

1 DHCPv6 Snooping Commands

Command	Function
clear ipv6 dhcp snooping binding	Clear all dynamic user information in the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Snooping binding database.
clear ipv6 dhcp snooping prefix	Clear all user information in the DHCPv6 Snooping prefix database.
clear ipv6 dhcp snooping statistics	Clear statistics about DHCPv6 packets processed by DHCPv6 Snooping.
ipv6 dhcp snooping	Enable DHCPv6 Snooping globally.
ipv6 dhcp snooping database write-delay	Write all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time.
ipv6 dhcp snooping database write-to-flash	Write dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.
ipv6 dhcp snooping information option	Add Option 18 or 37 to DHCPv6 request packets.
ipv6 dhcp snooping information option format remote-id	Set the Remote ID sub-option to a user-defined string or the host name when Option 37 is in extended padding mode.
ipv6 dhcp snooping filter-dhcp-pkt	Configure an interface to filter all DHCPv6 request packets.
ipv6 dhcp snooping link-detection	Clear dynamically bound entries on an interface in linkdown state.
ipv6 dhcp snooping trust	Configure an interface as a DHCPv6 Snooping trusted port.
ipv6 dhcp snooping vlan	Enable DHCPv6 Snooping on a VLAN.
ipv6 dhcp snooping vlan information option change-vlan-to vlan	Change the padded VLAN to a specified VLAN when Option 18 is in extended padding mode.
ipv6 dhcp snooping vlan information option format-type interface-id string	Set the Interface ID to a user-defined string for forwarding when Option 18 is in extended padding mode.

renew ipv6 dhcp snooping database	Import information in a flash memory to the DHCPv6 Snooping binding database.
show ipv6 dhcp snooping	Display DHCPv6 Snooping configurations.
show ipv6 dhcp snooping vlan	Display VLANs to which DHCPv6 Snooping does not take effect.
show ipv6 dhcp snooping binding	Display dynamic user information in the DHCPv6 Snooping binding database.
show ipv6 dhcp snooping prefix	Display user information in the DHCPv6 Snooping prefix database.
show ipv6 dhcp snooping statistics	Display statistics about DHCPv6 packets filtered due to DHCPv6 Snooping.
show ipv6 dhcp snooping packet	Display statistics about packets related to the DHCPv6 Snooping function.

1.1 clear ipv6 dhcp snooping binding

Function

Run the **clear ipv6 dhcp snooping binding** command to clear all dynamic user information in the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Snooping binding database.

Syntax

```
clear ipv6 dhcp snooping binding [ ipv6-address ] [ mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ]
```

Parameter Description

ipv6-address: IPv6 address of a user to be deleted.

mac-address: Media access control (MAC) address of a user to be deleted.

vlan *vlan-id*: Specifies the ID of the virtual local area network (VLAN) of a user to be deleted.

interface *interface-type interface-number*: Specifies the interface of a user to be deleted.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

After this command is run, all DHCPv6 users who access an interface with DHCPv6 Source Guard enabled need to re-apply for IPv6 addresses. Otherwise, they cannot access the Internet.

Examples

The following example clears all dynamic user information in the DHCPv6 Snooping binding database.

```
Hostname> enable
Hostname# clear ipv6 dhcp snooping binding
```

Notifications

N/A

Platform Description

N/A

1.2 clear ipv6 dhcp snooping prefix

Syntax

Run the **clear ipv6 dhcp snooping prefix** command to clear all user information in the DHCPv6 Snooping prefix database.

Syntax

```
clear ipv6 dhcp snooping prefix [ ipv6-address ] [ mac-address ] [ vlan vlan-id ] [ interface interface-type  
interface-number ]
```

Parameter Description

ipv6-address: IPv6 address of a user to be deleted.

mac-address: MAC address of a user to be deleted.

vlan *vlan-id*: Specifies the ID of the VLAN of a user to be deleted.

interface *interface-type interface-number*: Specifies the interface of a user to be deleted.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all user information in the DHCPv6 Snooping prefix database.

```
Hostname> enable  
Hostname# clear ipv6 dhcp snooping prefix
```

Notifications

N/A

Platform Description

N/A

1.3 clear ipv6 dhcp snooping statistics

Function

Run the **clear ipv6 dhcp snooping statistics** command to clear statistics about DHCPv6 packets processed by DHCPv6 Snooping.

