Chapter28:DHCP-Snooping Configuration

Table of Contents

Chapter 1 DHCP-Snooping Configuration

1.1 IGMP-Snooping Configuration Tasks

DHCP-Snooping is to prevent the fake DHCP server from providing the DHCP service by judging the DHCP packets, maintaining the binding relationship between MAC address and IP address. The L2 switch can conduct the DAI function and the IP source guard function according to the binding relationship between MAC address and IP address. The DHCP-snooping is mainly to monitor the DHCP packets and dynamically maintain the MAC-IP binding list. The L2 switch filters the packets, which do not meet the MAC-IP binding relationship, to prevent the network attack from illegal users.

- Enabling/Disabling DHCP-Snooping
- Enabling DHCP-Snooping in a VLAN ● Enabling DHCP anti-attack in a VLAN.
- Setting an Interface to a DHCP-Trusting Interface
- Enabling/Disabling binding table fast update function
- Enabling DAI in a VLAN
- Setting an Interface to an ARP-Trusting Interface
- Enabling Source IP Address Monitoring in a VLAN
- Setting anInterface to the One Which is Trusted by IP Source Address Monitoring
- Setting DHCP-Snooping Option 82
- Setting the Policy of DHCP-Snooping Option82 Packets
- Setting the TFTP Server for Backing up Interface Binding
- Setting a File Name for Interface Binding Backup
- Setting the Interval for Checking Interface Binding Backup
- Setting Interface Binding Manually
- Monitoring and Maintaining DHCP-Snooping
- Example of DHCP-Snooping Configuration

1.1.1 Enabling/Disabling DHCP-Snooping

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping	Enables DHCP-snooping.
no ip dhcp-relay snooping	Resumes the default settings.

This command is used to enable DHCP snooping in global configuration mode. After this command is run, the switch is to monitor all DHCP packets and form the corresponding binding relationship.

Note: If the client obtains the address of a switch before this command is run, the switch cannot add the corresponding binding relationship.

1.1.2 Enabling DHCP-Snooping in a VLAN

If DHCP snooping is enabled in a VLAN, the DHCP packets which are received from all distrusted physical ports in a VLAN will be legally checked. The DHCP response packets which are received from distrusted physical ports in a VLAN will then be dropped, preventing the faked or mis-configured DHCP server from providing address distribution services. For the DHCP request packet from distrusted ports, if the hardware address field in the DHCP request packet

does not match the MAC address of this packet, the DHCP request packet is then thought as a fake packet which is used as the attack packet for DHCP DOS and then the switch will drop it.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping vlan *vlan_id*	Enables DHCP-snooping in a VLAN.
no ip dhcp-relay snooping vlan *vlan_id*	Disables DHCP-snooping in a VLAN.

1.1.3 Enabling DHCP anti-attack in a VLAN.

To enable attack prevention in a VLAN, you need to configure the allowable maximum DHCP clients in a specific VLAN and conduct the principle of “first come and first serve”. When the number of users in the specific VLAN reaches the maximum number, new clients are not allowed to be distributed.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping max-client vlan *vlan_id number*	Enabling DHCP anti-attack in a VLAN.
no ip dhcp-relay snooping max-client vlan *vlan_id*	Disables DHCP anti-attack in a VLAN.

1.1.4 Setting an Interface to a DHCP-Trusting Interface

If an interface is set to be a DHCP-trusting interface, the DHCP packets received from this interface will not be checked.

Run the following commands in physical interface configuration mode.

Command	Operation
dhcp snooping trust	Setting an Interface to a DHCP-Trusting Interface
no dhcp snooping trust	Resumes an interface to a DHCP-distrusted interface.

The interface is a distrusted interface by default.

1.1.5 Enabling/Disabling binding table fast update function

This function is disabled by default. When this function is disabled and a port has been bound to client A, the DHCP request of the same MAC address on other ports will be regarded as a fake MAC attack even if client A is off line.

When this function is enabled, the above-mentioned case will not occur.

It is recommended to use this function in case that a client frequently changes its port and address lease, distributed by DHCP server, cannot be modified to a short period of time.

Command	Operation
ip dhcp-relay snooping rapid-refresh-bind	Enables the fast update function of the binding table.

no ip dhcp-relay snooping rapid-refresh-bind	Disables the fast update function of the binding table.

1.1.6 Enabling DAI in a VLAN

When dynamic ARP monitoring is conducted in all physical ports of a VLAN, a received ARP packet will be rejected if the source MAC address and the source IP address of this packet do not match up with the configured MAC-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all ARP packets.

Command	Operation
ip arp inspection vlan *vlanid*	Enables dynamic ARP monitoring on all distrusted ports in a VLAN.
no ip arp inspection vlan *vlanid*	Disables dynamic ARP monitoring on all distrusted ports in a VLAN.

1.1.7 Setting an Interface to an ARP-Trusting Interface

ARP monitoring is not enabled on those trusted interfaces. The interfaces are distrusted ones by default.

