vlan<2-100>)# no shutdown
switch(config-if-vlan<2-100>)# no arp process-grat-arp
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-if-vlan config-subif	Administrators or local user group members with execution rights for this command.

clear arp

```
clear arp
port <PORT-ID> [ip <A.B.C.D>|all] |[ipv6 <X:X::X:X>|all] vla
vrf [all-vrfs|{<VRF-NAME> [ip <A.B.C.D>] |[ipv6 <X:X::X:X>]}]
```

Description

Clears IPv4 and IPv6 neighbor entries from the ARP table. If you do not specify any VRF or port parameters, ARP table entries are cleared for the **default** VRF.

Parameter	Description
port <PORT-ID>	Specifies a port on the switch. For example: 1/1/1 .
ip <A.B.C.D> all]	(Optional) Include an IP address to clear neighbor entries for that specific address, or use the all parameter to clear entries for all IP addresses.

Parameter	Description
<code>ipv6 <X:X::X:X> all</code>	(Optional) Include an IPv6 address to clear neighbor entries for that specific address, or use the all parameter to clear entries for all IPv6 addresses.
<code>vrf</code>	Clears IPv4 and IPv6 neighbor entries for the specified VRF or for all VRFs. If no VRF is specified the default VRF is cleared.
<code>all-vrfs</code>	Clear neighbor entries for all VRFs
<code><VRF-NAME></code>	Clear neighbor entries for the specified VRF.
<code>ip <A.B.C.D></code>	(Optional) Include an IP address to clear just the neighbor entries for the specified IP address.
<code>ipv6 <X:X::X:</code>	(Optional) Include an IPv6 address to clear the neighbor entries for the specified IPv6 address.

Examples

Clearing all IPv4 and IPv6 neighbor ARP entries for the default VRF:

```
switch# clear arp
```

Clearing all ARP neighbor entries for a port:

```
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

Release	Modification
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4 parameter is deprecated.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

debug arp-security

```
debug arp-security <LOG-CATEGORY> [severity <LEVEL>]  
no debug arp-security [<LOG-CATEGORY>] [severity <LEVEL>]
```

Description

Enables ARP security debug logs. If <SEVERITY> is omitted, all severities are logged.

The **no** form of this command disables ARP security debug logs.

Parameter	Description
<code><LOG-CATEGORY></code>	Selects the ARP security debug log category. Available categories are: <ul style="list-style-type: none">▪ all: Selects all ARP security debug log categories.▪ config: Selects the ARP security config debug log category.▪ inspection: Selects the ARP security inspection debug log category.▪ packet: Selects the ARP security packet debug log category.
<code>severity <LEVEL></code>	Specifies how to filter the ARP security debug logging by setting the minimum severity level for which debug logging will be performed. The selected severity level and all severities above (more severe) will be included in the logging. <ul style="list-style-type: none">▪ emerg: Sets ARP security debug log filtering to Emergency only.▪ alert: Sets ARP security debug log filtering to Alert and above.▪ critical: Sets ARP security debug log filtering to Critical and above.▪ error: Sets ARP security debug log filtering to Error and above.▪ warning: Sets ARP security debug log filtering to Warning and above.▪ notice: Sets ARP security debug log filtering to Notice and above.▪ info: Sets ARP security debug log filtering to Info and above.▪ debug: Sets ARP security debug log filtering to all severities.

Examples

Enable ARP security debug logging for all categories and all severities:

```
switch# debug arp-security all
```

Enable ARP security config debug log for severity level Error and above:

```
switch# debug arp-security config severity error
```

Enable ARP security inspection debug log for severity level Notice and above:

```
switch# debug arp-security inspection severity notice
```

Enable ARP security debug packet for severity level Critical and above:

```
switch# debug arp-security packet severity critical
```

Enable ARP security debug logging for all categories and severity level Alert and above:

```
switch# debug arp-security all severity alert
```

Disable ARP security debug logging:

