

# **DHCP-SNOOPING Configuration Commands**

# Table of Contents

<b>1</b>	<b>DHCP-snooping Configuration Commands.....</b>	<b>- 1 -</b>
1.1	DHCP-snooping Configuration Tasks.....	- 1 -
1.1.1	Enabling or disabling DHCP-Snooping.....	- 2 -
1.1.2	Enabling DHCP-Snooping on VLAN.....	- 2 -
1.1.3	Configuring the DHCP-Trusted Port.....	- 3 -
1.1.4	Enabling the DAI Function on VLAN.....	- 3 -
1.1.5	Configuring the ARP-Trusted Port.....	- 3 -
1.1.6	Enabling Source IP Monitoring on VLAN.....	- 4 -
1.1.7	Configuring Source-IP-Trusted Port.....	- 4 -
1.1.8	Configuring the TFTP Server to Backup the Port-Binding Relationship	- 5 -
1.1.9	Configuring the Filename of Port-Binding Relationship Backup.....	- 5 -
1.1.10	Configuring the Interval for Checking Port-Binding Relationship Backup.... .....	- 6 -
1.1.11	Configuring Port-Binding Manually.....	- 6 -
1.1.12	Monitoring and Maintaining DHCP-Snooping.....	- 7 -
1.1.13	DHCP-Snooping Configuration Example.....	- 8 -

# 1 DHCP-snooping Configuration Commands

## 1.1 DHCP-snooping Configuration Tasks

The task of the DHCP-snooping is to judge the DHCP message, prevent the fake DHCP server from providing DHCP service and maintain the mapping between MAC address and IP address. According to the mapping between MAC address and IP address, the DAI function and the IP source guard function can be complete. DHCP-snooping functions contain DHCP message listening, dynamic maintenance of the mapping table of MAC address and IP address. The layer-2 switch filters the messages that do not satisfy the mapping relationship and prevents the network attack from illegal users.

- Enabling or disabling DHCP-Snooping
- Enabling DHCP-Snooping on VLAN
- Configuring the DHCP-Trusted Port
- Enabling the DAI Function on VLAN
- Configuring the ARP-Trusted Port
- Enabling Source IP Monitoring on VLAN
- Configuring Source-IP-Trusted Port
- Configuring the TFTP Server to Backup the Port-Binding Relationship
- Configuring the Filename of Port-Binding Relationship Backup
- Configuring the interval of Port-Binding Relationship Backup
- Configuring Port-Binding Manually
- Monitoring and Maintaining DHCP-Snooping
- DHCP-Snooping Configuration Example

### 1.1.1 Enabling or disabling DHCP-Snooping

Perform the following configuration globally:

Run.	To
<b>ip dhcp-relay snooping</b>	Enable the DHCP-snooping function.
<b>no ip dhcp-relay snooping</b>	Resume the default settings.

The command is a globally control command to start up the DHCP snooping function. If the command is configured, the switch monitors all DHCP messages and relative binding relationship is formed.

**Note:**

Before the command is configured at the client, the switch cannot add the corresponding binding relationship when the switch obtains an address.

### 1.1.2 Enabling DHCP-Snooping on VLAN

If the DHCP snooping function is configured on VLAN, all DHCP messages received from illegal physical ports in the whole VLAN will be legally monitored. The DHCP response messages from all illegal physical ports in the whole VLAN will be dropped, preventing illegal users from forging addresses or the incorrectly configured DHCP server from allocating addresses. For the DHCP request messages from illegal ports, if the MAC address that the message is sent to does not match the hardware address field, the message will be considered as the DHCP DOS attack message that is forged by user, so the switch will drop the message.

Perform the following configuration globally:

Run.	To
<b>ip dhcp-relay snooping vlan <i>vlan_id</i></b>	Enable DHCP-snooping on VLAN.
<b>no ip DHCP-snooping vlan <i>vlan_id</i></b>	Disable DHCP-snooping on VLAN

### 1.1.3 Configuring the DHCP-Trusted Port

If a DHCP-trusted port is configured, the DHCP messages from the DHCP-trusted port will not be checked.

Perform the following operations in physical port configuration mode:

Run	To
<b>Dhcp snooping trust</b>	Configure the DHCP-trusted port.
<b>no Dhcp snooping trust</b>	Resume the DHCP-trusted port to a distrusted port.

The ports are distrusted by default.

