AOS-CX 10.10 IP Services Guide

4100i, 6000, 6100 Switch Series

Hewlett Packard Enterprise

Published: August 2022
Version: 2

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

Acknowledgments

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

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

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

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

UNIX® is a registered trademark of The Open Group.

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

Contents

About this document 8
Applicable products 8
Latest version available online 8
Command syntax notation conventions 8
About the examples 9
Identifying switch ports and interfaces 9

IRDP 11
Configuring IRDP 12
IRDP commands 13
diag-dump irdp basic 13
ip irdp 14
ip irdp holdtime 14
ip irdp maxadvertinterval 15
ip irdp minadvertinterval 16
ip irdp preference 17
show ip irdp 18

IPv6 Router Advertisement 19
Configuring IPv6 RA 19
IPv6 RA scenario 21
IPv6 RA commands 21
ipv6 address <global-unicast-address> 21
ipv6 address autoconfig 22
ipv6 address link-local 23
ipv6 nd cache-limit 24
ipv6 nd dad attempts 25
ipv6 nd hop-limit 25
ipv6 nd mtu 26
ipv6 nd ns-interval 27
ipv6 nd prefix 27
ipv6 nd ra dns search-list 29
ipv6 nd ra dns server 30
ipv6 nd ra lifetime 31
ipv6 nd ra managed-config-flag 31
ipv6 nd ra max-interval 32
ipv6 nd ra min-interval 33
ipv6 nd ra other-config-flag 34
ipv6 nd ra reachable-time 35
ipv6 nd ra retrans-timer 35
ipv6 nd route 36
ipv6 nd router-preference 37
ipv6 nd suppress-ra 38
show ipv6 nd global traffic 39
show ipv6 nd interface 40
show ipv6 nd interface prefix 42
show ipv6 nd interface route 43
show ipv6 nd ra dns search-list 44
show ipv6 nd ra dns server 45

sFlow **46**
- sFlow agent 46
- Configuring the sFlow agent 47
- sFlow scenario 48
- sFlow scenario 2 49
- sFlow agent commands 51
  - clear sflow statistics 51
  - sflow 52
  - sflow agent-ip 53
  - sflow collector 54
  - sflow disable 55
  - sflow header-size 55
  - sflow max-datagram-size 56
  - sflow polling 57
  - sflow sampling 58
  - show sflow 59

DHCP client **61**
- DHCP client 61
  - DHCP client commands 61
    - ip dhcp 61
    - show ip dhcp 62
- DHCP relay agent 62
  - DHCPv4 relay agent 62
    - Configuring the DHCPv4 relay agent 63
    - DHCPv4 relay scenario 1 64
    - DHCPv4 relay scenario 2 65
    - DHCPv4 relay commands 67
  - DHCPv6 relay agent 75
    - DHCPv6 relay scenario 1 75
    - DHCP relay (IPv6) commands 76

DHCP snooping **81**
- DHCP server interoperation 81
- DHCPv4 snooping conditions for dropping DHCPv4 packets 81
- Protocol details 82
- DHCPv4 snooping commands 82
  - clear dhcpv4-snooping binding 82
  - clear dhcpv4-snooping statistics 83
  - dhcpv4-snooping 84
  - dhcpv4-snooping (in config-vlan context) 85
  - dhcpv4-snooping allow-overwrite-binding 85
  - dhcpv4-snooping authorized-server 86
  - dhcpv4-snooping event-log client 87
  - dhcpv4-snooping external-storage 88
  - dhcpv4-snooping flash-storage 89
  - dhcpv4-snooping max-bindings 91
  - dhcpv4-snooping option 82 91
  - dhcpv4-snooping static-attributes 93
  - dhcpv4-snooping trust 94
  - dhcpv4-snooping verify mac 94
  - show dhcpv4-snooping 95
  - show dhcpv4-snooping binding 97
  - show dhcpv4-snooping statistics 98
- DHCPv6 snooping commands 99
  - clear dhcpv6-snooping binding 99

clear dhcpv6-snooping statistics 100
dhcpv6-snooping 101
dhcpv6-snooping (in config-vlan context) 101
dhcpv6-snooping authorized-server 102
dhcpv6-snooping event-log client 103
dhcpv6-snooping external-storage 104
dhcpv6-snooping flash-storage 105
dhcpv6-snooping max-bindings 107
dhcpv6-snooping trust 108
show dhcpv6-snooping 108
show dhcpv6-snooping binding 110
show dhcpv6-snooping statistics 111

IP Source Lockdown 112

IPv4 source lockdown commands 112
ipv4 source-binding 112
ipv4 source-lockdown 113
ipv4 source-lockdown hardware retry 114
show ipv4 source-binding 115
show ipv4 source-lockdown 115
IPv6 source lockdown commands 118
ipv6 source-binding 118
ipv6 source-lockdown 119
ipv6 source-lockdown hardware retry 120
show ipv6 source-binding 121
show ipv6 source-lockdown 121

Internet Control Message Protocol (ICMP) 125

ICMP message types 125
When ICMP messages are sent 125
ICMP redirect messages 126
When ICMP redirect messages are sent 126
ICMP commands 126
ip icmp redirect 126
ip icmp throttle 127
ip icmp unreachable 128

DNS 129

DNS client 129
Configuring the DNS client 129
DNS client commands 130
ip dns domain-list 130
ip dns domain-name 131
ip dns host 131
ip dns server address 132
show ip dns 133

ARP 135

ARP commands 136
arp inspection 136
arp inspection trust 137
arp process-grat-arp 137
arp ipv4 mac 138
clear arp 139
ip local-proxy-arp 140
ipv6 neighbor mac 141

ip proxy-arp 142
show arp 142
show arp inspection interface 143
show arp inspection statistics 144
show arp state 145
show arp summary 146
show arp timeout 147
show arp vrf 148
show ipv6 neighbors 149
show ipv6 neighbors state 150

Support and Other Resources 152

Accessing Aruba Support 152
Accessing Updates 153
Aruba Support Portal 153
My Networking 153
Warranty Information 153
Regulatory Information 153
Documentation Feedback 154

Chapter 1
About this document

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

Applicable products

This document applies to the following products:

- Aruba 4100i Switch Series (JL817A, JL818A)
- Aruba 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A)
- Aruba 6100 Switch Series (JL675A, JL676A, JL677A, JL678A, JL679A)

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
`example-text`	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets (`[ ]`).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ *<example-text>* ■ <example-text> ■ *example-text* ■ *example-text*	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ■ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (< >). Substitute the text—including the enclosing angle brackets—with an actual value. ■ 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.
|	Vertical bar. A logical `OR` that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.

Convention	Usage
`{ }`	Braces. Indicates that at least one of the enclosed items is required.
`[ ]`	Brackets. Indicates that the enclosed item or items are optional.
... or . . .	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

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

```
switch>
```

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

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

`switch(`*`CONTEXT-NAME`*`)#`

Indicates the configuration context for a feature. For example:

```
switch(config-if)#
```

Identifies the `interface` context.

Variable information in CLI prompts

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

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

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

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

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

Identifying switch ports and interfaces

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

member/slot/port

On the 4100i 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.

On the 6000 and 6100 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.

Chapter 2
IRDP

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.

On the switches covered by this guide, IRDP is configured on a VLAN interface.