```
switch# no debug arp-security
```

Command History

Release	Modification
10.11.1000	Command introduced on 8325 Switch Series
10.11.1000	Command introduced on 10000 Switch Series

Command Information

Platforms	Command context	Authority
8325 8325H 8325P 10000	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.

ip local-proxy-arp

```
ip local-proxy-arp [uplink-passthrough]  
no ip local-proxy-arp [uplink-passthrough]
```

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. If the optional uplink-passthrough parameter is specified for an interface on a 10000 switch series, the local proxy ARP configuration will only proxy for non-uplink ports.

The **no ip local-proxy-arp** command disables local proxy ARP on the specified interface. The **no ip local-proxy-arp uplink-passthrough** command disables local proxy ARP uplink-passthrough for the specified interface, while allowing local proxy ARP to remain configured on the interface.

Parameter	Description
uplink-passthrough	(For 10000 Switch series only) Enables local proxy ARP passthrough to uplink members. NOTE: When enabling ip local-proxy-arp uplink-passthrough , ip local-proxy-arp will be implicitly enabled.

Examples

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 on interface **1/1/1**.

```
switch# interface 1/1/1
switch(config-if)# no ip local-proxy-arp
```

Enable local proxy ARP uplink-passthrough on a VLAN interface on a 10000 Switch series.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip local-proxy-arp uplink-passthrough
switch(config-if-vlan)# show running-config current-context
interface vlan 2
ip local-proxy-arp
ip local-proxy-arp uplink-passthrough
```

Command History

Release	Modification
10.16	Support added for the 6200 Switch Series.
10.15.1010	The uplink-passthrough parameter was introduced on 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8325	config-if	Administrators or local user group members with execution

Platforms	Command context	Authority
8325H 8325P 8360 9300 9300S 10000	config-if-vlan	rights for this command.

ip local-proxy-arp exclude <ip-address>

```
ip local-proxy-arp exclude <ip-address>
no ip local-proxy-arp exclude <ip-address>
```

Description

Enables exemption of a specific IP address from local proxy ARP for the specified interface. This allows specified IP addresses to bypass local proxy ARP processing on the interface.

The maximum IP addresses can be exempted from Local Proxy ARP per interface are 256.

The maximum IP addresses can be exempted from Local proxy ARP across all interfaces are 256.

The **no ip local-proxy-arp exclude <ip-address>** disables exemption of a specific IP address from local proxy ARP for the specified interface, while local proxy ARP remains configured on the interface. This allows specified IP addresses to be processed by local proxy ARP on the interface.

Parameter	Description
ip-address	IP address to exclude from local proxy ARP. In the no form, is the IP address to remove from local proxy ARP exemption. <i>Required</i>

Examples

Configuring local proxy ARP IP exemption on a L3 physical interface:

```
switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# ip local-proxy-arp exclude 192.168.1.1

switch(config-if-vlan)# show running-config current-context
interface 1/1/1
    no shutdown
    ip local-proxy-arp exclude 192.168.1.1
```

Configuring local proxy ARP IP exemption on a VLAN interface:

```
switch# configure terminal
switch(config)# interface vlan 2
switch(config-if-vlan)# ip local-proxy-arp exclude 192.168.1.1

switch(config-if-vlan)# show running-config current-context
interface vlan 2
    ip local-proxy-arp exclude 192.168.1.1
```

Configuring local proxy ARP IP exemption on a L3 lag interface:

```
switch# configure terminal
switch(config)# interface lag 10
switch(config-lag-if)# ip local-proxy-arp exclude 192.168.1.1

switch(config-lag-if)# show running-config current-context
interface lag 10
    ip local-proxy-arp exclude 192.168.1.1
```

Configuring local proxy ARP IP exemption on a sub interface:

```
switch# configure terminal
switch(config)# interface 1/1/1.10
switch(config-if-subif)# ip local-proxy-arp exclude 192.168.1.1

switch(config-if-vlan)# show running-config current-context
interface 1/1/1.10
    ip local-proxy-arp exclude 192.168.1.1
```