Syntax

```
clear ipv6 dhcp snooping statistics
```

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears statistics about DHCPv6 packets processed by DHCPv6 Snooping.

```
Hostname> enable
Hostname# clear ipv6 dhcp snooping statistics
```

Notifications

N/A

Platform Description

N/A

1.4 ipv6 dhcp snooping

Function

Run the **ipv6 dhcp snooping** command to enable DHCPv6 Snooping globally.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

DHCPv6 Snooping is disabled globally by default.

Syntax**ipv6 dhcp snooping****no ipv6 dhcp snooping****default ipv6 dhcp snooping****Parameter Description**

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables DHCPv6 Snooping globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ipv6 dhcp snooping database write-delay

Function

Run the **ipv6 dhcp snooping database write-delay** command to write all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time.

Run the **no** form of this command to remove this configuration.

The function of writing all dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time is not configured by default.

Syntax

ipv6 dhcp snooping database write-delay *time*

no ipv6 dhcp snooping database write-delay

Parameter Description

time: Period for saving database records, in seconds. The value range is from 600 to 86400.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to write dynamic user information in the DHCPv6 Snooping binding database to a flash memory at a scheduled time. This prevents binding information loss after a device restarts, there is no need to re-obtain IPv6 addresses to restore communication.

Note

A high saving frequency reduces the lifespan of the flash memory.

Examples

The following example writes all dynamic user information in the DHCPv6 Snooping binding database to a flash memory every 3600s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping database write-delay 3600
```

Notifications

N/A

Common Errors

The configured period exceeds the limit.

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping database write-to-flash](#)

1.6 ipv6 dhcp snooping database write-to-flash

Function

Run the **ipv6 dhcp snooping database write-to-flash** command to write dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.

Syntax

```
ipv6 dhcp snooping database write-to-flash
```

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to write dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.

Examples

The following example writes dynamic user information in the DHCPv6 Snooping binding database to a flash memory in real time.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping database write-to-flash
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping database write-delay](#)

1.7 ipv6 dhcp snooping information option

Function

Run the **ipv6 dhcp snooping information option** command to add Option 18 or 37 to DHCPv6 request packets.

Run the **no** form of this command to remove this configuration.

Option 18 or 37 is not added to DHCPv6 request packets by default.

Syntax

ipv6 dhcp snooping information option [**standard-format**]

no ipv6 dhcp snooping information option [**standard-format**]

Parameter Description

standard-format: Uses the standard padding format for Option 18 or 37.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to add Option 18 or 37 to DHCPv6 request packets, so that a DHCP server can assign addresses based on Option 18 or 37.

When Option 18 or 37 is enabled, the extended padding mode is used by default.

Caution

- Option 18 or 37 for DHCPv6 Snooping and DHCP Relay are mutually exclusive.
 - In wireless access scenarios, the **Circuit ID** sub-option is fixed at **0** in both standard padding and extended padding modes of Option 18.
-

Examples

The following example adds Option 18 or 37 to DHCPv6 request packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping information option
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping information option format remote-id](#)
- [ipv6 dhcp snooping vlan information option change-vlan-to vlan](#)
- [ipv6 dhcp snooping vlan information option format-type interface-id string](#)

1.8 ipv6 dhcp snooping information option format remote-id

Function

Run the **ipv6 dhcp snooping information option format remote-id** command to set the **Remote ID** sub-option to a user-defined string or the host name when Option 37 is in extended padding mode.

Run the **no** form of this command to remove this configuration.

When Option 37 is in extended padding mode, **Remote ID** is not set to a user-defined string or host name by default.

Syntax

