

## DHCP-Snooping Configuration Commands

# Table of Contents

Chapter 1 DHCP-Relay Snooping Configuration Commands .....	1
1.1.1 ip dhcp-relay snooping .....	1
1.1.2 ip dhcp-relay snooping vlan .....	2
1.1.3 ip dhcp-relay snooping vlan <i>vlan_id</i> max-client .....	3
1.1.4 ip dhcp-relay snooping database-agent .....	3
1.1.5 ip dhcp-relay snooping db-file .....	4
1.1.6 ip dhcp-relay snooping write-time .....	5
1.1.7 ip dhcp-relay snooping write-immediately .....	5
1.1.8 ip dhcp-relay snooping log .....	6
1.1.9 ip dhcp-relay snooping rapid-refresh-bind .....	7
1.1.10 dhcp-relay snooping information option .....	7
1.1.11 ip verify source vlan .....	8
1.1.12 ip arp inspection vlan .....	9
1.1.13 ip source binding .....	10
1.1.14 arp inspection trust .....	11
1.1.15 dhcp snooping trust .....	11
1.1.16 dhcp snooping deny .....	12
1.1.17 dhcp snooping information circuit-id .....	12
1.1.18 dhcp snooping information remote-id string .....	13
1.1.19 dhcp snooping information vendor-specific .....	14
1.1.20 dhcp snooping information append .....	15
1.1.21 dhcp snooping information drop .....	16
1.1.22 ip-source trust .....	17
1.1.23 show ip dhcp-relay snooping .....	18
1.1.24 show ip dhcp-relay snooping binding .....	18
1.1.25 debug ip dhcp-relay snooping .....	19
1.1.26 debug ip dhcp-relay event .....	19
1.1.27 debug ip dhcp-relay binding .....	20

## Chapter 1 DHCP-Relay Snooping Configuration Commands

The DHCP-relay snooping configuration commands include:

- ip dhcp-relay snooping
- ip dhcp-relay snooping vlan
- ip dhcp-relay snooping database-agent
- ip dhcp-relay snooping db-file
- ip verify source vlan
- ip arp inspection vlan
- ip source binding
- arp inspection trust
- dhcp snooping trust
- ip-source trust
- show ip dhcp-relay snooping
- show ip dhcp-relay snooping binding
- debug ip dhcp-relay snooping
- debug ip dhcp-relay event
- debug ip dhcp-relay binding

### 1.1.1 ip dhcp-relay snooping

#### Syntax

**ip dhcp-relay snooping**

**no ip dhcp-relay snooping**

To enable or disable the DHCP-relay snooping function in a VLAN, run **ip dhcp-relay snooping**. To resume the corresponding default settings, run **no dhcp-relay snooping**.

#### Parameter

None

## Default

The dhcp-relay snooping function is disabled by default.

## Usage Guidelines

None

## Example

The following example shows how to enable the DHCP-relay snooping function:

```
Switch_config#ip dhcp-relay snooping
Switch_config#
```

### 1.1.2 ip dhcp-relay snooping vlan

## Syntax

**ip dhcp-relay snooping vlan *vlan\_id***

**no ip dhcp-relay snooping vlan *vlan\_id***

## Parameter

Parameter	Description
<i>vlan id</i>	ID of a VLAN Range: 1-4094

## Default

None

## Usage Guidelines

This command is used to configure the VLAN of DHCP snooping.

## Example

The following example shows how to conduct the snooping inspection to the DHCP packets in VLAN2.

```
switch(config)# ip dhcp-relay snooping vlan 2
switch(config)#
```

### 1.1.3 ip dhcp-relay snooping vlan *vlan\_id* max-client

#### Syntax

**ip dhcp-relay snooping vlan *vlan\_id* max-client *number***

**no ip dhcp-relay snooping vlan *vlan\_id* max-client**

#### Parameter

Parameter	Description
<i>vlan_id</i>	VLAN id. The value ranges from 1 to 4094.
<i>number</i>	The max user number: 0~65535

#### Default

The max user number is 65535 by default.

#### Usage Guidelines

You can use this command to set the maximum users in a VLAN of DHCP snooping. During this settings, the principle “first come and first be distributed” will be followed. When the number of users in the VLAN reaches the maximum value, new clients are then forbidden to distribute.