Removing local proxy ARP IP exemption on a L3 physical interface:

```
switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# no ip local-proxy-arp exclude 192.168.1.1

switch(config-if-vlan)# show running-config current-context
interface 1/1/1
    no shutdown
```

Removing local proxy ARP IP exemption on a VLAN interface.

```
switch# configure terminal
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip local-proxy-arp exclude 192.168.1.1
```

Removing local proxy ARP IP exemption on a sub interface.

```
switch# configure terminal
switch(config)# interface 1/1/1.1
switch(config-if-subif)# no ip local-proxy-arp exclude 192.168.1.1
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.
10000	config-if-vlan	
8325	config-lag-if	
8325H	config-if-subif	
8100		

ipv6 local-proxy-nd

```
ipv6 local-proxy-nd [uplink-passthrough]
no ipv6 local-proxy-nd [uplink-passthrough]
```

Description

Enables local proxy ND for the specified interface.

The **no ipv6 local-proxy-nd** command disables local proxy ND for the specified interface. The **no ipv6 local-proxy-nd uplink-passthrough** series command disables local proxy ARP uplink-passthrough for the specified interface on 10000 Switch series, while local proxy ARP remains configured on the interface.

Parameter	Description
uplink-passthrough	<p>(For 10000 Switch series only) Change local-proxy-nd into the uplink-passthrough state to segment the network. uplink-passthrough will change the local-proxy-nd behavior to only proxy for the downstream ports. This is only available when configuring a VLAN interface.</p> <p>NOTE: When enabling ipv6 local-proxy-nd uplink-passthrough, ip local-proxy-arp will be implicitly enabled. This will apply local proxy ARP to all VLAN members.</p>

Usage

Before enabling local proxy ND, disable Internet Control Message Protocol (ICMP) redirect messages. Disabling the ICMP redirect ensures that hosts don't communicate through other gateways which could possibly have better routes and thereby skip the proxy.

Example

Enable local proxy ND on a L3 physical interface.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 local-proxy-nd
```

Enable local proxy ND on a VLAN interface.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 local-proxy-nd
```

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 local-proxy-nd
```

Enable local proxy ND uplink-passthrough on a VLAN interface on a 1000 Switch series.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 local-proxy-nd uplink-passthrough
switch(config-if-vlan)# show running-config current-context
interface vlan 2
ip local-proxy-nd
ip local-proxy-nd uplink-passthrough
```

Disable local proxy ND for the specified interface. This command will also disable the uplink-passthrough option if it is configured.

```
switch(config-if)# no ipv6 local-proxy-nd
```

Disable local proxy ND uplink-passthrough on a VLAN interface on a 10000 Switch series and unsegment the network. This command will apply local proxy ND to all VLAN members.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ipv6 local-proxy-nd uplink-passthrough
```

Command History

Release	Modification
10.15.1010	The uplink-passthrough parameter was introduced on 10000 Switch series.
10.07 or earlier	--

Command Information

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

ipv6 local-proxy-nd exclude <ipv6-address>

```
ipv6 local-proxy-nd exclude <ipv6-address>
no ipv6 local-proxy-nd exclude <ipv6-address>
```

Description

Enables IP exemption for local proxy ND for the specified interface and IPv6 address. When configured, the switch will not respond to neighbor solicitation (NS) messages for the specified IPv6 address.

Maximum IPv6 addresses can be exempted from Local Proxy ND per interface are 256.

Maximum IPv6 addresses can be exempted from Local proxy ND across all interfaces are 256.

The **no ipv6 local-proxy-nd exclude <ipv6-address>** disables IP exemption for local proxy ND for the specified interface and IPv6 address, while local proxy ND remains configured on the interface. After executing this command, the switch will respond to neighbor solicitation (NS) messages for the specified IPv6 address.