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 VLAN interface 2 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 vlan 2
switch(config-if-vlan)# ip irdp broadcast
switch(config-if-vlan)# ip irdp holdtime 5000
switch(config-if-vlan)# ip irdp maxadvertinterval 30
switch(config-if-vlan)# ip irdp minadvertinterval 25
switch(config-if-vlan)# 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 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
`broadcast`	Advertisements are sent as broadcast packets to IP address 255.255.255.255.
`multicast`	Advertisements are sent as multicast packets to the multicast group with IP address 24.0.0.1. Default.

Examples

Enabling IRDP on interface vlan 2 with packet type set to the default value (multicast).

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp
```

Enabling IRDP on interface vlan 2 with packet type set to broadcast.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp broadcast
```

Disabling IRDP.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip irdp
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 VLAN interface 2 to 5000 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp holdtime 5000
```

Removing the the hold time for VLAN interface 2 to 5000 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip irdp holdtime 5000
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 VLAN interface 2 to 30 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp maxadvertinterval 30
```

Removing the advertisement interval for VLAN interface 2 to 30 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip irdp maxadvertinterval 30
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 VLAN interface 2 to 25 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp minadvertinterval 25
```

Removing the minimum advertisement interval for VLAN interface 2 to 25 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip irdp minadvertinterval 25
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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
<LEVEL>	Specifies the IRDP preference level. Range: -2147483648 to 2147483647. Default: 0.

Example

Setting the IRDP preference level for VLAN interface 2 to 25.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp preference 25
```

Removing the IRDP preference level for VLAN interface 2 to 25.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip irdp preference 25
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ip irdp

`show ip irdp`

Description

Displays IRDP configuration settings.

Example

```
switch# sh ip irdp

 ICMP Router Discovery Protocol

 Interface       Status   Advertising Minimum  Maximum  Holdtime Preference
                          Address     Interval Interval
 --------------- -------- ----------- -------- -------- -------- -----------
 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	ipv6 nd dad attempts
Number of neighbor entries in the ND cache.	131072	`ipv6 nd cache-limit`

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

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 `interface vlan 2`.
- 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 vlan 2
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 vlan 2
Interface vlan2 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: vlan2
     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.

Procedure

1. Configure the VLAN interfaces with IPv6 addresses.
   ```
   switch# config
   switch(config)# interface vlan 2
   switch(config-if-vlan)# ipv6 address 2001::1/64
   switch(config)# interface vlan 3
   switch(config-if-vlan)# ipv6 address 3001::1/64
   switch(config)# interface vlan 4
   switch(config-if-vlan)# ipv6 address 4001::1/64
   ```
2. Enable transmission of all IPv6 RA messages.
   ```
   switch(config-if-vlan)# 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 vlan 2
switch(config-if-vlan)#  ipv6 address 3731:54:65fe:2::a7
```

Disabling a global unicast address:

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

Disabling unicast autoconfiguring:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ipv6 address autoconfig
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 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

Parameter	Description
	`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 vlan 2
switch(config-if-vlan)# ipv6 address link-local
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd dad attempts 5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd hop-limit 64
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd mtu 1300
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd ns-interval 1200
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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: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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd ra lifetime 1200
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd ra managed-config-flag
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd ra max-interval 30
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd ra  min-interval 25
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd ra other-config-flag
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan	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 vlan 2
switch(config-if-vlan)# ipv6 nd ra reachable-time 2000
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan	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 are 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 vlan 2
switch(config-if-vlan)# ipv6 nd ra retrans-timer 400
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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: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		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.

Parameter	Description
`medium`	Sets DRP to medium. Default.
`low`	Sets DRP to low.

Examples

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 nd router-preference high
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	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 vlan 2
switch(config-if-vlan)# ipv6 nd suppress-ra mtu dnssl rdnss
switch(config-if-vlan)# 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-vlan`	Administrators or local user group members with execution rights for this command.

show ipv6 nd global traffic

`show ipv6 nd global traffic`

Description

Displays IPV6 Neighbor Discovery traffic details on a device.

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>]`

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.

Examples

Showing information for all VRFs:

```
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 vlan 2:

```
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 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>]`

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.

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 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 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`

Description

Displays domain name information on all interfaces.

Examples

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

Description

Displays DNS server information on all interfaces.

Examples

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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.

Chapter 4
sFlow

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
- Interface counters polling

- Agent IP configuration for IPv4 and IPv6
- Header size configuration
- Max datagram size configuration
- Ingress sampling for all forwarded traffic (L2, L3)
- Enable/Disable sFlow per interface
- Support for three remote collectors
- An out-of-band collector can be defined on the management VRF
- A collector can be defined on the 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 via SNMP

Configuring the sFlow agent

Procedure

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

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

sFlow setting	Default value	Command to change it
Maximum size of an sFlow datagram.	1400 bytes	`sflow max-datagram-size`

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.

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 **vlan 2** with IP address **10.10.10.1/24.**
   ```
   switch(config)# interface vlan 2
   switch(config-if-vlan)# no shutdown
   switch(config-if-vlan)# ip address 10.10.10.1/24
   switch(config)# quit
   ```
6. Configure interface **vlan 3** with IP address **10.10.11.1/24.**
   ```
   switch(config)# interface vlan 3
   switch(config-if-vlan)# no shutdown
   switch(config-if-vlan)# ip address 10.10.11.1/24
   switch(config)# quit
   ```
7. Configure interface **vlan 4** with IP address **10.10.12.1/24.**
   ```
   switch(config)# interface vlan 4
   switch(config-if-vlan)# no shutdown
   switch(config-if-vlan)# ip address 10.10.12.1/24
   switch(config)# quit
   ```
8. Verify sFlow configuration

```
switch# show sflow

sFlow Global Configuration

----------------------------------------

sFlow                          enabled

Collector IP/Port/Vrf          10.10.10.2/6343/default

Agent Address                  10.0.0.1

Sampling Rate                  1024

Polling Interval               30

Header Size                    128

Max Datagram Size              1400


sFlow Status

----------------------------------------

Running - Yes


sFlow enabled on Interfaces:

----------------------------------------

lag100


sFlow Statistics

----------------------------------------

Number of Samples              200
```

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.

Procedure

1. Configure switch 1.
   a. Enable sFlow globally.
      ```
      switch# config
      switch(config)# sflow
      ```
   b. Set the sFlow agent IP address to **10.10.12.1**.
      ```
      switch(config)# sflow agent-ip 10.10.12.1
      ```
   c. Set the sFlow collector IP address to **10.10.12.2**.
      ```
      switch(config)# sflow collector 10.10.12.2
      ```

d. Configure sFLow sampling rate and polling interval.

```
switch(config)# sflow sampling 5000
switch(config)# sflow polling 10
```

e. Create VLAN **8**.

```
switch(config)# vlan 8
switch(config-vlan-8)# no shutdown
switch(config)# exit
```

f. Define LAG **100** and assign VLAN **vlan 8** to it.

```
switch(config)# interface lag 100
switch(config-lag-if)# no shutdown
switch(config-lag-if)# vlan access 8
switch(config-lag-if)# lacp mode active
```

g. Configure interface **vlan 5**.

