1 DHCP Snooping Commands

Command	Function
clear ip dhcp snooping binding	Clear all dynamic users in the Dynamic Host Configuration Protocol (DHCP) snooping binding database.
ip dhcp snooping	Enable DHCP Snooping globally.
ip dhcp snooping bootp-bind	Enable DHCP Snooping to support Bootstrap Protocol (BOOTP) binding.
ip dhcp snooping check-giaddr	Enable DHCP Snooping to support relay request packet processing.
ip dhcp snooping database write-delay	Write all dynamic user information in the DHCP Snooping binding database to a flash memory at a scheduled time.
ip dhcp snooping database write-to-flash	Write dynamic user information in the DHCP Snooping binding database to flash in real time.
ip dhcp snooping information option	Add Option 82 to DHCP request packets.
ip dhcp snooping information option format remote-id	Set the Remote ID sub-option to a user-defined string or the host name when Option 82 is in extended mode.
ip dhcp snooping monitor	Enable DHCP Snooping monitoring globally.
ip dhcp snooping station-move aging	Enable DHCP Snooping to fast age terminal migration entries.
ip dhcp snooping station-move permit	Enable DHCP Snooping to support binding entry migration.
ip dhcp snooping suppression	Configure an interface in the suppression state so as to discard all DHCP packets sent to the interface.
ip dhcp snooping trust	Configure an interface as a DHCP Snooping trusted port.
ip dhcp snooping verify mac-address	Enable source MAC address verification.
ip dhcp snooping vlan	Enable DHCP Snooping on a specified VLAN.

ip dhcp snooping vlan information option change-vlan-to vlan	Set the VLAN filed in Circuit ID of Option 82 in extended mode to a specified VLAN.
ip dhcp snooping vlan information option format-type circuit-id string	Set Circuit ID to user-defined content for forwarding when Option 82 is in extended mode.
ip dhcp snooping vlan max-user	Configure the maximum number of users bound to a VLAN.
renew ip dhcp snooping database	Import information in the current backup file to the DHCP Snooping binding database.
show ip dhcp snooping	Display the DHCP Snooping configurations.
show ip dhcp snooping binding	Display user information in the DHCP Snooping binding database.

1.1 clear ip dhcp snooping binding

Function

Run the **clear ip dhcp snooping binding** command to clear all dynamic users in the Dynamic Host Configuration Protocol (DHCP) snooping binding database.

Syntax

clear ip dhcp snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*]

Parameter Description

ip-address: IP address of a user.

mac-address: Media Access Control (MAC) address of a user.

vlan-id: Virtual local area network (VLAN) ID of a user.

interface-type interface-number: Interface of a user.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

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

Examples

The following example clears all dynamic users in the DHCP Snooping binding database.

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

Notifications

N/A

Platform Description

N/A

1.2 ip dhcp snooping

Function

Run the **ip dhcp snooping** command to enable DHCP Snooping globally.

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

DHCP Snooping is disabled globally by default.

Syntax

ip dhcp snooping

no ip dhcp snooping

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After DHCP Snooping is enabled globally, you can run the **show ip dhcp snooping** command to check whether this function is enabled.

Examples

The following example enables DHCP Snooping globally.