#### Example

The following example shows how to set snooping detection for DHCP packets on VLAN 2 and the number of maximum users is 3.

```
Switch_config#ip dhcp-relay snooping vlan 2 max-client 3
Switch_config#
```

### 1.1.4 ip dhcp-relay snooping database-agent

#### Syntax

**ip dhcp-relay snooping database-agent *A.B.C.D***

**no ip dhcp-relay snooping database-agent *A.B.C.D***

To configure the TFTP server for backing up DHCP-snooping binding, run **ip dhcp-relay snooping database-agent *A.B.C.D***.

#### Parameter

Parameter	Description
-----------	-------------

A.B.C.D	Stands for the IP address of the TFTP server.
---------	---

## Default

There is no standby servers by default.

## Usage Guidelines

If the address of the TFTP server is not configured, the binding backup is not conducted.

## Example

The following example shows how to set the address of a server of backing up DHCP snooping binding to 192.168.1.1.

```
Switch_config#ip dhcp-relay snooping database-agent 192.168.1.1
Switch_config#
```

### 1.1.5 ip dhcp-relay snooping db-file

## Syntax

**ip dhcp-relay snooping db-file *name* [*timestamp*]**

**no ip dhcp-relay snooping db-file [*timestamp*]**

## Parameter

Parameter	Description
<i>Name</i>	File name which is saved during DHCP snooping binding backup.
<i>timestamp</i>	File name which is saved with timesatmp.

## Default

There is no file.

## Usage Guidelines

If the file name is not configured, the binding backup is not conducted.

## Example

The following example shows how to set the file name of binding backup to **dhcp\_binding.txt**.

```
switch(config)# ip dhcp-relay snooping db-file dhcp_binding.txt  
switch(config)#
```

### 1.1.6 ip dhcp-relay snooping write-time

#### Syntax

**ip dhcp-relay snooping write-time** *num*

**no ip dhcp-relay snooping write-time**

#### Parameter

Parameter	Description
<i>Num</i>	Stands for the interval of backing up the DHCP snooping binding.

#### Default

The Default of the interval is 30 minutes.

#### Usage Guidelines

The binding update will be checked during interval configuration. If the binding is updated, the binding information need be backed up.

#### Example

The following example shows how to set the interval of backing up the binding to 60 minutes.

```
switch(config)# ip dhcp-relay snooping write 60  
switch(config)#
```

### 1.1.7 ip dhcp-relay snooping write-immediately

#### Syntax

**ip dhcp-relay snooping write-immediately**

**no ip dhcp-relay snooping write-immediately**

#### Parameter

None

## Default

None

## Usage Guidelines

The command enables the item update is immediately written into the binding item database. It is recommended that do not enable the function when there are many items.

## Example

The following example shows how to back up the binding item immediately after its configuration item is updated.

```
Switch_config#ip dhcp-relay snooping write-immediately
Switch_config#
```

### 1.1.8 ip dhcp-relay snooping log

## Syntax

```
ip dhcp-relay snooping log
no ip dhcp-relay snooping log
```

## Parameter

None

## Default

None

## Usage Guidelines

After this function is enabled, if there are any packet of dhcp server in the untrust port, the syslog indicates that there is an illegal dhcp server.

## Example

The following example shows how to enable the log function of dhcp snooping.

```
Switch_config#ip dhcp-relay snooping log
Switch_config#
```



### 1.1.9 ip dhcp-relay snooping rapid-refresh-bind

#### Syntax

**ip dhcp-relay snooping rapid-refresh-bind**

**no ip dhcp-relay snooping rapid-refresh-bind**

To enable dhcp snooping rapid refresh item function, run the first one of the above commands. To return to the default setting, use the no form of this command.

#### Parameter

None

#### Default

None

#### Usage Guidelines

After this function is enabled, the DHCP attack of fake MAC will be closed; when the client is allowed to change the access port, the IP address can be directly acquired without waiting for the expiration of the IP lease.

After this function is enabled, if the client changes its access port, the device with snooping enabled will take it as the dhcp packet attack of the fake mac and drop the dhcp packets.

#### Example

None

### 1.1.10 dhcp-relay snooping information option

#### Syntax

**ip dhcp-relay snooping information option [ format snmp-ifindex | manual | cm-type | hn-type [host] | hw-type ]**

**no ip dhcp-relay snooping information option [ format snmp-ifindex | manual | cm-type | hn-type [host] | hw-type ]**

#### Parameter

Parameter	Description
<b>format</b>	Fills in option 82 in <b>SNMP ifindex</b> mode (optional).