```
ipv6 dhcp snooping information option format remote-id { hostname | string ascii-string }
no ipv6 dhcp snooping information option format remote-id { hostname | string ascii-string }
```

Parameter Description

hostname: Sets **Remote ID** to the host name.

string *ascii-string*: Sets **Remote ID** to a user-defined string.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When Option 37 is enabled for DHCPv6 packets in extended padding mode, this command is used to customize the content of **Remote ID**.

Examples

The following example sets **Remote ID** to a host name when Option 37 is in extended padding mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping information option format remote-id hostname
```

Notifications

When the value of the *ascii-string* parameter exceeds 63 characters, the following notification will be displayed:

```
% Failed to execute command, because of "Remote-ID string cannot exceed 63
characters".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping information option](#)

1.9 ipv6 dhcp snooping filter-dhcp-pkt

Function

Run the **ipv6 dhcp snooping filter-dhcp-pkt** command to configure an interface to filter all DHCPv6 request packets.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

No interface is configured to filter all DHCPv6 request packets by default.

Syntax

```
ipv6 dhcp snooping filter-dhcp-pkt
no ipv6 dhcp snooping filter-dhcp-pkt
default ipv6 dhcp snooping filter-dhcp-pkt
```

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to reject all DHCPv6 packets on an untrusted port, that is, to forbid all users on this port to apply for addresses via DHCPv6.

This command can be configured only on L2 switching ports, aggregation ports (APs), or encapsulation sub-interfaces.

Examples

The following example configures GigabitEthernet 0/1 to filter all DHCPv6 request packets sent to this interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp snooping filter-dhcp-pkt
```

Notifications

When this command is configured on a DHCPv6 trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When this command is not configured on an L2 switching port, AP, or L2 encapsulation sub-interface, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ipv6 dhcp snooping link-detection

Function

Run the **ipv6 dhcp snooping link-detection** command to clear dynamically bound entries on an interface in linkdown state.

Run the **no** form of this command to remove this configuration.

Dynamically bound entries on an interface in linkdown state are not cleared by default.

Syntax

ipv6 dhcp snooping link-detection

no ipv6 dhcp snooping link-detection**Parameter Description**

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears dynamically bound entries on an interface in linkdown state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping link-detection
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ipv6 dhcp snooping trust

Function

Run the **ipv6 dhcp snooping trust** command to configure an interface as a DHCPv6 Snooping trusted port.

Run the **no** form of this command to remove this configuration.

All interfaces are DHCPv6 Snooping untrusted ports by default.

Syntax**ipv6 dhcp snooping trust****no ipv6 dhcp snooping trust****Parameter Description**

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure interfaces connected to legitimate DHCPv6 servers as trusted ports. DHCPv6 response packets received on trusted ports are forwarded normally, while those received on untrusted ports are discarded.

This command can be configured only on L2 switching ports, APs, and L2 encapsulation sub-interfaces.

Caution

Generally, uplink interfaces, that is, interfaces connected to trusted DHCPv6 servers are configured as trusted ports.

Examples

The following example configures GigabitEthernet 0/1 as a DHCPv6 Snooping trusted port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ipv6 dhcp snooping trust
```

Notifications

When an interface configured with other access security control options is configured as a DHCPv6 Snooping trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security config conflict".
```

When this command is not configured on an L2 switching port or AP, the following notification will be displayed:

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping](#)

1.12 ipv6 dhcp snooping vlan

Function

Run the **ipv6 dhcp snooping vlan** command to enable DHCPv6 Snooping on a VLAN.

Run the **no** form of this command to remove this configuration.

After DHCPv6 Snooping is enabled globally, it takes effect to all VLANs by default.

Syntax

```
ipv6 dhcp snooping vlan { vlan-range | vlan-min [ vlan-max ] }
```

```
no ipv6 dhcp snooping vlan { vlan-range | vlan-min [ vlan-max ] }
```

Parameter Description

vlan-range: Range of VLANs in which DHCPv6 Snooping takes effect. The value is a character string, for example 1, 3–5, 7, and 9–11.

vlan-min: Minimum ID of a VLAN to DHCPv6 Snooping takes effect. The value range is from 1 to 4094.

vlan-max: Maximum ID of a VLAN to DHCPv6 Snooping takes effect. The value range is from 1 to 4094.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to enable or disable DHCPv6 Snooping for a specific VLAN. This function takes effect only when DHCPv6 Snooping is enabled globally.