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

Notifications

When this command is run to enable DHCP Snooping after DHCP Snooping monitoring is enabled globally, the following notification will be displayed:

```
% Failed to execute command, because of "Conflict with DHCP snooping monitor".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip dhcp snooping bootp-bind

Function

Run the **ip dhcp snooping bootp-bind** command to enable DHCP Snooping to support Bootstrap Protocol (BOOTP) binding.

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

DHCP Snooping does not support BOOTP binding by default.

Syntax

ip dhcp snooping bootp-bind

no ip dhcp snooping bootp-bind

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After being enabled, DHCP Snooping snoops and forwards only BOOTP packets by default. After a BOOTP client successfully applies for an IP address, DHCP Snooping adds the BOOTP user to the static binding database.

Examples

The following example enables DHCP Snooping to support BOOTP binding.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping bootp-bind
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip dhcp snooping check-giaddr

Function

Run the **ip dhcp snooping check-giaddr** command to enable DHCP Snooping to support relay request packet processing.

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

DHCP Snooping does not support relay request packet processing by default.

Syntax

ip dhcp snooping check-giaddr

no ip dhcp snooping check-giaddr

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this function is enabled, services (IP Source Guard and Dot1x authentication) using DHCP Snooping binding entries generated based on relay requests cannot be deployed. Otherwise, users fail to access the Internet.

After this function is enabled, the **ip dhcp snooping verify mac-address** command cannot be configured. Otherwise, DHCP relay request packets are discarded, and users fail to obtain addresses.

Examples

The following example enables DHCP Snooping to support relay request packet processing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping check-giaddr
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.5 ip dhcp snooping database write-delay

Function

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

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

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

Syntax

ip dhcp snooping database write-delay *time*

no ip 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 DHCP Snooping binding database to a flash memory at a scheduled time. This prevents user information loss after the device restarts, and there is no need to re-obtain IP addresses to restore communication.

Note

A high saving frequency reduces the lifespan of the flash.

Examples

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

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

Notifications

N/A

Common Errors

The configured period exceeds the limit.

Platform Description

N/A

Related Commands

N/A

1.6 ip dhcp snooping database write-to-flash

Function

Run the **ip dhcp snooping database write-to-flash** command to write dynamic user information in the DHCP Snooping binding database to flash in real time.

Syntax

ip dhcp snooping database write-to-flash

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Wireless user information is not written to flash.

If a device is upgraded from a non-QinQ version to a QinQ version (or vice versa), binding entries cannot be restored because the two versions correspond to different flashes.

Examples

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

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping database write-to-flash
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 ip dhcp snooping information option

Function

Run the **ip dhcp snooping information option** command to add Option 82 to DHCP request packets.

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

Option 82 is not added to DHCP request packets by default.

Syntax

ip dhcp snooping information option [**standard-format** | **user-defined**]

no ip dhcp snooping information option [**standard-format** | **user-defined**]

Parameter Description

standard-format: Uses the standard format for Option 82.

user-defined: Uses the user-defined format for Option 82.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to add Option 82 to DHCP request packets so that a DHCP server assigns addresses based on Option 82.

When enabled, Option 82 is in extended mode by default.

Caution

Option 82 for DHCP Snooping is exclusive to that for DHCP Relay.

Examples

The following example adds Option 82 to DHCP request packets.

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

Notifications

N/A

Common Errors

Option 82 for DHCP Snooping and that for DHCP Relay are enabled at the same time. As a result, Option 82 in the DHCP packets is incorrect.

Platform Description

N/A

Related Commands

N/A

1.8 ip dhcp snooping information option format remote-id

Function

Run the **ip 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 82 is in extended mode.

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

Remote ID in Option 82 is not set to a user-defined string or host name by default.

Syntax

ip dhcp snooping information option format remote-id { **string** *ascii-string* | **hostname** }

no ip dhcp snooping information option format remote-id

Parameter Description

string *ascii-string*: Sets **Remote ID** in Option 82 to a user-defined string.

hostname: Sets **Remote ID** in Option 82 to the host name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When DHCP Option 82 is enabled in extended mode, this command is used to customize the content of **Remote ID** in Option 82.

Examples

The following example sets **Remote ID** in Option 82 to the host name.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip 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

N/A

1.9 ip dhcp snooping monitor

Function

Run the **ip dhcp snooping monitor** command to enable DHCP Snooping monitoring globally.

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

DHCP Snooping monitoring is disabled globally by default.

Syntax

ip dhcp snooping monitor

no ip dhcp snooping monitor

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After the DHCP Snooping monitoring function is enabled, DHCP Snooping only copies DHCP packets and generates binding entries based on the interaction status, but does not check the validity of the packets.

The DHCP Snooping monitoring and DHCP Snooping functions are mutually exclusive.

After the DHCP Snooping monitoring function is enabled, if the VLAN field in the **show ip dhcp snooping binding** command is set to **0**, VLAN information is not carried in binding entries generated for routed ports.

Examples

The following example enables DHCP Snooping monitoring globally.

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

Notifications

When DHCP Snooping monitoring is configured after DHCP Snooping is enabled globally, the following notification will be displayed:

```
% Failed to execute command, because of "Conflict with DHCP snooping".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 ip dhcp snooping station-move aging

Function

Run the **ip dhcp snooping station-move aging** command to enable DHCP Snooping to fast age terminal migration entries.

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

Fast aging of client migration entries is enabled for DHCP Snooping by default.