Run the following commands in interface configuration mode.

Command	Operation
arp inspection trust	Setting an Interface to an ARP-Trusting Interface
no arp inspection trust	Resumes an interface to an ARP-distrusting interface.

1.1.8 Enabling Source IP Address Monitoring in a VLAN

After source IP address monitoring is enabled in a VLAN, IP packets received from all physical ports in the VLAN will be rejected if their source MAC addresses and source IP addresses do not match up with the configured MAC-to-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all IP packets received from the physical interface.

Run the following commands in global configuration mode.

Command	Operation
ip verify source vlan *vlanid*	Enables source IP address checkup on all distrusted interfaces in a VLAN.
no ip verify source vlan *vlanid*	Disables source IP address checkup on all interfaces in a VLAN.

Note: If the DHCP packet (also the IP packet) is received, it will be forwarded because global snooping is configured.

1.1.9 Setting anInterface to the One Which is Trusted by IP Source Address Monitoring

The source address detection function will not be enabled for the IP source address trust interface.

Run the following commands in interface configuration mode.

Command	Operation
ip-source trust	Sets an interface to the one with a trusted source IP address.
no ip-source trust	Resumes an interface to the one with a distrusted source IP address.

1.1.10 Setting DHCP-Snooping Option 82

Option 82 brings the local information to a server and helps the server to distribute addresses to clients.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping information option	Sets that option82, which is in the default format, is carried when DHCP-snooping forwards the DHCP packets.
no ip dhcp-relay snooping information option	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

To specify the format of option82, conduct the following settings in global mode.

Command	Operation
ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type / cm-type/ [host]}	Sets the format of option82 that the DHCP packets carry when they are forwarded by DHCP-Snooping.
no ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type /cm-type/[[host]}	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the circuit-id:

Command	Operation

dhcp snooping information circuit-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information circuit-id **hex** **[***xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system..
	This command is set on the port that connects the client.
no dhcp snooping information circuit-id	Deletes the manually configured option82 circuit-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the remote-id:

Command	Operation
dhcp snooping information remote-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information remote-id **hex** **[***xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no dhcp snooping information remote-id	Deletes the manually configured option82 remote-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the vendor-specific:

Command	Operation
dhcp snooping information vendor-specific string STRING	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.

dhcp snooping information vendor-specific hex [*xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no **dhcp snooping information vendor-specific**	Deletes the manually configured option82 vendor-specific.

1.1.11 Setting the Policy of DHCP-Snooping Option82 Packets

You can set the policy for the DHCP request packets, which carry with option82, after these packets are received. The policies include the following ones:

"Drop" policy: Run the following command in port mode to drop the request packets with option82.

Command	Operation
dhcp snooping information drop	Drops the request packets that contain option82.

"Append" policy: Run the following command in port mode to add the request packets with option82.

Command	Operation
dhcp snooping information append	Enables the function to add option82 on a port.
dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Stands for the first parameter carried by option82 vendor-specific (suboption9).
dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Stands for the second parameter carried by option82 vendor-specific (suboption9).

1.1.12 Setting the TFTP Server for Backing up Interface Binding

After the switch configuration is rebooted, the previously-configured interface binding will be lost. In this case, there is no binding relationship on this interface. After source IPaddress monitoring is enabled, the switch rejected forwarding all IP packets. After the TFTP server is configured for interface binding backup, the binding relationship will be backed up to the server through the TFTP protocol. After the switch is restarted, the switch automatically downloads the binding list from the TFTP server, securing the normal running of the network. Run the following commands in global configuration mode.

Command	Operation

ip dhcp-relay snooping database-agent *ip-address*	*C*onfigures the IP address of the TFTP server which is to back up interface binding.
no ip dhcp-relay snooping database-agent *ip-address*	Cancels the TFTP Server for backing up interface binding.

1.1.13 Setting a File Name for Interface Binding Backup

When backing up the interface binding relationship, the corresponding file name will be saved on the TFTP server. In this way, different switches can back up their own interface binding relationships to the same TFTP server.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping db-file *name* [timestamp]	Configures a file name for interface binding backup.
no ip dhcp-relay snooping db-file	Cancels a file name for interface binding backup.

1.1.14 Setting the Interval for Checking Interface Binding Backup

The MAC-to-IP binding relationship on an interface changes dynamically. Hence, you need check whether the binding relationship updates after a certain interval. If the binding relationship updates, it need be backed up again. The default time interval is 30mins. Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping write-immediately	Configures DHCP Snooping immediate backup when the binding information changes. no ip dhcp-relay snooping {write-time | write-immediately} Resumes the interval of checking interface binding backup to the default settings.
ip dhcp-relay snooping write-time *num*	Configures the interval for checking interface binding backup. The unit is min.
no ip dhcp-relay snooping write-time	Resumes the interval of checking interface binding backup to the default settings.

1.1.15 Setting Interface Binding Manually

If a host does not obtain the address through DHCP, you can add the binding item on an interface of a switch to enable the host to access the network. You can run no ip source binding MAC IP to delete items from the corresponding binding list.