Parameter	Description
ipv6-address	IPv6 address to exclude from local proxy ND, In the no form, is the IPv6 address to remove from exclusion, <i>Required</i>

Examples

Configuring local proxy ND IP exemption on a L3 physical interface:

```
switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# ipv6 local-proxy-nd exclude 2001:db8::1

switch(config-if)# show running-config current-context
interface 1/1/1
    ipv6 local-proxy-nd exclude 2001:db8::1
```

Configuring local proxy ND IP exemption on a VLAN interface:

```
switch# configure terminal
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 local-proxy-nd exclude 2001:db8::1

switch(config-if-vlan)# show running-config current-context
interface vlan 2
    ipv6 local-proxy-nd exclude 2001:db8::1
```

Configuring local proxy ND IP exemption on a L3 lag interface:

```
switch# configure terminal
switch(config)# interface lag 10
switch(config-lag-if)# ipv6 local-proxy-nd exclude 2001:db8::1

switch(config-lag-if)# show running-config current-context
interface lag 10
    ipv6 local-proxy-nd exclude 2001:db8::1
```

Configuring local proxy ND IP exemption on a sub interface:

```
switch# configure terminal
switch(config)# interface 1/1/1.10
switch(config-if-subif)# ipv6 local-proxy-nd exclude 2001:db8::1

switch(config-if-subif)# show running-config current-context
interface 1/1/1.10
    ipv6 local-proxy-nd exclude 2001:db8::1
```

Disabling local proxy ND IP exemption on a L3 physical interface:

```

switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 local-proxy-nd exclude 2001:db8::1

switch(config-if)# show running-config current-context
interface 1/1/1
no shutdown

```

Disabling local proxy ND IP exemption on a VLAN interface:

```

switch# configure terminal
switch(config)# interface vlan 2
switch(config-if-vlan)# no ipv6 local-proxy-nd exclude 2001:db8::1

```

Disabling local proxy ND IP exemption on a sub interface.

```

switch# configure terminal
switch(config)# interface 1/1/1.10
switch(config-if-subif)# no ipv6 local-proxy-nd exclude 2001:db8::1

```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.
10000	config-if-vlan	
8325	config-lag-if	
8325H	config-if-subif	
8100		

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:

```
switch# interface vlan 3
switch(config-if-vlan)# ip proxy-arp
```

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

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-if-vlan config-lag-vlan	Administrators or local user group members with execution rights for this command.

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
<IPV6-ADDR>>	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.
mac <MAC-ADDR>>	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.

Example

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

Release	Modification
10.07 or earlier	--

Command Information

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

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
IPv4 Address      MAC                Port                Physical Port      State
-----
192.168.1.2      00:50:56:96:7b:e0  vlan10             1/1/29             stale
192.168.1.3      00:50:56:96:7b:ac  vlan10             1/1/1              reachable

Total Number Of ARP Entries Listed- 2.
-----
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show arp inspection interface

```
show arp inspection interface [<IFNAME>] [vlan <VLAN-ID>] [vsx-peer]
```

Description

Shows the current configuration of dynamic ARP inspection on an interface.

Parameter	Description
<IFNAME>	Specifies the interface.
<VLAN-ID>	Specifies the VLAN ID. Range: 1 to 4094.
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 current configuration of dynamic ARP inspection on all interfaces:

```
switch# show arp inspection interface
```

```
-----  
Interface          Trust-State  
-----  
1/1/1              Untrusted  
-----
```

Showing current configuration of dynamic ARP inspection on all interfaces with VSX peer:

```
switch# show arp inspection interface vsx-peer
```

```
-----  
Interface          Trust-State  
-----  
1/1/1              Untrusted  
lag100             Trusted  
-----
```

Showing current configuration of dynamic ARP inspection on a particular interface:

```
switch# show arp inspection interface 1/1/1
```

```
-----  
Interface          Trust-State  
-----  
1/1/1              Untrusted  
-----
```

Showing current configuration of dynamic ARP inspection on interface VLAN 2:

```
switch# show arp inspection interface vlan 2
```

```
-----  
Interface          Trust-State  
-----  
vlan2              Trusted  
-----
```

Command History

Release	Modification
10.12	Command introduced on the 8100 and 8360 Switch Series
10.11.1000	Command introduced on the 8325 Switch Series
10.11.1000	Command introduced on the 10000 Switch Series

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 10000	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 arp inspection statistics

```
show arp inspection statistics vlan [<VLAN-ID>] [vsx-peer]
```

Description

Shows statistics about forwarded and dropped ARP packets. When <VLAN-ID> is not specified, information is shown for all configured VLANs.