<b>snmp-ifindex</b>	
<b>format manual</b>	Fills in option 82 manually (optional).
<b>format cm-type</b>	Fills in option 82 in <b>cm-type</b> mode (optional).
<b>Format      hn-type</b> <b>[host]</b>	Fills in option 82 in <b>cisco</b> mode (optional). Host stands for the main switch.
<b>format hw-type</b>	Fills in option 82 in <b>hw-type</b> mode (optional).

## Default

Option 82 will not be added to or removed from the report by default.

## Usage Guidelines

This command is used to set whether DHCP option82 can be handled when a switch is conducting DHCP snooping. If **format snmp-ifindex** is designated, Use the **SNMP ifindex** mode to fill in option 82; otherwise, fill in option 82 according to RFC3046.

## Example

The following example shows how to fill in option 82 in **SNMP ifindex** mode:

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping information option format snmp-ifindex
```

The following example shows how to fill in option 82 in **manual** mode:

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping vlan [WORD]    //[WORD] is the vlan name that
means need for enable snooping function
```

```
Switch_config# ip dhcp-relay snooping information option format manual
```

### 1.1.11 ip verify source vlan

## Syntax

```
ip verify source vlan vlanid
```

```
no ip verify source vlan vlanid
```

## Parameter

Parameter	Description
<i>vlan id</i>	ID of a VLAN Range: 1-4094

## Default

None

## Usage Guidelines

This command is used to configure a VLAN for monitoring the source IP address. The “no” form of this command is used to cancel this VLAN. If the source IP and source MAC of the IP packet are not the legal client address assigned by the dhcp server monitored by dhcp snooping, then such a packet is regarded as an illegal packet in the vlan with IP source address monitoring enabled, and the packet is discarded Text.

## Example

The following example shows how to conduct source IP address monitoring to the packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
switch(config)# ip verify source vlan 2
```

```
switch(config)#
```

## 1.1.12 ip arp inspection vlan

## Syntax

**ip arp inspection vlan *vlanid***

**no ip arp inspection vlan *vlanid***

## Parameter

Parameter	Description
<i>vlan id</i>	Queries the time of the timer. Range: 1-4094

## Default

None

## Usage Guidelines

This command is used to configure a VLAN for monitoring the source address of the ARP packet. The “no” form of this command is used to cancel this VLAN. Under the VLAN that enables ARP packet source address monitoring, ARP packets with SIP and

SMAC corresponding to the IP address and mac address assigned by the dhcp server to the client are discarded.

### Example

The following example shows how to conduct source address monitoring to the ARP packets from all physical interfaces (except trusted interfaces) in VLAN2.

```
Switch_config#ip arp inspection vlan 2
Switch_config#
```

### 1.1.13 ip source binding

#### Syntax

**ip source binding** *xx:xx:xx:xx:xx:xx A.B.C.D interface name vlan vlan-id*

**no ip source binding** *xx:xx:xx:xx:xx:xx A.B.C.D vlan vlan-id*

To add MAC-to-IP binding to an interface, run **ip source binding** *xx-xx-xx-xx-xx-xx A.B.C.D interface name*.

#### Parameter

Parameter	Description
<i>xx-xx-xx-xx-xx-xx</i>	MAC address.
<i>A.B.C.D</i>	IP address
<i>Name</i>	Name of the interface
<i>vlan-id</i>	vlan id number

#### Default

None

#### Usage Guidelines

None

### Example

The following example shows how to bind MAC address **08:00:3e:00:00:01** to IP address **192.168.1.2** on interface GigaEthernet0/1.

```
Switch_config#ip source binding 08:00:3e:00:00:01 192.168.1.2 interface GigaEthernet0/1
Switch_config#
```

### 1.1.14 arp inspection trust

#### Syntax

**arp inspection trust**

**no arp inspection trust**

#### Parameter

None

#### Default

The interfaces are distrusted ones by default.

#### Usage Guidelines

The ARP monitoring is not conducted to the ARP-trusted interface. The “no” form of this command is used to configure the Default of this interface.

#### Example

The following example shows how to set interface GigaEthernet0/1 to an ARP-trusted interface.