Syntax

ip dhcp snooping station-move aging

no ip dhcp snooping station-move aging

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When a terminal is migrated between different sub VLANs of the same super VLAN and a binding entry is generated in the new sub VLAN, this command is used to enable DHCP Snooping to fast age binding entries in other sub VLANs.

Examples

The following example disables fast aging of terminal migration entries.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no ip dhcp snooping station-move aging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 ip dhcp snooping station-move permit

Function

Run the **ip dhcp snooping station-move permit** command to enable DHCP Snooping to support binding entry migration.

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

DHCP Snooping does not support binding entry migration by default.

Syntax

ip dhcp snooping station-move permit

no ip dhcp snooping station-move permit

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When no DHCP request for an IP address is initiated after terminal migration, this command is used to enable DHCP Snooping to find the latest binding entries in the super VLAN based on the target sub VLAN and generates binding entries of the target sub VLAN.

Examples

The following example enables DHCP Snooping to support binding entry migration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping station-move permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 ip dhcp snooping suppression

Function

Run the **ip dhcp snooping suppression** command to configure an interface in the suppression state so as to discard all DHCP packets sent to the interface.

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

No interface is configured in the suppression state by default.

Syntax

ip dhcp snooping suppression

no ip dhcp snooping suppression

Parameter Description

N/A

Command Modes

Interface configuration mode

Wireless security configuration mode

Default Level

14

Usage Guidelines

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

This command can be configured only on L2 switching ports or aggregation ports (APs).

Examples

The following example configures GigabitEthernet 0/1 in the suppression state.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping suppression
```

Notifications

When this command is configured on a DHCP 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 for wired access, 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

1.13 ip dhcp snooping trust

Function

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

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

All interfaces are DHCP Snooping untrusted ports by default.

Syntax

ip dhcp snooping trust

no ip 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 DHCP servers as trusted ports. DHCP 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, or encapsulation sub-interfaces.

Caution

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

Examples

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

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip 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, 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

1.14 ip dhcp snooping verify mac-address

Function

Run the **ip dhcp snooping verify mac-address** command to enable source MAC address verification.

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

Source MAC address verification is disabled by default.

Syntax

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After source MAC address verification is enabled, the MAC addresses in link layer headers and the **CLIENT MAC** fields in DHCP request packets from untrusted ports are checked for consistence. If the verification fails, packets are discarded.

Examples

The following example enables source MAC address verification.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip dhcp snooping verify mac-address
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 ip dhcp snooping vlan

Function

Run the **ip dhcp snooping vlan** command to enable DHCP Snooping on a specified VLAN.

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

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

Syntax

ip dhcp snooping vlan { *vlan-range* | { *vlan-min* [*vlan-max*] } }

no ip dhcp snooping vlan { *vlan-range* | *vlan-min* [*vlan-max*] }

Parameter Description

vlan-range: Range of VLANs to which DHCP 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 which DHCP Snooping takes effect. The value range is from 1 to 4094.

vlan-max: Maximum ID of a VLAN to which DHCP 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 DHCP Snooping for a specified VLAN. This function takes effect only when DHCP Snooping is enabled globally.

Examples

The following example enables DHCP Snooping for VLAN 1000.

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

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

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip 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

1.16 ip dhcp snooping vlan information option change-vlan-to vlan

Function

Run the **ip dhcp snooping vlan information option change-vlan-to vlan** command to set the VLAN filed in **Circuit ID** of Option 82 in extended mode to a specified VLAN.

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

When Option 82 is in extended mode, the VLAN in **Circuit ID** is not configured as the specified VLAN by default.

Syntax

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

no ip dhcp snooping vlan *vlan-id* **information option**

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 DHCP Option 82 is enabled in extended mode, this command is used to change the value of the VLAN field in **the Circuit ID** of Option 82 to a specified VLAN.

Examples

The following example changes VLAN 4094 in **Circuit ID** of Option 82 to VLAN 4093 when Option 82 is added to DHCP request packets.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ip dhcp snooping vlan information option format-type circuit-id string

Function

Run the **ip dhcp snooping vlan information option format-type circuit-id string** command to set **Circuit ID** to user-defined content for forwarding when Option 82 is in extended mode.

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

When Option 82 is in extended mode, **Circuit ID** is not set to user-defined content for forwarding by default.

Syntax

ip dhcp snooping vlan *vlan-id* **information option format-type circuit-id string** *ascii-string*

no ip dhcp snooping vlan *vlan-id* **information option**

Parameter Description

vlan-id: ID of the VLAN where DHCP request packets are from.

ascii-string: User-defined **Circuit 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 DHCP Option 82 is enabled in extended mode, this command is used to customize **Circuit ID** in Option 82.

Examples

The following example sets **Circuit ID** of Option 82 to port-name when Option 82 is added to DHCP request packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information
option format-type circuit-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 "Circuit-ID string must be 3 to 63
characters".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 ip dhcp snooping vlan max-user

Function

Run the **ip dhcp snooping vlan max-user** command to configure the maximum number of users bound to a VLAN.

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

The maximum number of users bound to a VLAN is not configured by default.

Syntax

ip dhcp snooping vlan *vlan-range* **max-user** *user-number*

no ip dhcp snooping vlan *vlan-range* **max-user** *user-number*

Parameter Description

vlan-range: Range of VLANs to which DHCP Snooping takes effect.

user-number: Maximum number of allowed users. The value range is from 1 to 26624.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the maximum number of users bound based on the interface and VLAN, so as to prevent forge DHCP packets in accordance with the network topology.

Examples

The following example binds a maximum of 30 users to VLANs 1 to 10 and VLAN 20 on interface 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user
30
```