Parameter	Description
<VLAN-ID>	Specifies the VLAN ID or range of IDs separated by a dash "-". Range: 1 to 4094.

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

Showing ARP packet statistics for a range of VLANs:

```
switch# show arp inspection statistics vlan 1-100
```

VLAN	Name	Forwarded	Dropped
1	DEFAULT_VLAN_1	0	0

Showing ARP packet statistics for VLANs with VSX peer:

```
switch# show arp inspection statistics vlan vsx-peer
```

VLAN	Name	Forwarded	Dropped
1	DEFAULT_VLAN_1	0	0
200	VLAN200	0	0

Command History

Release	Modification
10.12	Command introduced on the 8100 and 8360 Switch Series
10.11.1000	Command introduced on the 8325 Switch Series
10.11.1000	Command introduced on the 10000 Switch Series

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 10000	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 arp inspection vlan

```
show arp inspection vlan [<VLAN-ID>] [vsx-peer]
```

Description

Shows the current configuration of dynamic ARP inspection on a VLAN. When <VLAN-ID> is not specified, information is shown for all configured VLANs.

Parameter	Description
<VLAN-ID>	Specifies the VLAN ID or range of IDs separated by a dash "-". Range: 1 to 4094.
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 dynamic ARP configuration for all VLANs:

```
switch# show arp inspection vlan
-----
VLAN   Name                ARP Inspection
-----
1      DEFAULT_VLAN_1     -
100    VLAN100             -
200    VLAN200             Enabled
-----
```

Showing dynamic ARP configuration for a particular VLAN:

```
switch# show arp inspection vlan 1
-----
VLAN   Name                ARP Inspection
-----
1      DEFAULT_VLAN_1     -
-----
```

Showing dynamic ARP configuration for VLANs with VSX peer:

```
switch# show arp inspection vlan vsx-peer
-----
VLAN   Name                ARP Inspection
-----
1      DEFAULT_VLAN_1     -
-----
```

Command History

Release	Modification
10.12	Command introduced on the 8100 and 8360 Switch Series

Release	Modification
10.11.1000	Command introduced on the 8325 Switch Series
10.11.1000	Command introduced on the 10000 Switch Series

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 10000	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 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.

Parameter	Description
all	Shows the ARP cache entries for all VRF (Virtual Router Forwarding) instances.
failed	Shows the ARP cache entries that are in <code>failed</code> state. The neighbor might have been deleted.
incomplete	Shows the ARP cache entries that are in <code>incomplete</code> 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.
permanent	Shows the ARP cache entries that are in <code>permanent</code> state. ARP entries that are in a permanent state can be removed by administrative action only.
reachable	Shows the ARP cache entries that are in <code>reachable</code> state, meaning that the neighbor is known to have been reachable recently.
stale	Shows ARP cache entries that are in <code>stale</code> state. ARP cache entries are in the <code>stale</code> 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.
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 arp state failed
```

IPv4 Address	MAC	Port	Physical Port	State
192.168.1.4		vlan10		failed

Command History

Release	Modification
10.07 or earlier	--

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 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.

Parameter	Description
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.
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 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        32489

vsx-primary# show arp summary vsx-peer
ARP Entry's State          IPv4          IPv6
-----
Number of Reachable ARP entries  25858        32168
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        32488
-----

```

Command History

Release	Modification
10.07 or earlier	--

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 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.