```
switch(config)# interface vlan 5
switch(config-if-vlan)# no shutdown
switch(config-lag-if)# no routing
switch(config-if-vlan)# vlan access 8
```

h. Configure VLANs **4** and **5** as members of LAG **100.**

```
switch# (config)#interface vlan 4
switch(config-if-vlan)# no shutdown
switch(config-if-vlan)# lag 100
switch(config-if-vlan)# exit
switch(config)# interface vlan 5
switch(config-if-vlan)# no shutdown
switch(config-if-vlan)# lag 100
switch(config-if-vlan)# exit
```

i. Configure interface **vlan 5** with IP address **10.10.12.1/24**.

```
switch# (config)#interface vlan 5
switch(config-if-vlan)# no shutdown
switch(config-if-vlan)# ip address 10.10.12.1/24
switch(config-if-vlan)# quit
```

j. Verify sFlow configuration.

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

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

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

sFlow Statistics
----------------------------------------
Number of Samples              200
```

2. Configure switch 2.
   a. Create VLAN **8**.
      ```
      switch(config)# vlan 8
      switch(config-vlan-8)# no shutdown
      switch(config)# exit
      ```
   b. Define LAG **100** and assign VLAN **vlan 8** to it.
      ```
      switch(config)# interface lag 100
      switch(config-lag-if)# no shutdown
      switch(config-lag-if)# vlan access 8
      switch(config-lag-if)# lacp mode active
      ```
   c. Configure interface **1/1/1**.
      ```
      switch(config)# interface 1/1/1
      switch(config-if)# no shutdown
      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` `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 (`x.x.x.x`), where `x` is a decimal number from 0 to 255, or IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F. The agent address is used to identify the switch in all sFlow datagrams sent to sFlow collectors. It is usually set to an IP address on the switch that is reachable from 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 (`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.
`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 (`default`) 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 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
`sampling <RATE>`	Specifies the sampling rate. Range: 1 to 16777215. 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	`config`	Administrators or local user group members with execution rights for this command.

show sflow

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

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.

Examples

Showing sFlow information for all interfaces:

```
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

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

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

sFlow Statistics
----------------------------------------
Number of Samples              200
```

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
Number of Samples              30
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
Number of 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
10.07 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 client

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

DHCP client commands

ip dhcp

```
ip dhcp
no ip dhcp
```

Description

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

The `no` form of the command disables DHCP mode and is supported only on interface VLANs.

Examples

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
```

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

`ip dhcp` is supported only on one vlan at a time.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`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

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
10.09 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.

DHCP relay agent

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

Supported interfaces

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

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.

Configuring a BOOTP/DHCP relay gateway

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

Configuring the DHCPv4 relay agent

Prerequisites

- An enabled layer 3 VLAN

Procedure

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

Example

This example creates the following configuration:

- Enables the DHCPv4 relay agent.
- Enables interface **1/1/1** and assigns an IPv4 address to it. (By default, all interfaces are layer 3 and disabled.)

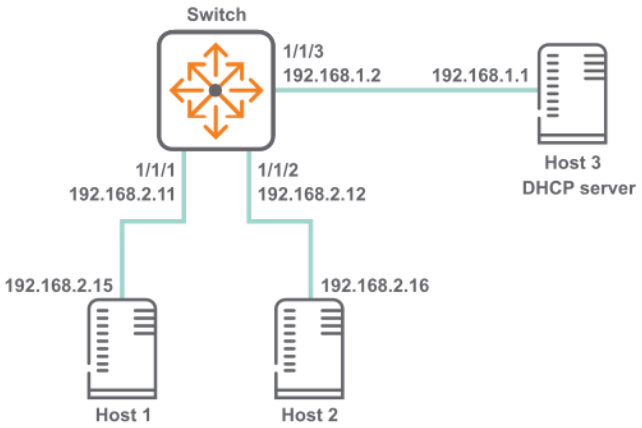
- Defines an IP helper address of **10.10.20.209** on the interface.
- Enables DHCP option 82 support and replaces all option 82 information with the values from the switch with the switch MAC address as the remote ID.

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

```
switch(config)# dhcp-relay
switch(config)# interface 1/1/1
switch(config-if)# vlan access 100
switch(config-if)# exit
switch(config)# interface vlan 100
switch(config-if-vlan)# ip address 198.51.100.1/24
switch(config-if-vlan)# 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
 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
```

DHCPv4 relay scenario 1

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



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 interface vlan 100

```
switch(config)# interface 1/1/1
switch(config-if)# vlan access 100
switch(config-if)# exit
switch(config)# interface 1/1/2
switch(config-if)# vlan access 100
switch(config-if)# exit
switch(config)# interface vlan 100
switch(config-if-vlan)# ip address 192.168.2.11/24
switch(config-if-vlan)# ip helper-address 192.168.1.1
```

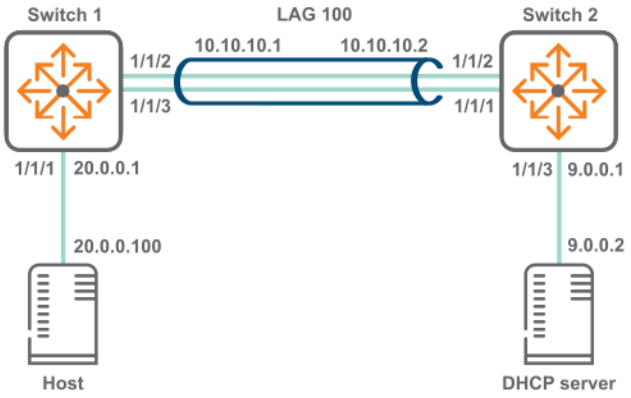
3. Verify DHCP relay configuration.

```
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(config)# show ip helper-address

IP Helper Addresses

Interface: vlan100
  IP Helper Address                VRF
  -----------------               -----------------
  192.168.1.1                      default
```

DHCPv4 relay scenario 2

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)# vlan access 200
switch(config-lag-if)# lacp mode active
switch(config-lag-if)# exit
switch(config)# interface vlan 200
switch(config-if-vlan)# ip address 10.0.10.1/24
```

   b. Assign an IP address to interface vlan 100 and an IP helper address to reach the DHCP server.

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# vlan access 100
switch(config-if)# exit
switch(config)# interface vlan 100
switch(config-if-vlan)# ip address 20.0.0.1/8
switch(config-if-vlan)# 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)# vlan access 200
switch(config-lag-if)# lacp mode active
switch(config-lag-if)# exit
switch(config)# interface vlan 200
switch(config-if-vlan)# ip address 10.0.10.2/24
```

b. Assign an IP address to interface vlan 300.

