

DHCP Snooping Commands

This chapter contains the following sections:

- ip dhcp snooping, on page 2
- ip dhcp snooping vlan, on page 3
- ip dhcp snooping trust, on page 4
- ip dhcp snooping information option allowed-untrusted, on page 5
- ip dhcp snooping verify, on page 6
- ip dhcp snooping database, on page 7
- ip dhcp snooping binding, on page 8
- clear ip dhcp snooping database, on page 10
- show ip dhcp snooping, on page 11
- show ip dhcp snooping binding, on page 12
- ip arp inspection, on page 13
- ip arp inspection vlan, on page 14
- ip arp inspection validate, on page 15
- ip arp inspection list create, on page 16
- ip mac, on page 17
- ip arp inspection list assign, on page 18
- ip arp inspection logging interval, on page 19
- show ip arp inspection, on page 20
- show ip arp inspection list, on page 21
- show ip arp inspection statistics, on page 22
- clear ip arp inspection statistics, on page 23

ip dhcp snooping

Use the **ip dhcp snooping** Global Configuration mode command to enable Dynamic Host Configuration Protocol (DHCP) Snooping globally. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping

no ip dhcp snooping

Default Configuration

DHCP snooping is disabled.

Command Mode

Global Configuration mode

User Guidelines

For any DHCP Snooping configuration to take effect, DHCP Snooping must be enabled globally. DHCP Snooping on a VLAN is not active until DHCP Snooping on a VLAN is enabled.

Example

The following example enables DHCP Snooping on the device.

```
switchxxxxxx(config)# ip dhcp snooping
```

ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** Global Configuration mode command to enable DHCP Snooping on a VLAN. Use the **no** form of this command to disable DHCP Snooping on a VLAN.

Syntax

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping vlan *vlan-id*

Parameters

- ***vlan-id***—Specifies the VLAN ID.

Default Configuration

DHCP Snooping on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

DHCP Snooping must be enabled globally before enabling DHCP Snooping on a VLAN.

Example

The following example enables DHCP Snooping on VLAN 21.

```
switchxxxxxx(config)# ip dhcp snooping vlan 21
```

ip dhcp snooping trust

Use the **ip dhcp snooping trust** Interface Configuration (Ethernet, Port-channel) mode command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to restore the default configuration.

Syntax

ip dhcp snooping trust

no ip dhcp snooping trust

Default Configuration

The interface is untrusted.

Command Mode

Interface (Ethernet, Port Channel) Configuration mode

User Guidelines

Configure as trusted the ports that are connected to a DHCP server or to other switches or routers. Configure the ports that are connected to DHCP clients as untrusted.

Example

The following example configures gi1/0/4 as trusted for DHCP Snooping.

```
switchxxxxxx(config)# interface gi1/0/4
switchxxxxxx(config-if)# ip dhcp snooping trust
```

ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** Global Configuration mode command to allow a device to accept DHCP packets with option-82 information from an untrusted port. Use the **no** form of this command to drop these packets from an untrusted port.

Syntax

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Default Configuration

DHCP packets with option-82 information from an untrusted port are discarded.

Command Mode

Global Configuration mode

Example

The following example allows a device to accept DHCP packets with option-82 information from an untrusted port.

```
switchxxxxxx(config)# ip dhcp snooping information option allowed-untrusted
```

ip dhcp snooping verify

Use the **ip dhcp snooping verify** Global Configuration mode command to configure a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address. Use the **no** form of this command to disable MAC address verification in a DHCP packet received on an untrusted port.

Syntax

ip dhcp snooping verify

no ip dhcp snooping verify

Default Configuration

The switch verifies that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address in the packet.

Command Mode

Global Configuration mode

Example

The following example configures a device to verify that the source MAC address in a DHCP packet received on an untrusted port matches the client hardware address.

```
switchxxxxxx(config)# ip dhcp snooping verify
```

ip dhcp snooping database

Use the **ip dhcp snooping database** Global Configuration mode command to enable the DHCP Snooping binding database file. Use the **no** form of this command to delete the DHCP Snooping binding database file.

Syntax

ip dhcp snooping database

no ip dhcp snooping database

Default Configuration

The DHCP Snooping binding database file is not defined.

Command Mode

Global Configuration mode

User Guidelines

The DHCP Snooping binding database file resides on Flash. To ensure that the lease time in the database is accurate, the Simple Network Time Protocol (SNTP) must be enabled and configured. The device writes binding changes to the binding database file only if the device system clock is synchronized with SNTP.

Example

The following example enables the DHCP Snooping binding database file.

```
switchxxxxxx(config)# ip dhcp snooping database
```

ip dhcp snooping binding

Use the **ip dhcp snooping binding** Privileged EXEC mode command to configure the DHCP Snooping binding database and add dynamic binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

Syntax

ip dhcp snooping binding *mac-address vlan-id ip-address interface-id* **expiry** {*seconds* | **infinite**}

no ip dhcp snooping binding *mac-address vlan-id*

Parameters

- ***mac-address***—Specifies a MAC address.
- ***vlan-id***—Specifies a VLAN number.
- ***ip-address***—Specifies an IP address.
- ***interface-id***—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.
- **expiry**
  - ***seconds***—Specifies the time interval, in seconds, after which the binding entry is no longer valid. (Range: 10–4294967294).
  - **infinite**—Specifies infinite lease time.