Examples

The following example enables DHCPv6 Snooping for VLAN 1000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping vlan 1000
```

The following example enables DHCPv6 Snooping for VLAN 1 to VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ipv6 dhcp snooping vlan 1-10
```

Notifications

When the configured VLAN ID is beyond the range of 1 to 4094, the following notification will be displayed:

```
% Failed to execute command, because of "Not supported vlan range".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 ipv6 dhcp snooping vlan information option change-vlan-to vlan

Function

Run the **ipv6 dhcp snooping vlan information option change-vlan-to vlan** command to change the padded VLAN to a specified VLAN when Option 18 is in extended padding mode.

Run the **no** form of this command to remove this configuration.

When Option 18 is in extended padding mode, the padded VLAN is not changed to a specified VLAN by default.

Syntax

ipv6 dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id*

no ipv6 dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id*

Parameter Description

vlan-id: VLAN ID. The value range is from 1 to 4094.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When Option 18 is enabled for DHCPv6 packets in extended padding mode, this command is used to change the padded VLAN to a specified VLAN.

Examples

The following example adds Option 18 to DHCPv6 request packets and changes VLAN 4094 in the **Interface ID** sub-option of Option 18 to VLAN 4093.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if)# ipv6 dhcp snooping vlan 4094 information option change-vlan-to vlan 4093
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping information option](#)
- [ipv6 dhcp snooping vlan information option format-type interface-id string](#)

1.14 ipv6 dhcp snooping vlan information option format-type interface-id string

Function

Run the **ipv6 dhcp snooping vlan information option format-type interface-id string** command to set the **Interface ID** to a user-defined string for forwarding when Option 18 is in extended padding mode.

Run the **no** form of this command to remove this configuration.

When Option 18 is in extended padding mode, **Interface ID** is not set to a user-defined string for forwarding by default.

Syntax

```
ipv6 dhcp snooping vlan vlan-id information option format-type interface-id string ascii-string  
no ipv6 dhcp snooping vlan vlan-id information option format-type interface-id string ascii-string
```

Parameter Description

vlan-id: VLAN of DHCPv6 request packets.

ascii-string: User-defined **Interface ID** content. The value is a string of 3 to 63 bytes in ASCII format.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

When DHCPv6 Option 18 is enabled in extended padding mode, this command is used to set **Interface ID** to a user-defined string.

Examples

The following example sets **Interface ID** to a port name when Option 18 is added to DHCPv6 request packets.

```
Hostname> enable  
Hostname# configure terminal  
Hostname(config)# interface gigabitethernet 0/1
```



```
Hostname(config-if)# ipv6 dhcp snooping vlan 4094 information option format-type  
interface-id string port-name
```

Notifications

When the user-defined character string is not 3 to 63 characters, the following notification is displayed:

```
% Failed to execute command, because of "Interface-ID string must be 3 to 63  
characters".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping information option](#)
- [ipv6 dhcp snooping vlan information option change-vlan-to vlan](#)

1.15 renew ipv6 dhcp snooping database

Function

Run the **renew ipv6 dhcp snooping database** command to import information in a flash memory to the DHCPv6 Snooping binding database.

Syntax

```
renew ipv6 dhcp snooping database
```

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to import the information in a flash memory to the DHCPv6 Snooping binding database.

Caution

- Lease expiration records in the backup file are ignored.
 - Only records that do not exist in the database are added.
-

Examples

The following example imports information in a flash memory to the DHCPv6 Snooping binding database.

```
Hostname> enable
Hostname# renew ipv6 dhcp snooping database
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [ipv6 dhcp snooping database write-to-flash](#)

1.16 show ipv6 dhcp snooping

Function

Run the **show ipv6 dhcp snooping** command to display DHCPv6 Snooping configurations.

Syntax