Parameter	Description
<INTERFACE>	Specifies a physical port, VLAN, or LAG on the switch. For physical ports, use the format <code>member/slot/port</code> (for example, 1/3/1).
<code>vsx-peer</code>	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

Release	Modification
10.07 or earlier	--

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 arp vlan

```
show arp vlan [all | <VLAN-ID>]
```

Description

Shows IPv4 neighbors learned on all L2 VLAN interfaces or for a specific VLAN. The command has the following limitations:

1. MAC-IP bindings are learned via L2 VLANs and are deleted when an SVI is created for the same VLAN.
2. The MAC-IP is learned based on the incoming packets. The source of truth is ARP and ND packets.
3. DAD ARP and DAD ND packets cannot be used to learn MAC-IP.
4. Multi-homing is not supported. VSX MLAG connected hosts learning is supported.
5. Migrating to **arp-suppression-extended** from **arp-suppression** will not have any functionality impact.

The **arp-suppression-extended** command provides all of the existing functionality of the **arp-suppression** command as well as ARP suppression support on L2 VLANs.

6. L2 Neighbor learning is based solely on stolen ARP packets. There is a possibility that ARP packets may be directly forwarded if the L2 VTEPs have not yet programmed the CPU RX rule or added the VLAN to the list of interfaces for stealing, following some internal events (e.g, VLAN shut/no-shut). As a result, a remote L3 VTEP will learn the remote host as reachable by performing flood and learn, which is expected. After the BR timers expire, L3 VTEPs begin probing by sending ARP requests. The requests prompt the L2 VTEPs to learn about the connected hosts from the ARP reply packets and then send RT2 to the other VTEPs.

Parameter	Description
all	Specifies all L2 VLANs.
<VLAN-ID>	Specifies a particular VLAN.

Examples

Showing ARP entries for all L2 VLANs:

```
switch# show arp vlan all

IPv4 Address      MAC                Vlan      Source
-----
10.10.10.2        00:50:56:bd:27:bc  vlan10    dynamic
10.0.0.2          aa:00:00:00:00:01  vlan20    evpn

Total Number Of ARP Entries Listed: 2.
-----

switch# show arp vlan 10

IPv4 Address      MAC                Vlan      Source
-----
10.10.10.2        00:50:56:bd:27:bc  vlan10    dynamic

Total Number Of ARP Entries Listed: 1.
-----
```

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
8325 10000	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 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.

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

Showing ARP entries for VRF **vrf1**.

```
switch# show arp vrf vrf1

IPv4 Address      MAC                Port      Physical Port      State
VRF
-----
100.1.250.50     00:50:56:8d:44:13  vlan1001  1/1/2
reachable vrf1
100.2.250.60     00:50:56:8d:45:63  vlan1002  vxlan1 (1920:1680:1:1::2)
permanent vrf1

Total Number Of ARP Entries Listed: 2.
-----
```

This example from a different network shows 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

Total Number Of ARP Entries Listed: 2.
-----
```

Command History

Release	Modification
10.07 or earlier	--

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 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
<code>all-vrfs</code>	Specifies all VRFs.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Length: 1 to 32 alphanumeric characters.
<code>vsx-peer</code>	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.
```

```
switch# show ipv6 neighbors vrf vrf1
IPv6 Address          MAC                Port
Physical Port  State  VRF
-----
1000:2:1:1::250:60  00:50:56:8d:45:63  vlan1002  vxlan1 (1920:1680:1:1::2)
permanent vrf1
1000:1:1:1::250:50  00:50:56:8d:44:13  vlan1001  1/1/2
reachable vrf1
```

Total Number Of IPv6 Neighbors Entries Listed: 2.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

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.