Default Configuration

No static binding exists.

Command Mode

Privileged EXEC mode

User Guidelines

Use the **ip dhcp snooping binding** command to add manually a dynamic entry to the DHCP database.

After entering this command, an entry is added to the DHCP Snooping database. If the DHCP Snooping binding file exists, the entry is also added to that file.

The entry would not be added to the configuration files. The entry would be displayed in the show commands as a “DHCP Snooping” entry. An entry added by this command can override the existed dynamic entry. The entry is displayed in the show commands as a DHCP Snooping entry.

Use the **no ip dhcp snooping binding** command to delete manually a dynamic entry from the DHCP database.

A dynamic temporary entries for which the IP address is 0.0.0.0 cannot be deleted.

Example

The following example adds a binding entry to the DHCP Snooping binding database.

```
switchxxxxxx# ip dhcp snooping binding 0060.704C.73FF 23 176.10.1.1 gi1/0/4 expiry 900
```

clear ip dhcp snooping database

Use the **clear ip dhcp snooping database** Privileged EXEC mode command to clear the DHCP Snooping binding database.

Syntax

clear ip dhcp snooping database

Command Mode

Privileged EXEC mode

Example

The following example clears the DHCP Snooping binding database.

```
switchxxxxxx# clear ip dhcp snooping database
```

show ip dhcp snooping

Use the **show ip dhcp snooping** EXEC mode command to display the DHCP snooping configuration for all interfaces or for a specific interface.

Syntax

show ip dhcp snooping *[interface-id]*

Parameters

- ***interface-id***—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following example displays the DHCP snooping configuration.

```
switchxxxxxx# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 21
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 6666 seconds
```

Interface	Trusted
---------	-------
gi1/0/1	Yes
gi1/0/2	Yes

show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** User EXEC mode command to display the DHCP Snooping binding database and configuration information for all interfaces or for a specific interface.

Syntax

show ip dhcp snooping binding [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan-id*] [*interface-id*]

Parameters

- **mac-address** *mac-address*—Specifies a MAC address.
- **ip-address** *ip-address*—Specifies an IP address.
- **vlan** *vlan-id*—Specifies a VLAN ID.
- ***interface-id***—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following examples displays the DHCP snooping binding database and configuration information for all interfaces on a device.-

```
switchxxxxxx# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 2
```

Mac Address	IP Address	Lease (sec)	Type	VLAN	Interface
0060.704C.73FF	10.1.8.1	7983	snooping	3	gi1/0/1
0060.704C.7BC1	10.1.8.2	92332	snooping (s)	3	gi1/0/2

ip arp inspection

Use the **ip arp inspection** Global Configuration mode command globally to enable Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to disable ARP inspection.

Syntax

ip arp inspection

no ip arp inspection

Default Configuration

ARP inspection is disabled.

Command Mode

Global Configuration mode

User Guidelines

Note that if a port is configured as an untrusted port, then it should also be configured as an untrusted port for DHCP Snooping, or the IP-address-MAC-address binding for this port should be configured statically. Otherwise, hosts that are attached to this port cannot respond to ARPs.

Example

The following example enables ARP inspection on the device.

```
switchxxxxxx(config)# ip arp inspection
```

ip arp inspection vlan

Use the **ip arp inspection vlan** Global Configuration mode command to enable ARP inspection on a VLAN, based on the DHCP Snooping database. Use the **no** form of this command to disable ARP inspection on a VLAN.

Syntax

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

Parameters

- ***vlan-id***—Specifies the VLAN ID.

Default Configuration

DHCP Snooping based ARP inspection on a VLAN is disabled.

Command Mode

Global Configuration mode

User Guidelines

This command enables ARP inspection on a VLAN based on the DHCP snooping database.

Example

The following example enables DHCP Snooping based ARP inspection on VLAN 23.

```
switchxxxxxx(config)# ip arp inspection vlan 23
```

ip arp inspection validate

Use the **ip arp inspection validate** Global Configuration mode command to perform specific checks for dynamic Address Resolution Protocol (ARP) inspection. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection validate

no ip arp inspection validate

Default Configuration

ARP inspection validation is disabled.

Command Mode

Global Configuration mode

User Guidelines

The following checks are performed:

- **Source MAC address**: Compares the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses.
- **Destination MAC address**: Compares the destination MAC address in the Ethernet header against the target MAC address in the ARP body. This check is performed for ARP responses.
- **IP addresses**: Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

Example

The following example executes ARP inspection validation.

```
switchxxxxxx(config)# ip arp inspection validate
```

ip arp inspection list create

Use the **ip arp inspection list create** Global Configuration mode command to create a static ARP binding list and enters the ARP list configuration mode. Use the **no** form of this command to delete the list.