```
Switch_config_g0/1#arp inspection trust
```

### 1.1.15 dhcp snooping trust

#### Syntax

**dhcp snooping trust**

**no dhcp snooping trust**

#### Parameter

None

#### Default

The default interface is a distrusted one.

## Usage Guidelines

DHCP snooping is not conducted to the DHCP-trusted interface. The “no” form of this command is used to resume the Default of this interface.

## Example

The following example shows how to set interface GigaEthernet0/1 to a DHCP-trusted interface.

```
Switch_config_g0/1#dhcp snooping trust
```

### 1.1.16 dhcp snooping deny

#### Syntax

**dhcp snooping deny**

**no dhcp snooping deny**

#### Parameter

None

#### Default

DHCP snooping is allowed on the default interface.

## Usage Guidelines

After this command is configured, DHCP snooping trust, IP-sourcetrust and ARP inspection trust are automatically enabled. The “no” form of this command is used to configure the Default of this interface.

## Example

The following example shows how to disable DHCP snooping on interface GigaEthernet0/1.

```
Switch_config_g0/1#dhcp snooping deny
```

### 1.1.17 dhcp snooping information circuit-id

#### Syntax

**dhcp snooping information circuit-id {string *STRING* | hex *xx-xx-xx-xx-xx-xx*}**

## Parameter

Parameter	Description
<b>string</b> <i>STRING</i>	Stands for the character string carried by the sub-option of option82 circuit-id.
<b>hex</b> <i>xx-xx-xx-xx-xx-xx</i>	Stands for the Hex system carried by option82 circuit-id.

## Default

None

## Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (the switch of manually set option82 need be enabled. See the command, **ip dhcp-relay snooping information option format manual**)

## Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3.

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3#dhcp snooping information circuit-id string group1
```

## 1.1.18 dhcp snooping information remote-id string

## Syntax

**dhcp snooping information remote-id {string *STRING* | hex *xx-xx-xx-xx-xx-xx*}**

## Parameter

Parameter	Description
<b>string</b> <i>STRING</i>	Stands for the character string carried by the sub-option of option82 remote-id.
<b>hex</b> <i>xx-xx-xx-xx-xx-xx</i>	Stands for the Hex system carried by option82 remote-id.

## Default

None

## Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (The switch of manually set option82 need be enabled. See the command, **ip dhcp-relay snooping information option format manual**)

## Example

The following example shows how to set option82 to group1 manually on interface g0/3, which belongs to interface g0/3.

```
Switch_config# ip dhcp-relay snooping
```

```
Switch_config# ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3# dhcp snooping information remote-id string group1
```

### 1.1.19 dhcp snooping information vendor-specific

## Syntax

```
dhcp snooping information vendor-specific { string STRING | hex  
xx-xx-xx-xx-xx-xx }
```

## Parameter

Parameter	Description
<b>string <i>STRING</i></b>	Stands for the character string carried by the sub-option of option82 vendor-specific.
<b>hex <i>xx-xx-xx-xx-xx-xx</i></b>	Stands for the Hex system carried by option82 vendor-specific.

## Default

None



## Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping. (The switch of manually set option82 need be enabled. See the command, **ip dhcp-relay snooping information option format manual**)

## Example

The following example shows how to set vendor-specific (suboption 9) of option 82 by the hex system on interface g0/3.

```
Switch_config# ip dhcp-relay snooping
```

```
Switch_config# ip dhcp-relay snooping vlan 1
```

```
Switch_config#ip dhcp-relay snooping information option format manual
```

```
Switch_config#interface g0/3
```

```
Switch_config_g0/3#  dhcp      snooping      information      vendor-specific      hex
00-00-00-09-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
```

### 1.1.20 dhcp snooping information append

## Syntax

**dhcp snooping information append**

**dhcp snooping information append first-subop9-param { hex XX-XX-XX-XX-XX-XX | hostname | vlanip }**

**dhcp snooping information append second-subop9-param { hex XX-XX-XX-XX-XX-XX | hostname | vlanip }**

**no dhcp snooping information append**

**no dhcp snooping information append first-subop9-param**

**no dhcp snooping information append second-subop9-param**

## Parameter

Parameter	Description
<b>first-subop9-param</b> <b>hex [xx-xx-xx-xx-xx-xx]</b>	Stands for the Hex system of the first parameter carried by option82 vendor-specific (suboption9).
<b>second-subop9-param</b> <b>hex [xx-xx-xx-xx-xx-xx]</b>	Stands for the Hex system of the second parameter carried by option82 vendor-specific (suboption9).