Parameter	Description
all	Shows all ARP cache entries.
failed	Shows ARP cache entries that are in <code>failed</code> state. The neighbor might have been deleted. Set the neighbor to be unreachable.
incomplete	Shows ARP cache entries that are in <code>incomplete</code> 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.
permanent	Shows ARP cache entries that are in <code>permanent</code> state.
reachable	Shows ARP cache entries that are in <code>reachable</code> state, meaning that the neighbor is known to have been reachable recently.
stale	Shows ARP cache entries that are in <code>stale</code> state. ARP cache entries are in the <code>stale</code> 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.
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

```
switch# show ipv6 neighbors state all
```

IPv6 Address	MAC	Port	Physical Port	State
100::2	48:0f:cf:af:f1:cc	lag1	lag1	reachable
300::3	48:0f:cf:af:33:be	vlan3	1/4/20	reachable
fe80::4a0f:cfff:feaf:f1cc	48:0f:cf:af:f1:cc	lag1	lag1	reachable
200::3	48:0f:cf:af:33:be	1/4/11	1/4/11	reachable
fe80::4a0f:cfff:feaf:33be	48:0f:cf:af:33:be	vlan3	1/4/20	reachable

Total Number Of IPv6 Neighbors Entries Listed- 5.

Command History

Release	Modification
10.07 or earlier	--

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 neighbors vlan

```
show ipv6 neighbors vlan [all | <VLAN-ID>]
```

Description

Shows IPv6 neighbors learned on all L2 VLAN interfaces or for a specific VLAN. The command has the following limitations:

1. MAC-IP bindings are learned via L2 VLANs and are deleted when an SVI is created for the same VLAN.
2. The MAC-IP is learned based on the incoming packets. The source of truth is ARP and ND packets.
3. DAD ARP and DAD ND packets cannot be used to learn MAC-IP.
4. Single homed devices are supported. Multi-homing is not supported.
5. L2 Neighbor learning is based solely on stolen ND packets. There is a possibility that ND packets may be directly forwarded if the L2 VTEPs have not yet programmed the CPU RX rule or added the VLAN to the list of interfaces for stealing following some internal events. An L3 VTEP may learn the remote host as reachable by performing NS and NA, which is expected. After the BR timers expire, L3 VTEPs begin probing by sending NS requests, which prompts the L2 VTEPs to learn about the connected hosts from the NA reply packets and then send RT2 to the other VTEPs.

Parameter	Description
all	Specifies all L2 VLANs.
<VLAN-ID>	Specifies a particular VLAN.

Examples

Showing IPv6 neighbors for all VLANs:

```

switch# show ipv6 neighbors vlan all

IPv6 Address                               MAC                               Vlan    Source
-----
--
10::2                                       00:50:56:bd:27:bc               vlan10
dynamic
2002:1::2                                   aa:00:00:00:00:02               vlan20  evpn

Total Number Of IPv6 Neighbors Entries Listed: 2.
-----
--

switch# show ipv6 neighbors vlan 10

IPv6 Address                               MAC                               Vlan    Source
-----
--
10::2                                       00:50:56:bd:27:bc               vlan10
dynamic

Total Number Of IPv6 Neighbors Entries Listed: 1.
-----
--

```

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
8325 10000	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 tech arp-security

show tech arp-security

Description

Shows the output of these three commands:

- `show arp inspection statistics vlan`
- `show arp inspection vlan`
- `show arp inspection interface`

Examples

Showing the output of the three ARP security show commands:

```
switch(config-if)# show tech arp-security
=====
Show Tech executed on Mon Nov 28 09:53:54 2019
=====
[Begin] Feature arp-security
=====

*****
Command : show arp inspection statistics vlan
*****

-----
VLAN   Name                Forwarded    Dropped
-----
1      DEFAULT_VLAN_1     0           0
200    VLAN200             0           0
-----

*****
Command : show arp inspection vlan
*****

-----
VLAN   Name                ARP-Inspection
-----
1      DEFAULT_VLAN_1     -
200    VLAN200             Enabled
-----

*****
Command : show arp inspection interface
*****

-----
Interface    Trust-State
-----
1/1/1        Untrusted
lag100       Trusted
-----

=====
[End] Feature arp-security
=====

=====
Show Tech commands executed successfully
=====
```

Command History

Release	Modification
10.11.1000	Command introduced on the 8325 Switch Series
10.11.1000	Command introduced on the 10000 Switch Series

Command Information

Platforms	Command context	Authority
8325 8325H 8325P 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

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 ip mac

```
arp ip <IP-ADDR> mac <MAC-ADDR>
no arp ip <IP-ADDR> mac <MAC-ADDR>
```

Description

Configures static ARP multicast on the interface.