Syntax

ip arp inspection list create *name*

no ip arp inspection list create *name*

Parameters

- ***name***—Specifies the static ARP binding list name. (Length: 1–32 characters).

Default Configuration

No static ARP binding list exists.

Command Mode

Global Configuration mode

User Guidelines

Use the **ip arp inspection list assign** command to assign the list to a VLAN.

Example

The following example creates the static ARP binding list ‘servers’ and enters the ARP list configuration mode.

```
switchxxxxxx(config)# ip arp inspection list create servers
```

ip mac

Use the **ip mac** ARP-list Configuration mode command to create a static ARP binding. Use the **no** form of this command to delete a static ARP binding.

Syntax

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

Parameters

- ***ip-address***—Specifies the IP address to be entered to the list.
- ***mac-address***—Specifies the MAC address associated with the IP address.

Default Configuration

No static ARP binding is defined.

Command Mode

ARP-list Configuration mode

Example

The following example creates a static ARP binding.

```
switchxxxxxx(config)# ip arp inspection list create servers
switchxxxxxx(config-arp-list)# ip 172.16.1.1 mac 0060.704C.7321
switchxxxxxx(config-arp-list)# ip 172.16.1.2 mac 0060.704C.7322
```

ip arp inspection list assign

Use the **ip arp inspection list assign** Global Configuration mode command to assign a static ARP binding list to a VLAN. Use the **no** form of this command to delete the assignment.

Syntax

ip arp inspection list assign *vlan-id name*

no ip arp inspection list assign *vlan-id*

Parameters

- ***vlan-id***—Specifies the VLAN ID.
- ***name***—Specifies the static ARP binding list name.

Default Configuration

No static ARP binding list assignment exists.

Command Mode

Global Configuration mode

Example

The following example assigns the static ARP binding list Servers to VLAN 37.

```
switchxxxxxx(config)# ip arp inspection list assign 37 servers
```

ip arp inspection logging interval

Use the **ip arp inspection logging interval** Global Configuration mode command to set the minimum time interval between successive ARP SYSLOG messages. Use the **no** form of this command to restore the default configuration.

Syntax

ip arp inspection logging interval {*seconds* | **infinite**}

no ip arp inspection logging interval

Parameters

- ***seconds***—Specifies the minimum time interval between successive ARP SYSLOG messages. A 0 value means that a system message is immediately generated. (Range: 0–86400)
- **infinite**—Specifies that SYSLOG messages are not generated.

Default Configuration

The default minimum ARP SYSLOG message logging time interval is 5 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the minimum ARP SYSLOG message logging time interval to 60 seconds.

```
switchxxxxxx(config)# ip arp inspection logging interval 60
```

show ip arp inspection

Use the **show ip arp inspection** EXEC mode command to display the ARP inspection configuration for all interfaces or for a specific interface.

Syntax

show ip arp inspection [*interface-id*]

Parameters

- ***interface-id***—Specifies an interface ID. The interface ID can be one of the following types: Ethernet port or Port-channel.

Command Mode

User EXEC mode

Example

The following example displays the ARP inspection configuration.

```
switchxxxxxx# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 222  seconds
 Interface    Trusted
----------- -----------
gi1/0/1          Yes
gi1/0/2          Yes
```

show ip arp inspection list

Use the **show ip arp inspection list** Privileged EXEC mode command to display the static ARP binding list.

Syntax

show ip arp inspection list

Command Mode

Privileged EXEC mode

Example

The following example displays the static ARP binding list.

```
switchxxxxxx# show ip arp inspection list
List name: servers
Assigned to VLANs: 1,2
```

IP	ARP
172.16.1.1	0060.704C.7322
172.16.1.2	0060.704C.7322

show ip arp inspection statistics

Use the **show ip arp inspection statistics** EXEC command to display statistics for the following types of packets that have been processed by this feature: Forwarded, Dropped, IP/MAC Validation Failure.

Syntax

show ip arp inspection statistics [*vlan vlan-id*]

Parameters

- ***vlan-id***—Specifies VLAN ID.

Command Mode

User EXEC mode

User Guidelines

Counters values are kept when disabling the ARP Inspection feature.

Example

```
switchxxxxxx# show ip arp inspection statistics
Vlan   Forwarded Packets Dropped Packets   IP/MAC Failures
----  ----------------- ---------------  ---------------
2     1500           100                        80
```

clear ip arp inspection statistics

Use the **clear ip arp inspection statistics** Privileged EXEC mode command to clear statistics ARP Inspection statistics globally.

Syntax

clear ip arp inspection statistics [**vlan** *vlan-id*]

Parameters

- ***vlan-id***—Specifies VLAN ID.

Command Mode

Privileged EXEC mode

Example

```
switchxxxxxx# clear ip arp inspection statistics
```