<b>hostname</b>	Stands for the host name carried by option82 vendor-specific (suboption9).
<b>vlanip</b>	Stands for the IP address of the interface vlan carried by option82 vendor-specific (suboption9).

## Default

None

## Usage Guidelines

This command can be set on each port that connects the client. This command is used to configure option82 of the DHCP packet, which is sent by DHCP client to DHCP server and monitored by DHCP snooping.

This command without parameters acts as a switch command. When append is enabled, the information of this command will be added to suboption9 of option82. The added information is first-subop9-param and second-subop9-param.

## Example

The following example shows how to expand the packet with option82 on interface g0/3 and add parameter 1 for suboption9 with the hex system 61-62-63-61-62-63.

```
Switch_config_g0/3# dhcp snooping information append
```

```
Switch_config_g0/3#dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
```

61-62-63-61-62-63 is the hex system for the added parameter.

### 1.1.21 dhcp snooping information drop

## Syntax

**dhcp snooping information drop**

**no dhcp snooping information drop**

## Parameter

None

## Default

None

## Usage Guidelines

This command can be set on each port that connects the client.

After this command is set, the request packets that contain option82 will be dropped on the stipulated port.

## Example

The following example shows how to drop the dhcp packet with option82 on interface g0/3.

```
Switch_config_g0/3# dhcp snooping information drop
```

### 1.1.22 ip-source trust

#### Syntax

**ip-source trust**

**no ip-source trust**

#### Parameter

None

#### Default

The default interface is a distrusted one.

## Usage Guidelines

Source IP address snooping is not conducted to the source-IP-trusted interface. The “no” form of this command is used to resume the Default of this interface.

## Example

The following example shows how to set interface GigaEthernet0/1 to a source-ip-trusted interface.

```
Switch_config_g0/1#ip-source trust
```

### 1.1.23 show ip dhcp-relay snooping

#### Syntax

**show ip dhcp-relay snooping**

#### Parameter

None

#### Default

None

#### Usage Guidelines

This command is used to display the information about DHCP-relay snooping configuration.

#### Example

The following example shows how to display the information about DHCP-relay snooping configuration.

```
Switch_config#show ip dhcp-relay snooping
```

### 1.1.24 show ip dhcp-relay snooping binding

#### Syntax

**show ip dhcp-relay snooping binding [all]**

#### Parameter

None

#### Default

None

#### Usage Guidelines

This command is used to display the binding information about DHCP-relay snooping.

If the **all** parameter is in the command sentence, all binding information about DHCP-relay snooping will be displayed.

### Example

The following example shows how to display the binding information about DHCP-relay snooping.

```
Switch_config#show ip dhcp-relay snooping binding
```

## 1.1.25 debug ip dhcp-relay snooping

### Syntax

**debug ip dhcp-relay snooping**

**no debug ip dhcp-relay snooping**

### Parameter

None

### Default

None

### Usage Guidelines

This command is used to enable or disable the debugging switch of DHCP-relay snooping.

### Example

The following example shows how to enable the debugging switch of DHCP-relay snooping.

```
Switch#debug ip dhcp-relay snooping  
Switch#
```

## 1.1.26 debug ip dhcp-relay event

### Syntax

**debug ip dhcp-relay eventr**

**no debug ip dhcp-relay event**

#### Parameter

None

#### Default

None

#### Usage Guidelines

This command is used to enable or disable the event debugging switch of DHCP-relay.

#### Example

The following example shows how to enable the event debugging switch of DHCP-relay.

```
Switch#debug ip dhcp-relay event
Switch#
```

### 1.1.27 debug ip dhcp-relay binding

#### Syntax

**debug ip dhcp-relay binding**  
**no debug ip dhcp-relay binding**

#### Parameter

None

#### Default

None

#### Usage Guidelines

This command is used to enable or disable the binding debugging switch of DHCP-relay snooping.

#### Example

The following example shows how to enable the binding debugging switch of DHCP-relay snooping.

```
Switch#debug ip dhcp-relay binding
```

Switch#