```
switch(config)# interface 1/1/3
switch(config-if)# no shutdown
switch(config-if)# vlan access 300
switch(config-if)# exit
switch(config)# interface vlan 300
switch(config-if-vlan)# ip address 9.0.0.1/24
```

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 20.0.0.0 and 10.0.10.1.

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

DHCPv4 relay commands

dhcp-relay

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

Description

Enables DHCP relay support. DHCP relay is enabled by default. DHCP relay is not supported on the management interface.

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

Examples

This example enables DHCP relay support.

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

This example removes DHCP relay support.

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	`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
4100i	`config`	Administrators or local user group members with execution rights for this command.

dhcp-relay option 82

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

Description

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

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

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.
`validate`	Validate option 82 information in DHCP server responses and drop invalid responses.
`drop`	Drop any inbound client DHCP packet that contains option 82 information.
`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 `ip source-interface`.
`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
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	`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
System Mac [f4:03:43:80:27:00]
VRF :BLUE, Source Ip:200.0.0.10
vsx: Not Present
Interface vlan2: 1
Client Packet Statistics:
Valid Dropped O82_Valid O82_Dropped vsx_drops
----- ------- --------- ----------- ---------
0 0 0 0 0
Server Packet Statistics:
Valid Dropped O82_Valid O82_Dropped Invalid_IP_Drops To_Dsnoop
----- ------- --------- ----------- ---------------- ---------
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 Dropped O82_Valid O82_Dropped Invalid_IP_Drops To_Dsnoop
----- ------- --------- ----------- ---------------- ---------
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.
[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
4100i	`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 (`x.x.x.x`), where `x` is a is a decimal number from 0 to 255.

Examples

Setting the IP address of the gateway for interface vlan 100 to 10.10.10.10:

```
switch(config)# interface vlan100
switch(config-if)# ip bootp-gateway 10.10.10.10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	`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 agent forwards DHCP client requests to all defined servers.

This command requires that you define a source IP address for DHCP relay with the command `ip source-interface`. The configured source IP on the VRF is used to forward DHCP packets to the server.

A helper address cannot be defined on the OOBM interface.

The `no` form of this command removes an IP helper address.

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

Examples

Defining the IP helper address 10.10.10.209 on interface vlan 100:

```
switch(config)# interface vlan100
switch(config-if-vlan)# ip helper-address 10.10.10.209
```

Removing the IP helper address 10.10.10.209 on interface vlan 100:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	`config-if`	Administrators or local user group members with execution rights for this command.

show dhcp-relay

`show dhcp-relay`

Description

Shows DHCP relay configuration settings.

Example

Showing DHCP relay settings:

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	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>]`

Description

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

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

Examples

Showing the designated bootp gateway for all interfaces:

```
switch(config)# show dhcp-relay bootp-gateway

BOOTP Gateway Entries
```

```
Interface            Source IP
-------------------- ---------------
vlan10               1.1.1.1
vlan20               2.2.2.2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	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>]`

Description

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

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

Examples

Showing the IP helper addresses for all interfaces:

```
switch(config)# show ip helper-address

IP Helper Addresses

Interface: vlan11
  IP Helper Address                  VRF
  -----------------                 -----------------
  10.10.10.209                       default

Interface: vlan20
  IP Helper Address                  VRF
  -----------------                 -----------------
  3.3.3.3                            default
  20.20.20.20                        default
```

Showing the IP helper addresses for interface vlan20:

```
switch(config)# show ip helper-address interface vlan20

IP Helper Addresses

Interface: vlan20
  IP Helper Address                  VRF
  -----------------                 -----------------
  3.3.3.3                            default
  20.20.20.20                        default
```

Command History

Release	Modification
10.07 or earlier	--

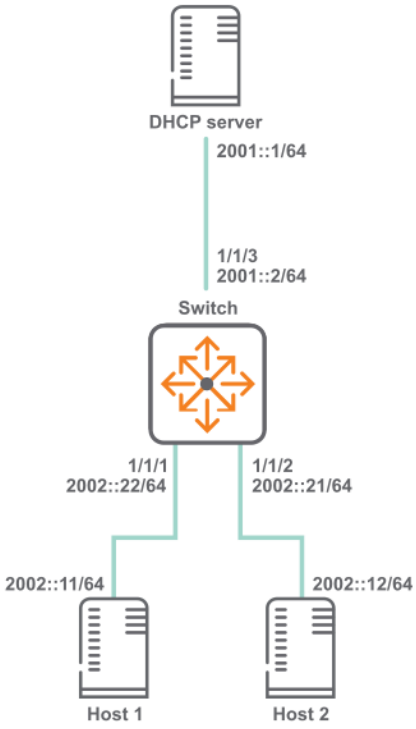
Command Information

Platforms	Command context	Authority
4100i	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 scenario 1

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



Procedure

1. Enable DHCP relay.

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

2. Define an IPv6 helper address on interfaces `1/1/1` and `1/1/2` .

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 address 2002::22/64
switch(config-if)# ipv6 helper-address 2001::1
switch(config-if)# interface 1/1/2
switch(config-if)# ipv6 address 2002::21/64
switch(config-if)# ipv6 helper-address 2001::1
switch(config-if)# quit
```

3. Verify DHCP relay configuration.

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

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

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

DHCP relay (IPv6) commands

dhcpv6-relay

```
dhcpv6-relay
no dhcpv6-relay
```

Description

Enables DHCPv6 relay support. DHCPv6 relay is disabled by default.

DHCP relay is not supported on the management interface

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

Examples

Enables DHCPv6 relay support.

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

Removes DHCPv6 relay support.

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	config	Administrators or local user group members with execution rights for this command.

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
4100i	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 `x` 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 `x` 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
4100i	`config-if`	Administrators or local user group members with execution rights for this command.

show dhcpv6-relay

`show dhcpv6-relay`

Description

Shows DHCP relay configuration settings.

Example

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	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>]`

Description

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

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

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 1/1/1

 Interface: 1/1/1
 IPv6 Helper Address                          Egress Port
 -------------------------------------------- -----------
 2001:db8:0:1::                               -
 FF01::1:1000                                 1/1/2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i	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.

Chapter 6
DHCP snooping

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`.

DHCP server interoperation

DHCP server may not be configured with DHCP snooping.

DHCPv4 snooping conditions for dropping DHCPv4 packets

Applies only to DHCPv4 snooping.

Packet types that are dropped	Conditions for dropping the packets
DHCPOFFER, DHCPACK, DHCPNACK	▪ A packet from a DHCP server is received on an untrusted port. ▪ The switch is configured with a list of authorized DHCP server addresses

Packet types that are dropped	Conditions for dropping the packets
	and a DHCP response received on a trusted port, but the source IP address is not an authorized DHCP server.
DHCPRELEASE, DHCPDECLINE	▪ A broadcast packet that has a MAC address in the DHCP binding database, but the port in the DHCP binding database does not match the port on which the packet is received.
All DHCP packet types	▪ 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. ▪ A DHCP packet containing DHCP relay information (option 82) is received on an untrusted port.

Protocol details

1. When a port is configured as a trusted port, all the dynamic IP binding entries learned on that port will be deleted.
2. 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.
3. 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.

DHCPv4 snooping commands

clear dhcpv4-snooping binding

```
clear dhcpv4-snooping binding {all | ip <IPV4-ADDR> vlan <VLAN-ID> | port <PORT-NUM> |
vlan <VLAN-ID>}
```

Description

Clears DHCPv4 snooping binding entries.

Parameter	Description
`all`	Specifies that all DHCPv4 binding information is to be cleared.
`ip <IPV4-ADDR> vlan <VLAN-ID>`	Specifies the IPv4 address and VLAN for which all DHCPv4 binding information is to be cleared.
`port <PORT-NUM>`	Specifies the port number for which all DHCPv4 binding information is to be cleared.
`vlan <VLAN-ID>`	Specifies the VLAN for which all DHCPv4 binding information is to be cleared.