```
show ipv6 dhcp snooping
```

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays DHCPv6 Snooping configurations.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping
DHCPv6 snooping status                : ENABLE
DHCPv6 snooping database write-delay time : 0 seconds
DHCPv6 snooping binding-delay time     : 0 seconds
DHCPv6 snooping option18/37 status     : DISABLE
DHCPv6 snooping link detection         : DISABLE
Interface          Trusted      Filter DHCPv6
-----
-----
```

GigabitEthernet 0/1	YES	DISABLE
---------------------	-----	---------

Table 1-1 Output Fields of the show ipv6 dhcp snooping Command

Field	Description
DHCPv6 snooping status	Indicates whether DHCPv6 snooping is enabled globally
DHCPv6 snooping database write-delay time	Interval for writing data to a flash memory.
DHCPv6 snooping binding-delay time	Delayed time for adding dynamically generated binding entries to the hardware filtering table.
DHCPv6 snooping option 18/37 status	Indicates whether Option 18 or 37 is added to DHCPv6 request packets.
DHCPv6 snooping link detection	Indicates whether dynamically bound entries on a linkdown interface are cleared.
Interface	Interface name
Trusted	Indicates whether an interface is a trusted port.
Filter DHCP	Indicates whether DHCPv6 request packet filtering is configured.

Notifications

N/A

Platform Description

N/A

1.17 show ipv6 dhcp snooping vlan**Function**

Run the **show ipv6 dhcp snooping vlan** command to display VLANs to which DHCPv6 Snooping does not take effect.

Syntax

```
show ipv6 dhcp snooping vlan
```

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays VLANs to which DHCPv6 Snooping does not take effect.

```

Hostname> enable
Hostname# show ipv6 dhcp snooping vlan
VLAN Name          Closed
2    VLAN 2          YES

```

Table 1-1 Output Fields of the show ipv6 dhcp snooping vlan Command

Field	Description
VLAN	VLAN ID.
Name	VLAN name.
Closed	Indicates whether DHCPv6 Snooping takes effect.

Notifications

N/A

Platform Description

N/A

1.18 show ipv6 dhcp snooping binding**Function**

Run the **show ipv6 dhcp snooping binding** command to display dynamic user information in the DHCPv6 Snooping binding database.

Syntax

```
show ipv6 dhcp snooping binding [ ipv6-address ] [ mac-address ] [ vlan vlan-id ] [ interface interface-type
interface-number ]
```

Parameter Description

ipv6-address: IPv6 address for which binding information is displayed.

mac-address: MAC address for which binding information is displayed.

vlan *vlan-id*: Specifies the VLAN for which binding information is displayed.

interface *interface-type interface-number*: Specifies the interface for which binding information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays dynamic user information in the DHCPv6 Snooping binding database.

```

Hostname> enable
Hostname# show ipv6 dhcp snooping binding
Total number of bindings: 1
NO.      MAC Address          IPv6 Address          Lease(sec)
VLAN    Interface
1        00d0.f801.0101         2001::10              42368
2        GigabitEthernet 0/1

```

Table 1-1 Output Fields of the show ipv6 dhcp snooping binding Command

Field	Description
Total number of bindings	Number of bindings in the DHCPv6 Snooping binding database
No.	Record number
MAC Address	MAC address of a user
IPv6 Address	IPv6 address of a user
Lease(sec)	Lease time of a record
VLAN	VLAN of a user
Interface	Wired access interface of a user

Notifications

N/A

Platform Description

N/A

1.19 show ipv6 dhcp snooping prefix**Function**

Run the **show ipv6 dhcp snooping prefix** command to display user information in the DHCPv6 Snooping prefix database.