### 1.1.4 Enabling the DAI Function on VLAN

When the dynamic ARP monitoring is performed on all physical ports of a VLAN, if the source MAC address and the source IP address of the ARP message received by a port do not satisfy the binding relationship of MAC address and IP address, the ARP message will be rejected. The MAC-to-IP mapping relationship can be configured on the port manually or dynamically. If the MAC-to-IP mapping is not configured on the physical port, the switch declines to forward all ARP message.

Run	To
<b>Ip arp inspection vlan <i>vlanid</i></b>	Enable the dynamic ARP monitoring on all illegal ports within a VLAN.
<b>No Ip arp inspection vlan <i>vlanid</i></b>	Disable the dynamic ARP monitoring on all illegal ports within a VLAN.

### 1.1.5 Configuring the ARP-Trusted Port

The ARP monitoring is not enabled on the ARP-trusted port. The ports are distrusted ports by default.

Perform the following operations in port configuration mode:

Run	To
-----	----

<b>Arp inspection trust</b>	Configure the ARP -trusted port.
<b>no Arp inspection trust</b>	Resume to the ARP-distrusted port.

### 1.1.6 Enabling Source IP Monitoring on VLAN

After source IP monitoring is enabled on a VLAN, if the source MAC address and the source IP address of the IP message received by a port do not satisfy the binding relationship of MAC address and IP address, the IP message will be rejected. The MAC-to-IP mapping relationship can be configured on the port manually or dynamically. If the MAC-to-IP mapping is not configured on the physical port, the switch declines to forward all IP message.

Perform the following configuration globally:

Run...	To...
<b>ip verify source vlan <i>vlanid</i></b>	Enable source IP address monitoring on all distrusted ports in a VLAN.
<b>No ip verify source vlan <i>vlanid</i></b>	Disable source IP address monitoring on all ports in a VLAN.

Note:

After the global snooping is configured, the received message may be the DHCP message and also the IP message.

### 1.1.7 Configuring Source-IP-Trusted Port

The source address checkup is not enabled on the source-IP-trusted ports.

Perform the following operations in port configuration mode:

Run...	To...
<b>Ip-source trust</b>	Configure the source-IP-trusted port.
<b>No ip-source trust</b>	Resume to a source-IP-distrusted port.

### 1.1.8 Configuring the TFTP Server to Backup the Port-Binding Relationship

After the switch configuration is saved and then the switch is restarted, the previously-configured port binding relationship does not exist again. In this case, if the source IP address monitoring function is enabled, the switch declines to forward the IP message. To resolve the problem, the TFTP server is adopted to backup the port-binding relationship. After the TFTP server is configured, the port-binding relationship will be automatically downloaded to the TFTP server through the TFTP protocol. In this case, the switch automatically downloads the port-binding table from the TFTP server after the switch is restarted.

Perform the following configuration globally:

Run...	To...
Ip dhcp-relay snooping database-agent <i>ip-address</i>	Configure the IP address of the TFTP server which is used to backup the port-binding relationship.
No ip dhcp-relay snooping database-agent	Delete the TFTP server configuration.

### 1.1.9 Configuring the Filename of Port-Binding Relationship Backup

It is the filename saved on the TFTP server when the TFTP server backups the port-binding relationship. Therefore, different switches can backup their own port-binding relationship to a same TFTP server.

Perform the following configuration globally:

Run...	To...
Ip dhcp-relay snooping db-file <i>name</i>	Configure the filename of port-binding relationship backup.
No ip dhcp-relay snooping db-file	Delete the filename of port-binding relationship backup.

### 1.1.10 Configuring the Interval for Checking Port-Binding Relationship Backup

The MAC-to-IP binding table dynamically changes; therefore, it need be checked after a certain time. If the binding table is updated, it need be backed up again. The default value of the interval is 30 minutes.

Perform the following configuration globally:

Run...	To...
Ip dhcp-relay snooping write <i>num</i>	Configure the interval for checking port-binding relationship backup (unit: minute).
No Ip dhcp-relay snooping write	Resume the interval for checking port-binding relationship backup to the default value.

### 1.1.11 Configuring Port-Binding Manually

For hosts whose MAC addresses are not obtained from the DHCP server, the items in the port-binding table can be manually configured on the port of a switch to enable the hosts to access the network normally.