Examples

Clearing all DHCPv4 binding information for IP address 192.168.2.4 and VLAN 5:

```
switch(config)# clear dhcpv4-snooping binding ip 192.168.2.4 vlan 5
```

Clearing all DHCPv4 binding information for port 1/1/1:

```
switch(config)# clear dhcpv4-snooping binding port 1/1/1
```

Clearing all DHCPv4 binding information for VLAN 10:

```
switch(config)# clear dhcpv4-snooping binding vlan 10
```

Clearing all DHCPv4 binding information:

```
switch(config)# clear dhcpv4-snooping binding all
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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 dhcpv4-snooping statistics

```
clear dhcpv4-snooping statistics
```

Description

Clears all DHCPv4 snooping statistics.

Examples

Clear all DHCPv4 snooping statistics:

```
switch# clear dhcpv4-snooping statistics
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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.

dhcpv4-snooping

```
dhcpv4-snooping
no dhcpv4-snooping
```

Description

Enables DHCPv4 snooping. DHCPv4 snooping is disabled by default. DHCP snooping is not supported on the management interface.
The no form of the command disables DHCPv4 snooping, flushing all the IP bindings learned since DHCPv4 snooping was enabled.

Examples

Enabling DHCPv4 snooping:

```
switch(config)# dhcpv4-snooping
```

Disabling DHCPv4 snooping:

```
switch(config)# no dhcpv4-snooping
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping (in config-vlan context)

```
dhcpv4-snooping
no dhcpv4-snooping
```

Description

Enables DHCPv4 snooping for the specified VLAN in the `config-vlan` context. DHCPv4 snooping is disabled by default for all VLANs.

The no form of the command disables DHCPv4 snooping on the specified VLAN, flushing all the IP bindings learned for this VLAN since DHCPv4 snooping was enabled for this VLAN.

Examples

Enabling DHCPv4 snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# dhcpv4-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Disabling DHCPv4 snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no dhcpv4-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config-vlan`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping allow-overwrite-binding

```
dhcpv4-snooping allow-overwrite-binding
no dhcpv4-snooping allow-overwrite-binding
```

Description

Allows binding to be overwritten for the same IP address. When enabled, and a DHCP server offers a host an IP address that is already bound to an existing host in the binding table, the existing binding is

overwritten for the new host if the new host is successfully able to acquire the same IP address. This overwriting is disabled by default, causing the DHCP server offers to be dropped.

The no form of the command disables DHCPv4 snooping overwrite binding.

Examples

Enabling DHCPv4 snooping overwrite binding:

```
switch(config)# dhcpv4-snooping allow-overwrite-binding
```

Disabling DHCPv4 snooping overwrite binding:

```
switch(config)# no dhcpv4-snooping allow-overwrite-binding
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping authorized-server

```
dhcpv4-snooping authorized-server <IPV4-ADDR> [vrf <VRF-NAME>]
no dhcpv4-snooping authorized-server <IPV4-ADDR> [vrf <VRF-NAME>]
```

Description

Adds an authorized (trusted) DHCP server to a list of authorized servers for use by DHCPv4 snooping. This command can be issued multiple times, adding a maximum of 20 authorized servers per VRF. By default, with an empty list of authorized servers, all DHCP servers are considered to be trusted for DHCPv4 snooping purposes.

The `mgmt` VRF cannot be used with this command.

The no form of this command deletes the specified DHCP server from the authorized list.

Parameter	Description
<IPV4-ADDR>	Specifies the IPv4 address of the trusted DHCPv4 server.
`vrf` *<VRF-NAME>*	Specifies the VRF name.

Usage

For authorized server lookup, the VRF is derived from the Switch Virtual Interface (SVI) configured for the incoming VLAN. If the SVI is not configured, the `default` VRF is assumed.

Examples

Adding DHCP servers 192.168.2.2, 192.168.2.3, and 192.168.2.10 to the authorized server list:

```
switch(config)# dhcpv4-snooping authorized-server 192.168.2.2
switch(config)# dhcpv4-snooping authorized-server 192.168.2.3 vrf default
switch(config)# dhcpv4-snooping authorized-server 192.168.2.10 vrf default
```

Removing DHCP server 192.168.2.3 from the authorized server list:

```
switch(config)# no dhcpv4-snooping authorized-server 192.168.2.3 vrf default
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping event-log client

```
dhcpv4-snooping event-log client
no dhcpv4-snooping event-log client
```

Description

This command enables/disables DHCPv4 client level event logs that help with client telemetry on a remote management station such as Aruba Central. By default, client level event logs are disabled. The `no` form of this command disables client-level event logs for DHCPv4 snooping after they are enabled. View these logged DHCPv4 snooping events by issuing the command `show events -c dhcpv4-snooping`.

Examples

Enabling DHCPv4 client level event logs:

```
switch(config)# # dhcpv4-snooping event-log client
```

Disabling external storage:

```
witch(config)# # no dhcpv4-snooping event-log client
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping external-storage

`dhcpv4-snooping external-storage volume <VOL-NAME> file <FILE-NAME>`
`no dhcpv4-snooping external-storage volume <VOL-NAME> file <FILE-NAME>`

Description

Configures external storage to be used for backing up IP bindings (used by DHCPv4 snooping) to a file. When configured, the switch stores all the IP bindings in an external storage file so that they are retained after the switch restarts. When the switch restarts, it reads the IP bindings from the configured external storage file to populate its local cache.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IP bindings in an external storage file.

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 `dhcpv4-snooping external-storage volume` command, first create the external storage volume using command `external-storage <VOLUME-NAME>`. See *External storage commands* in the *Command-Line Interface Guide*.
`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)# dhcpv4-snooping external-storage volume dhcp_snoop file dsnoop_
ipbindings
```

Disabling external storage:

```
switch(config)# no dhcpv4-snooping external-storage volume dhcp_snoop
```

Disabling external storage when flash storage is also configured (note the message indicating that flash storage will be used):

```
switch(config)# no dhcpv4-snooping external-storage volume dhcp_snoop
DHCPv4-Snooping will use flash storage to store IP Binding database
switch(config)#
```

Command History

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Updated example with flash storage information.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping flash-storage

```
dhcpv4-snooping flash-storage [delay <DELAY>]
no dhcpv4-snooping flash-storage [delay <DELAY>]
```

Description

Configures switch flash storage to be used for backing up client IP bindings (used by DHCPv4 snooping). When flash storage is configured (and external storage is not already configured for this purpose), the switch stores the IP bindings in switch flash storage. When the switch restarts, it reads the IP bindings from the switch flash storage to populate its local cache.

Writing the IP bindings to flash storage only occurs after the configured delay and if there has been a change in client IP bindings. Writing is skipped when client IP bindings have not changed since the previous write.

Omitting `delay <DELAY>` sets the default delay of 900 seconds.

To reduce switch flash aging it is recommended that you use external storage (command `dhcpv4-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)# dhcpv4-snooping flash-storage delay 1200
Warning: Using flash storage reduces switch lifetime. It is recommended to use an
external-storage.
Do you want to continue  (y/n)? y
switch(config)#
```

Unconfiguring usage of switch flash storage for IP bindings :

```
switch(config)# no dhcpv4-snooping flash-storage
```

Command History

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping max-bindings

```
dhcpv4-snooping max-bindings <MAX-BINDINGS>
no dhcpv4-snooping max-bindings <MAX-BINDINGS>
```

Description

Sets the maximum number of DHCP bindings allowed on the selected interface. For all interfaces on which this command is not run, the default max 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: 0 to 256.