Notifications

When an interface from a specified VLAN is a DHCP Snooping trusted port, the following notification will be displayed:

```
% Failed to execute command, because of "Security configuration conflict in
interface GigabitEthernet 0/1".
```

When the number of users bound to a VLAN on a specified interface exceeds the maximum number of allowed users configured in the command, the following notification will be displayed:

```
% Failed to execute command, because of "New max address number little more than
the current".
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 renew ip dhcp snooping database

Function

Run the **renew ip dhcp snooping database** command to import information in the current backup file to the DHCP Snooping binding database.

Syntax

renew ip dhcp snooping database

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

This command is used to import information in the current backup file to the DHCP Snooping binding database.

Note

- 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 the current backup file to the DHCP Snooping binding database.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 show ip dhcp snooping

Function

Run the **show ip dhcp snooping** command to display the DHCP Snooping configurations.

Syntax

show ip 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 DHCP Snooping configurations.

```
Hostname> enable
Hostname# show ip dhcp snooping
Switch DHCP snooping status                    :   ENABLE
DHCP snooping verify hardware address status    :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE
Interface                                           Trusted             Rate
limit(pps)
GigabitEthernet 0/1                                 YES                 unlimited
Default                                             No
```

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

Field	Description
Switch DHCP snooping status	Indicates whether DHCP Snooping is enabled globally.
DHCP snooping verify hardware address status	Status of the switch for verifying the source MAC address in DHCP Snooping packets.
DHCP snooping database write-delay time	Interval for writing data to a backup file.
DHCP snooping option 82 status	Indicates whether Option 82 is added to DHCP request packets.
DHCP snooping Support Bootp bind	Indicates whether to enable DHCP Snooping to support BOOTP

status	binding.
Interface	Interface name.
Trusted	Indicates whether an interface is a trusted port.
Rate limit	Rate limit for DHCP packets on an interface.

Notifications

N/A

Platform Description

N/A

1.21 show ip dhcp snooping binding

Function

Run the **show ip dhcp snooping binding** command to display user information in the DHCP Snooping binding database.

Syntax

show ip dhcp snooping binding

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 user information in the DHCP Snooping binding database.

```
Hostname> enable
Hostname# show ip dhcp snooping binding
Total number of bindings: 1
NO.   MACADDRESS         IPADDRESS       LEASE(SEC)   TYPE          VLAN
INTERFACE
1     0000.0000.0001     1.1.1.1         78128        DHCP-Snooping 1
GigabitEthernet 0/1
```

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

Field	Description
Total number of bindings	Current number of bindings in the DHCP Snooping binding database.
No.	Record number.
MACADDRESS	MAC address of a user.
IPADDRESS	IP address of a user.
LEASE (SEC)	Lease time of a record.
TYPE	Record type.
VLAN	VLAN of a user.
INNER-VLAN	ID of the inner VLAN of a user. This field is applicable to products that support QinQ VLAN tag termination.
INTERFACE	Interface to which a user's terminal connects.

Notifications

N/A

Platform Description

N/A