Note:

The items configured manually in the port-binding table have higher priority than the dynamically-configured items. If the manually-configured item has the same MAC address as the dynamically-configured item, the manually-configured item replaces the dynamically-configured item. The item in the port-binding table takes the MAC address as the unique index.

Perform the following configuration globally:

Run...	To...
ip source binding <i>MAC IP interface name</i>	Configure port binding manually.
No ip source binding <i>MAC IP</i>	Delete items in the port-binding table.



### 1.1.12 Monitoring and Maintaining DHCP-Snooping

Perform the following operations in management mode:

Run...	To...
<b>show ip dhcp-relay snooping</b>	Display the configuration information about DHCP-snooping.
<b>show ip dhcp-relay snooping binding</b>	Display the address-binding items that validate on the port.
<b>show ip dhcp-relay snooping binding all</b>	Display all address-binding items that are generated by DHCP snooping.
<b>[ no ] debug ip dhcp-relay [ snooping   binding   event ]</b>	Enable or disable the snooping, binding or event of the DHCP relay.

Display the configuration information about DHCP-snooping:

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

```
ip dhcp-relay snooping vlan 3
```

```
ip arp inspection vlan 3
```

```
DHCP Snooping trust interface:
```

```
FastEthernet0/1
```

```
ARP Inspect interface:
```

```
FastEthernet0/11
```

Display the information about dhcp-relay snooping binding:

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

Hardware Address	IP Address	remainder time	Type	VLAN	interface
00-e0-0f-26-23-89	192.2.2.101	86400	DHCP_SN	3	FastEthernet0/3

Display all information about dhcp-relay snooping binding:

```
switch#show ip dhcp-relay snooping binding all
```

Hardware Address	IP Address	remainder time	Type	VLAN	interface
00-e0-0f-32-1c-59	192.2.2.1	infinite	MANUAL	1	FastEthernet0/2
00-e0-0f-26-23-89	192.2.2.101	86400	DHCP_SN	3	FastEthernet0/3

Debug the information about dhcp-relay snooping:

```
switch#debug ip DHCP-snooping packet
DHCP: receive l2 packet from vlan 3, diID: 3
DHCP: DHCP packet len 277
DHCP: add binding on interface FastEthernet0/3
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 1
DHCP: DHCP packet len 300
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 3
DHCP: DHCP packet len 289
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 1
DHCP: DHCP packet len 300
DHCP: update binding on interface FastEthernet0/3
DHCP: IP address: 192.2.2.101, lease time 86400 seconds
DHCP: send packet continue
```

### 1.1.13 DHCP-Snooping Configuration Example

Figure 1 shows the networking of an example.

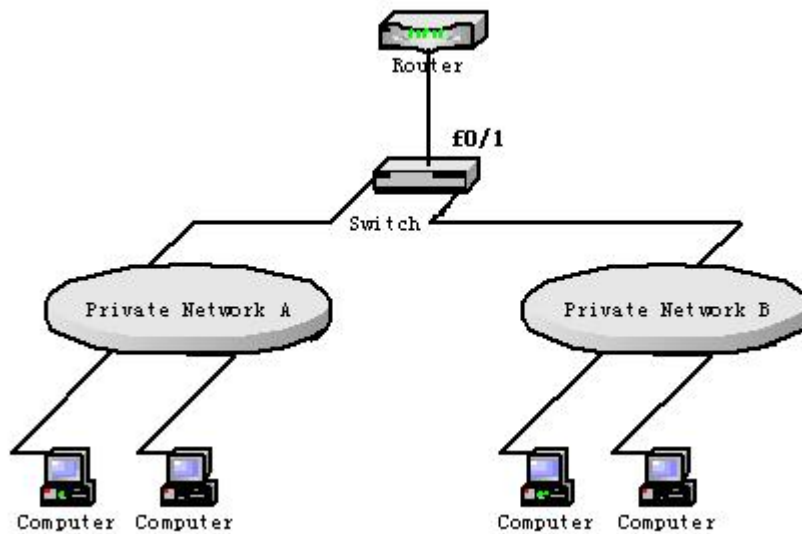


Figure 1 Configuring switch

- (1) Enable the DHCP-snooping of VLAN 1 that connects private network A.

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

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

- (2) Enable the DHCP-snooping of VLAN 2 that connects private network B.

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

```
Switch_config# ip dhcp-relay snooping vlan 2
```

- (3) Configure the DHCP-trusted port that the DHCP server connects.

```
Switch_config_f0/1# dhcp snooping trust
```