Examples

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

```
switch(config)# interface 1/1/1
switch(config-if)# dhcpv4-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 dhcpv4-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config-if	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping option 82

```
dhcpv4-snooping option 82 [remote-id {mac | subnet-ip}]
                          [untrusted-policy {drop | keep | replace}]
```

```
no dhcpv4-snooping option 82 [remote-id {mac | subnet-ip}]
                             [untrusted-policy {drop | keep | replace}]
```

Description

Configures the addition of option 82 DHCP relay information to DHCP client packets that are being forwarded on trusted ports. DHCP relay is enabled by default.

In the switch default state and when this command is entered without parameters (`dhcpv4-snooping option 82`), this default configuration is used:
`dhcpv4-snooping option 82 remote-id mac untrusted-policy drop`

When `remote-id` is omitted, its default (`mac`) is used. When `untrusted-policy` is omitted, its default (`drop`) is used.

The no form of this command disables DHCPv4 snooping option 82.

Parameter	Description
`remote-id`	Specifies what address to use as the remote ID for the `replace` option of `untrusted-policy`. 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.
`keep`	Forward DHCP packets (with option 82).
`replace`	Replace the option 82 information in the DHCP packets with whatever is set for `remote-id` (one of: `mac`, `subnet-ip`, or `mgmt-ip`) and forward the packets.

Examples

Configuring DHCPv4 snooping option 82 with the keep action:

```
switch(config)# dhcpv4-snooping option 82 untrusted-policy keep
```

Disabling DHCPv4 snooping option 82:

```
switch(config)# no dhcpv4-snooping option 82 untrusted-policy keep
```

Command History

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.

Release	Modification
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping static-attributes

```
dhcpv4-snooping static-attributes
no dhcpv4-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 OVSDB 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 DHCPv4 snooping static attributes:

```
switch(config)# dhcpv4-snooping static-attributes
```

Disabling the storage of DHCPv4 snooping static attributes:

```
switch(config)# no dhcpv4-snooping static-attributes
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping trust

```
dhcpv4-snooping trust
no dhcpv4-snooping trust
```

Description

Enables DHCPv4 snooping trust on the selected port. Only server packets received on trusted ports are forwarded. All the ports are untrusted by default.

The `no` form of the command disables DHCPv4 snooping trust on the selected port.

Examples

Enabling DHCPv4 snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# dhcpv4-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling DHCPv4 snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no dhcpv4-snooping trust
switch(config-if)# exit
switch(config)#
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

dhcpv4-snooping verify mac

```
dhcpv4-snooping verify mac
no dhcpv4-snooping verify mac
```

Description

This command enables verification of the hardware address field in DHCP client packets. When enabled, the DHCP client hardware address field and the source MAC address must be the same for packets received on untrusted ports or else the packet is dropped. This DHCP snooping MAC verification is enabled by default.

The no form of the command disables DHCPv4 snooping MAC verification.

Examples

Enabling DHCPv4 snooping MAC verification:

```
switch(config)# dhcpv4-snooping verify mac
```

Disabling DHCPv4 snooping MAC verification:

```
switch(config)# no dhcpv4-snooping verify mac
```

Command History

Release	Modification
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 for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	config	Administrators or local user group members with execution rights for this command.

show dhcpv4-snooping

```
show dhcpv4-snooping
```

Description

Shows the DHCPv4 snooping configuration.

Examples

Showing the DHCPv4 snooping configuration:

```
switch(config)# show dhcpv4-snooping

 DHCPv4-Snooping Information

  DHCPv4-Snooping         : Yes         Verify MAC Address  : Yes
  Allow Overwrite Binding : No          Enabled VLANs       : 1-100
```

```
  IP Binding Disabled VLANs :
  Static Attributes : Yes
  Client Event Logs : No

 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

                   Max       Static    Dynamic
  Port      Trust  Bindings  Bindings  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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Updated example with flash storage information.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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 dhcpv4-snooping binding

```
show dhcpv4-snooping binding
```

Description

Shows the DHCPv4 snooping binding configuration.

Parameter	Description
`detail`	Shows detailed information for active IP bindings on the system.

Examples

Showing the DHCPv4 snooping binding configuration:

```
switch(config)# show dhcpv4-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 dhcpv4-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
10.10	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 introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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 dhcpv4-snooping statistics

```
show dhcpv4-snooping statistics
```

Description

Shows the DHCPv4 snooping statistics.

Examples

Showing the DHCPv4 snooping statistics:

```
switch(config)# show dhcpv4-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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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 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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`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
<IPV6-ADDR>	Specifies the IPv6 address of the trusted DHCPv6 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 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
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	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/disables DHCPv6 client level event logs that help with client telemetry on a remote management station such as Aruba 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`.

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
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`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 `dhcpv6-snooping external-storage volume` command, first create the external storage volume using command `external-storage <VOLUME-NAME>`. See *External storage commands* in the *Command-Line Interface Guide*.
`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
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Updated example with flash storage information.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`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
`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)# 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
10.09	Command introduced for the 6000 and 6100 Switch Series.

Release	Modification
10.08	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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: 0 to 256.

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
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`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
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show dhcpv6-snooping

```
show dhcpv6-snooping
```

Description

Shows the DHCPv6 snooping configuration.

Examples

Showing the DHCPv6 snooping configuration:

```
switch(config)# show dhcpv6-snooping

 DHCPv6-Snooping Information

  DHCPv6-Snooping     : Yes    Enabled VLANs       : 1,5,7,100-110

 External Storage Information

  Volume Name          : dhcp_snoop
  File Name            : ip_binding
  Inactive Since       : 01:23:20 09/10/2021
  Error                : Failed to write external storage

 Flash Storage Information

  File Write Delay : 300 seconds

 Active Storage : External

 Authorized Server Configurations

  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

                    Max       Static    Dynamic
  Port      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
10.09	Command introduced for the 6000 and 6100 Switch Series.

Release	Modification
10.08	Updated example with flash storage information.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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
```

Description

Shows the DHCPv6 snooping binding configuration.

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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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
```

Description

Shows the DHCPv6 snooping statistics.

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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	Command introduced for the 4100i Switch Series.

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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.

Chapter 7
IP Source Lockdown

IP source lockdown provides added security by preventing IP source address spoofing on a per-port basis. Every packet is inspected for this purpose in hardware. When IP source lockdown is enabled, IP traffic received on an interface (port) is forwarded only if the VLAN, IP address, MAC address, interface (port) matches the IP binding database entry.

It is best to configure IP source lockdown during a switch maintenance period as enabling it may cause client traffic to be dropped for 10 to 15 seconds.

To use IPv4 source lockdown, the IPv4 binding database must be populated. The binding database is typically dynamically populated by DHCPv4 snooping that learns and saves the binding information. Alternatively, the IPv4 binding database can be statically populated with the `ipv4 source-binding` command described in this chapter. Often DHCPv4 snooping is used to dynamically populate most of the IP binding database along with the `ipv4 source-binding` command that is used to add the binding information for several known and trusted clients, typically administrators. For dynamic IP binding database population with DHCPv4 snooping, see DHCP snooping.

To use IPv6 source lockdown, the IPv6 binding database must be populated. The binding database is typically dynamically populated by DHCPv6 snooping that learns and saves the binding information. Alternatively, the IPv6 binding database can be statically populated with the `ipv6 source-binding` command described in this chapter. Often DHCPv6 snooping is used to dynamically populate most of the IPv6 binding database along with the `ipv6 source-binding` command that is used to add the binding information for several known and trusted clients, typically administrators. For dynamic IPv6 binding database population with DHCPv6 snooping, see DHCP snooping.

IP source lockdown should not be configured on ISL (inter-switch link) ports.

IPv4 source lockdown commands

ipv4 source-binding