The **no** form of this command removes the static ARP multicast configuration.

Parameter	Description
<IP-ADDR>	Specifies cluster's virtual IPv4 address.
<MAC-ADDR>	Specifies multicast MAC address in IANA format (xx:xx:xx:xx:xx:xx) and non IANA format (xxxx.xxxx.xxxx).

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 ip 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.

On 8320, 8325/8325H/9325P, 9300/9300S, and 10000: The clusters sends the IGMP join to any valid multicast group IP address that is within the range from 224.0.0.0 to 239.255.255.255 except reserved group IP addresses.

Command History

Release	Modification
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4 parameter is deprecated.
10.08	Added NLB support for 8360 Switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config-if and config-if-vlan	Administrators or local user group members with execution rights for this command.

show arp

```
show arp
```

Description

Displays the static ARP multicast information.

Examples

Displaying the static ARP multicast information:

```
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

Release	Modification
10.08	Added NLB support for 8360 Switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip igmp snooping vlan group

```
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

Port      Vers Mode Uptime   Expires   V1      V2      Sources  Sources
-----  - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1/1/6    2   EXC 0m 21s   1m 12s   Timer   Timer   Forwarded Blocked
```

Displaying multicast joins participating in the IGMP group:

```
switch# show ip igmp snooping vlan 2 group 232.0.0.1

IGMP ports and group information for group 232.0.0.1

VLAN ID    : 2
VLAN Name  : VLAN2

Group Address : 232.0.0.1
```

Last Reporter : 30.1.1.1
Group Type : Filter

Port	Vers	Mode	Uptime	Expires	V1 Timer	V2 Timer	Sources Forwarded	Sources Blocked
-								
vxlan(5.5.5.5)	3	INC	14m 52s	0m 0s			1	0

Group Address: 232.0.0.1
Source Address: 30.1.1.30
Source Type: Filter

Port	Mode	Uptime	Expires	Configured Mode
-				
vxlan1(5.5.5.5)	ING	14m 52s		Auto

Command History

Release	Modification
10.08	Added NLB support for 8360 Switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

Accessing HPE Aruba Networking Support

HPE Aruba Networking Support Services	https://www.hpe.com/us/en/networking/hpe-aruba-networking-support-services.html
AOS-CX Switch Software Documentation Portal	https://arubanetworking.hpe.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking Support Portal	https://networkingsupport.hpe.com/home
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-650-750-0350 (Backup—Toll Number)
International telephone	https://www.hpe.com/psnow/doc/a50011948enw

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:

HPE Aruba Networking Developer Hub	https://developer.arubanetworks.com/hpe-aruba-networking-aoscx/docs/about
Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Software Technical Update channel on YouTube.	Videos on new features introduced in this release: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

HPE Aruba Networking Hardware Documentation and Translations Portal	https://arubanetworking.hpe.com/techdocs/hardware/DocumentationPortal/Content/home.htm
HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing and Feature Packs	https://licensemanagement.hpe.com/
End-of-Life information	https://networkingsupport.hpe.com/end-of-life

Accessing Updates

You can access updates from the HPE Aruba Networking Support Portal at <https://networkingsupport.hpe.com>.

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://networkingsupport.hpe.com/notifications/subscriptions> (requires an active HPE Aruba Networking Support Portal account to manage subscriptions). Security notices are viewable without an HPE Aruba Networking Support Portal account.

Warranty Information

To view warranty information for your product, go to <https://www.arubanetworks.com/support-services/product-warranties/>.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at <https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

Additional regulatory information

HPE Aruba Networking 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

HPE Aruba Networking 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.