Note that the manually-configured binding items have higher priority than the dynamically-configured binding items. If the manually-configured binding item and the dynamically-configured binding item have the same MAC address, the manually-configured one updates the

dynamically-configured one. The interface binding item takes the MAC address as the unique index.

Run the following commands in global configuration mode.

Command	Operation
ip source binding *MAC IP* interface *name* [vlan *vlan-id*]	Configures Interface Binding Manually
no ip source binding *MAC IP* vlan *vlan-id*	Cancels an interface binding item.

1.1.6 Monitoring and Maintaining DHCP-Snooping

Run the following commands in EXEC mode:

Command	Operation
show ip dhcp-relay snooping	Displays the information about DHCP-snooping configuration.
show ip dhcp-relay snooping binding	Displays the effective address binding items on an interface.
show ip dhcp-relay snooping binding all	Displays all binding items which are generated by DHCP snooping.
[**no**] **debug ip dhcp-relay** [snooping |	Enables or disables the switch of DHCP
binding | event | all]	relay snooping binding or event.

The following shows the information about the DHCP snooping configuration.

```
switch#show ip dhcp-relay snooping
  ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
   GigaEthernet0/1
ARP Inspect interface:
   GigaEthernet0/11
```

The following shows the binding information about dhcp-relay snooping:

```
 switch#show ip dhcp-relay snooping binding
Hardware Address       IP Address       remainder time Type
                                                          VLAN      interface
                                                    DHCP_SN                3
00-e0-0f-26-23-89       192.2.2.101          86400
 GigaEthernet0/3
```

The following shows the binding information about dhcp-relay snooping:

```
 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
```

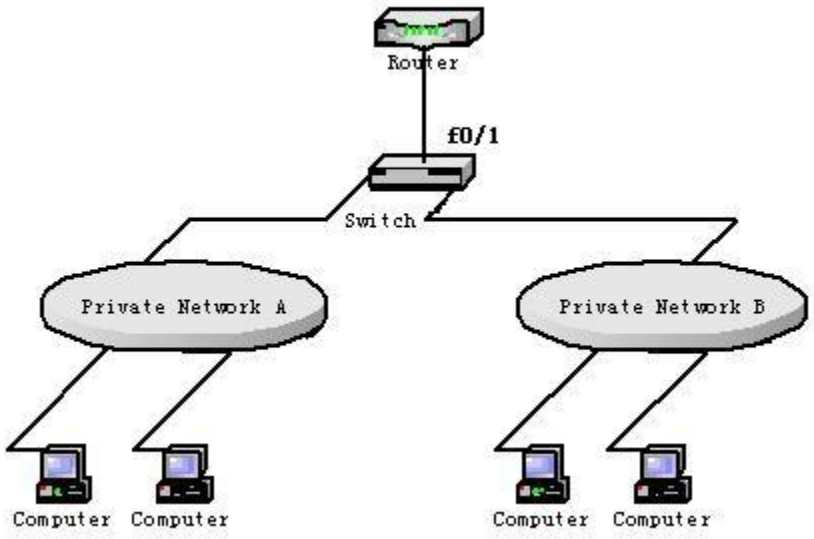
GigaEthernet0/2 00-e0-0f-26-23-89 GigaEthernet0/3	192.2.2.101	86400	DHCP_SN	3

The following shows the information about dhcp-relay snooping.

```
switch#debug ip dhcp-relay all
DHCPR: receive l2 packet from vlan 3, diID: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface GigaEthernet0/3
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 1
DHCPR: DHCP packet len 300
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 3
DHCPR: DHCP packet len 289
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 1
DHCPR: DHCP packet len 300
DHCPR: update binding on interface GigaEthernet0/3
DHCPR:    IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue
```

1.1.17 Example of DHCP-Snooping Configuration

The network topology is shown in figure 1.



Configuring Switch

Enable DHCP snooping in VLAN 1 which connects private network A. Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 1

Enable DHCP snooping in VLAN 2 which connects private network B.

Switch_config#ip dhcp-relay snooping

Switch_config#ip dhcp-relay snooping vlan 2

Sets the interface which connects the DHCP server to a DHCP-trusting interface.

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

Configure option82 instance manually interface

```
GigaEthernet0/1
  dhcp snooping information circuit-id hex 00-01-00-05 dhcp
  snooping information remote-id hex 00-e0-0f-13-1a-50
  dhcp snooping information vendor-specific hex
   00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34 dhcp snooping
information append dhcp snooping information append first-subop9-
                                                    param hex
  61-62-63-61-62-63
  !
  interface GigaEthernet0/2
    dhcp snooping trust
    arp inspection trust ip-
    source trust
  !
  !
  !
  ip dhcp-relay snooping ip dhcp-
  relay snooping vlan 1-100 ip arp
  inspection vlan 1 ip verify
  source vlan 1
  ip dhcp-relay snooping information option format manual
```