Syntax

```
show ipv6 dhcp snooping prefix [ ipv6-address ] [ mac-address ] [ vlan vlan-id ] [ interface interface-type
interface-number ]
```

Parameter Description

ipv6-address: IPv6 address for which user information is displayed.

mac-address: MAC address for which user information is displayed.

vlan *vlan-id*: Specifies the VLAN for which user information in the prefix database is displayed.

interface *interface-type interface-number*: Specifies the interface for which user information in the prefix database is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays user information in the DHCPv6 Snooping prefix database.

```
Hostname> enable
Hostname# show ipv6 dhcp snooping prefix
Total number of bindings: 1
NO.    MAC Address          IPv6 Address                Lease (sec)
VLAN   Interface
1      00d0.f801.0101         2001:2002::/64             42368      2
GigabitEthernet 0/1
```

Table 1-1Output Fields of the show ipv6 dhcp snooping prefix Command

Field	Description
Total number of bindings	Number of bindings in the DHCPv6 Snooping prefix database
No.	Record number
MAC Address	MAC address of a user
IPv6 Address	IPv6 address of a user
Lease(sec)	Lease time of a record
VLAN	VLAN of a user
Interface	Access interface of a user

Notifications

N/A

Platform Description

N/A

1.20 show ipv6 dhcp snooping statistics**Function**

Run the **show ipv6 dhcp snooping statistics** command to display statistics about DHCPv6 packets filtered due to DHCPv6 Snooping.

Syntax

```
show ipv6 dhcp snooping statistics
```

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays statistics about DHCPv6 packets filtered due to DHCPv6 Snooping.

```

Hostname> enable
Hostname# show ipv6 dhcp snooping statistics
Packets processed by DHCPv6 snooping = 0
Packets dropped because
Received on untrusted ports           = 0
Relay forward                         = 0
No binding entry                      = 0
Binding fail                          = 0
Unknown packet                       = 0
Unknown output interface              = 0
No enough memory                     = 0
Admin filter DHCPv6 packet           = 0

```

Table 1-1 Output Fields of the show ipv6 dhcp snooping statistics Command

Field	Description
Received on	Server response packets discarded on untrusted ports.

untrusted ports	
Relay forward	Discarded packets that are relayed once.
No binding entry	When the binding entry of a RELEASE or DECLINE packet does not exist or is incorrect, the packet is discarded.
Binding fail	Packets discarded because entry binding fails. Generally, entry binding fails because hardware resources are insufficient.
Unknown packet	Unknown DHCPv6 packets.
Unknown output interface	Packets sent from unknown outbound interface because the MAC address cannot be found or the interface is not set as a trusted port.
No enough memory	Packets discarded due to insufficient memory resources.
Admin filter-dhcpv6-pkt	DHCPv6 packets filtered due to the administrator configuration, mainly packets filtered after the ipv6 dhcp snooping filter-dhcp-pkt command is configured.

Notifications

N/A

Platform Description

N/A

1.21 show ipv6 dhcp snooping packet**Function**

Run the **show ipv6 dhcp snooping packet** command to display statistics about packets related to the DHCPv6 Snooping function.

Syntax

```
show ipv6 dhcp snooping packet
```

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays statistics about packets related to the DHCPv6 Snooping function.

```

Hostname> enable
Hostname# show ipv6 dhcp snooping packet
Total port num:3 (port which process none packet doesn't display)
Interface      Total Recv  Total Drop  Total Fwd  SOLICIT(Drop/Fwd)
ADVERTISE (Drop/Fwd)  REQUEST (Drop/Fwd)  REPLY (Drop/Fwd)
-----None
Gi0/1          1           0           1           0/1
0/0            0/0
Gi0/17        2           0           2           0/2
0/0            0/0
Lc0           1           0           1           0/0
0/1            0/0
  
```

Table 1-1 Output Fields of the show ipv6 dhcp snooping packet Command

Field	Description
Total port num	Number of interfaces with DHCPv6 Snooping packet records
Interface	Interface name
Total Recv	Total number of received packets from the specified interface
Total Drop	Total number of discarded packets from the specified interface
Total Fwd	Total number of forwarded packets from the specified interface
SOLICIT (Drop/Fwd)	Total number of discarded and forwarded SOLICIT packets from the specified interface
ADVERTISE (Drop/Fwd)	Total number of discarded and forwarded ADVERTISE packets from the specified interface
REQUEST (Drop/Fwd)	Total number of discarded and forwarded REQUEST packets from the specified interface
REPLY (Drop/Fwd)	Total number of discarded and forwarded REPLY packets from the specified interface

Notifications

N/A

Platform Description

N/A