```
ipv4 source-binding <VLAN-ID> <IPV4-ADDR> <MAC-ADDR> <IFNAME>
no ipv4 source-binding <VLAN-ID> <IPV4-ADDR> <MAC-ADDR> <IFNAME>
```

Description

Adds static IPv4 client source binding information to the switch IP binding database. Although DHCPv4 snooping is often used to dynamically populate the binding database, this command is available for manually adding entries to the switch IP binding database.

Statically configured IP binding information supersedes any dynamically collected binding information for the same client.

The no form of this command removes the specified binding that was statically configured with the `ipv4 source-binding` command. The no form has no effect on bindings that were dynamically configured with DHCPv4 snooping.

Parameter	Description
<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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`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).

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
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show ipv4 source-binding

```
show ipv4 source-binding
```

Description

Shows all IPv4 static source binding information irrespective of source lockdown configuration..

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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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>]
```

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.

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 : --
```

Showing the detailed binding record and related information for interface 1/1/2:

```
switch# show ipv4 source-lockdown binding interface 1/1/2

 Interface Name        : 1/1/2
 VLAN Id               : 100
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 120.168.43.52
 Time Remaining        : 115 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable
```

Showing the detailed binding record and related information for interface lag112 (identified in this example command by the IP address):

```
switch# show ipv4 source-lockdown binding ip 120.168.76.182

 Interface Name        : lag112
 VLAN Id               : 12
 MAC Address           : 00:50:56:96:d8:3d
 IP Address            : 120.168.76.182
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --
```

Showing the detailed binding record and related information for interface 1/1/1 (identified in this example command by the MAC address):

```
switch# show ipv4 source-lockdown binding mac 00:50:56:96:e4:cf

 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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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).

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
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show ipv6 source-binding

```
show ipv6 source-binding
```

Description

Shows all IPv6 static source binding information irrespective of source lockdown configuration.

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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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>]
```

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.

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 : --
```

Showing the detailed binding record and related information for interface 1/1/2:

```
switch# show ipv6 source-lockdown binding interface 1/1/2

 Interface Name        : 1/1/2
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 4000::1
 Time Remaining        : 3290 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable
```

Showing the detailed binding record and related information for interface 1/1/2 (identified in this example command by the IP address):

```
switch# show ipv6 source-lockdown binding ip 4000::1

 Interface Name        : 1/1/2
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 4000::1
 Time Remaining        : 515 seconds
 Lockdown Status       : No
 Hardware Status       : 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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
4100i 6000 6100	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.

Chapter 8
Internet Control Message Protocol (ICMP)

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 packed. Default setting.

The `no` form of this command disables the sending of ICMPv4 and ICMPv6 destination unreachable messages from the switch to a source host when a specific host is unreachable. This command does not prevent other hosts from sending an ICMP unreachable message.

Examples

Enabling ICMPv4 and ICMPv6 destination unreachable messages to a source host:

```
switch(config)# ip icmp unreachable
```

Disabling ICMPv4 and ICMPv6 destination unreachable messages to a source host:

```
switch(config)# no ip icmp unreachable
```

Command History

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.

Chapter 9
DNS

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
Domain Name: switch.com
Name Server(s): 1.1.1.1

Host Name                                                                    Address
-------------------------------------------------------------------------------------
myhost1                                                                      3.3.3.3
switch#
```

DNS client commands

ip dns domain-list

```
ip dns domain-list <DOMAIN-NAME> [vrf default]
no ip dns domain-list <DOMAIN-NAME> [vrf default]
```

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
`list <DOMAIN-NAME>`	Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.

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 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 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>]`

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.

Examples

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.

Chapter 10
ARP

ARP (Address Resolution Protocol) is used to map the network address assigned to a device to its physical address. For example, on an Ethernet network, ARP maps layer 3 IPv4 network addresses to layer 2 MAC addresses. (ARP does not work with IPv6 addresses. Instead, the Neighbor discovery protocol is used.)

ARP operates at layer 2. ARP requests are broadcast to all devices on the local network segment and are not forwarded by routers. ARP is enabled by default and cannot be disabled.

Proxy ARP

Proxy ARP allows a routing switch to answer ARP requests from devices on one network on behalf of devices on another network. The ARP proxy is aware of the location of the traffic destination, and offers its own MAC address as the final destination.

For example, if Proxy ARP is enabled on a routing switch connected to two subnets (10.10.10.0/24 and 20.20.20.0/24), the routing switch can respond to an ARP request from 10.10.10.69 for the MAC address of the device with IP address 20.20.20.69.

Typically, the host that sent the ARP request then sends its packets to the switch that has the ARP proxy. This switch then forwards the packets to the intended host through a mechanism such as a tunnel.

Proxy ARP is supported on L3 physical and VLAN interfaces. It is disabled by default. To enable proxy ARP, routing must be enabled on the interface.

Local proxy ARP

Local proxy ARP is a technique by which a device on a given network answers the ARP queries for a host address that is on the same network. It is primarily used to enable layer 3 communication between hosts within a common subnet that are separated by layer 2 boundaries (Example: PVLAN). Local proxy ARP is supported on L3 physical and VLAN interfaces.

Local proxy ARP is disabled by default. Routing must be enabled on the interface to enable local proxy ARP.

Dynamic ARP inspection

Dynamic ARP inspection is supported only on the Aruba 6000 and 6100 Switch Series.

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.

Only the following is supported:

- Enabling and disabling of Dynamic ARP Inspection on a VLAN level (it does not have to be SVI).
- Defining the member ports of a VLAN as either trusted or untrusted.
- Only ARP traffic on untrusted ports subjected to checks.
- Routed ports (RoPs) always treated as trusted.
- Listening to the DHCP Bindings table and check every ARP packet to match against the binding.

ARP ACLs are not supported in this release and the DHCP snooping table will be the only source of binding.

ARP commands

arp inspection

`arp inspection`

Description

Enables Dynamic ARP Inspection on the current VLAN, forcing all ARP packets from untrusted ports to be subjected to a MAC-IP association check against a binding table.

The `no` form of this command disables Dynamic ARP Inspection on the VLAN.

Examples

Enabling dynamic ARP inspection:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# arp inspection
```

Disabling dynamic ARP inspection:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# no arp inspection
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`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
10.07 or earlier	--

Command Information

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

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 Aruba 6300, 6400, 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.

arp ipv4 mac

`arp ipv4 <IPV4_ADDR> mac <MAC_ADDR>`
`no arp ipv4 <IPV4_ADDR> mac <MAC_ADDR>`

Description

Specifies a permanent static neighbor entry in the ARP table (for IPv4 neighbors).

The `no` form of this command deletes a permanent static neighbor entry from the ARP table.

Parameter	Description
`ipv4 <IPV4-ADDR>`	Specifies the IP address of the neighbor or the virtual IP address of the cluster in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255. . Range: 4096 to 131072. Default: 131072.
`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 ipv4 2.2.2.2 mac 01:00:5e:00:00:01
```

Removing a static ARP entry on interface VLAN**10**:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no arp ipv4 2.2.2.2 mac 01:00:5e:00:00:01
```

Command History

Release	Modification
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.

clear arp

`clear arp [port <PORT-ID> | vrf {all-vrfs | <VRF-NAME>}]`

Description

Clears IPv4 and IPv6 neighbor entries from the ARP table. If you do not specify any parameters, ARP table entries are cleared for the default VRF.

Parameter	Description
`port <PORT-ID>`	Specifies a physical port on the switch. Format: `member/slot/port`. For example: `vlan 2.`.
`all-vrfs`	Selects all VRFs.
`<VRF-NAME>`	Specifies the name of a VRF. Default: default.

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 vlan 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.

ip local-proxy-arp

```
ip local-proxy-arp
no ip local-proxy-arp
```

Description

Enables local proxy ARP on the specified interface. Local proxy ARP is supported on Layer 3 physical interfaces and on VLAN interfaces. To enable local proxy ARP on an interface, routing must be enabled on that interface.

The `no` form of this command disables local proxy ARP on the specified interface.

Examples

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
```

Command History

Release	Modification
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.

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 **vlan 2**.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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.

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.

show arp

```
show arp
```

Description

Shows the entries in the ARP (Address Resolution Protocol) table.

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
------------------------------------------------------------------------------
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`

Description

Displays the current configuration of dynamic ARP inspection on a VLAN or interface.

Examples

```
switch# show arp inspection interface

------------------------------------------------------------------------------
Interface           Trust-State
------------------------------------------------------------------------------
1/1/1               Untrusted
------------------------------------------------------------------------------
```

```
switch# show arp inspection interface vsx-peer
```

```
--------------------------------------------------------------------------------
Interface           Trust-State
--------------------------------------------------------------------------------
1/1/1               Untrusted
lag100              Trusted
--------------------------------------------------------------------------------
```

```
switch# show arp inspection interface 1/1/1

--------------------------------------------------------------------------------
Interface           Trust-State
--------------------------------------------------------------------------------
1/1/1               Untrusted
--------------------------------------------------------------------------------
```

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 inspection statistics

```
show arp inspection statistics
```

Description

Displays statistics about forwarded and dropped ARP packets.

Examples

```
switch# show arp inspection statistics vlan 1-200

-------------------------------------------------------------------
VLAN   Name              Forwarded           Dropped
-------------------------------------------------------------------
1      DEFAULT_VLAN_1    0                   0
-------------------------------------------------------------------
```

```
switch# show arp inspection statistics vlan

-------------------------------------------------------------------
VLAN   Name              Forwarded           Dropped
-------------------------------------------------------------------
1      DEFAULT_VLAN_1    0                   0
```

```
200     VLAN200           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 arp state

`show arp state {all | failed | incomplete | permanent | reachable | stale}`

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 `failed` state. The neighbor might have been deleted.
`incomplete`	Shows the ARP cache entries that are in `incomplete` state. An incomplete state means that address resolution is in progress and the link-layer address of the neighbor has not yet been determined. A solicitation request was sent, and the switch is waiting for a solicitation reply or a timeout.
`permanent`	Shows the ARP cache entries that are in `permanent` state. ARP entries that are in a permanent state can be removed by administrative action only.
`reachable`	Shows the ARP cache entries that are in `reachable` state, meaning that the neighbor is known to have been reachable recently.
`stale`	Shows ARP cache entries that are in `stale` state. ARP cache entries are in the `stale` state if the elapsed time is in excess of the ARP timeout in seconds since the last positive confirmation that the forwarding path was functioning properly.

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>]`

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.

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>]`

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 (for example, `1/3/1`).

Examples

Showing ARP timeout information for a VLAN:

```
switch# show arp timeout vlan2
Port             VRF                                 Timeout
-------------------------------------------------------------
vlan2            default                             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 arp vrf

`show arp {all-vrfs | vrf <VRF-NAME>}`

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.

Examples

Showing ARP entries for VRF **test**.

```
switch# show arp vrf test
ARP IPv4 Entries:
-------------------------------------------------------
IPv4 Address    MAC               Port    Physical Port  State      VRF
10.20.30.40     00:50:56:bd:6a:c5 1/1/29  1/1/29         reachable  test
-------------------------------------------------------
```

```
Total Number Of ARP Entries Listed: 1.
------------------------------------------------------

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.
------------------------------------------------------
```

Showing ARP entries for all VRFs.

```
switch# show arp all-vrfs
ARP IPv4 Entries:
------------------------------------------------------
IPv4 Address    MAC                Port    Physical Port  State      VRF
192.168.120.10  00:50:56:bd:10:be  1/1/32  1/1/32         reachable  red
10.20.30.40     00:50:56:bd:6a:c5  1/1/29  1/1/29         reachable  test
------------------------------------------------------
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>}`

Description

Shows entries in the ARP table for all IPv6 neighbors for all VRFs or for a specific VRF.

When no parameters are specified, this command shows all ARP entries for the default VRF, and state information for `reachable` and `stale` entries only.

Parameter	Description
`all-vrfs`	Specifies all VRFs.
`vrf <VRF-NAME>`	Specifies the name of a VRF. Length: 1 to 32 alphanumeric characters.

Examples

```
switch# show ipv6 neighbors
IPv6 Entries:

-------------------------------------------------------

IPv6 Address                  MAC                Port      Physical Port  State

fe80::a21d:48ff:fe8f:2700     a0:1d:48:8f:27:00  vlan2300  1/1/31         reachable

fe80::f603:43ff:fe80:a600     f4:03:43:80:a6:00  vlan2300  1/1/30         reachable

-------------------------------------------------------

Total Number Of IPv6 Neighbors Entries Listed: 2.

-------------------------------------------------------
```

Command History

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}`

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 `failed` state. The neighbor might have been deleted. Set the neighbor to be unreachable.
`incomplete`	Shows ARP cache entries that are in `incomplete` state. An incomplete state means that address resolution is in progress and the link-layer address of the neighbor has not yet been determined. This means that a solicitation request was sent, and you are waiting for a solicitation reply or a timeout.
`permanent`	Shows ARP cache entries that are in `permanent` state.

Parameter	Description
`reachable`	Shows ARP cache entries that are in `reachable` state, meaning that the neighbor is known to have been reachable recently.
`stale`	Shows ARP cache entries that are in `stale` state. ARP cache entries are in the `stale` state if the elapsed time is in excess of the ARP timeout in seconds since the last positive confirmation that the forwarding path was functioning properly.

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.

Chapter 11

Support and Other Resources

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
Aruba Support Portal	https://asp.arubanetworks.com/
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
Aruba Hardware Documentation	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

and Translations Portal	
Aruba software	https://asp.arubanetworks.com/downloads
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal

https://asp.arubanetworks.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://asp.arubanetworks.com/notifications/subscriptions (requires an active Aruba Support Portal (ASP) account to manage subscriptions). Security notices are viewable without an ASP account.

Warranty Information

To view warranty information for your product, go to https://www.arubanetworks.com/support-services/product-warranties/.

Regulatory Information

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

Aruba is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see https://www.arubanetworks.com/company/about-us/environmental-citizenship/.

Documentation Feedback

Aruba is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.