DHCP Snooping

Feature history for DHCP snooping

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 17.18.1	DHCP snooping: DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers.	Cisco C9350 Series Smart Switches

Understand DHCP snooping

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Uses the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

Other security features, such as dynamic Address Resolution Protocol (ARP) inspection (DAI), also uses information stored in the DHCP snooping binding database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or on a range of VLANs.

Note For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces, as untrusted DHCP messages will be forwarded only to trusted interfaces.

DHCP snooping and switch stacks

DHCP snooping is managed on the active switch. When you connect a new switch to the stack, it receives the DHCP snooping configuration. When a member leaves the stack, all DHCP snooping address bindings associated with the switch expires.

All snooping statistics are generated on the active switch. If a new active switch is elected, the statistics counters reset.

During a stack merge, if the switch is no more active, all DHCP snooping bindings are lost. In a stack partition, the active switch remains unchanged and the bindings belonging to partitioned switches expire. The new active switch of the partitioned stack begins processing the new incoming DHCP packets.

DHCP snooping binding database

A DHCP snooping binding database is a record system that

- stores information about untrusted interfaces when DHCP snooping is enabled,
- supports up to 4,000 bindings, and
- uses a checksum to verify entries for data integrity.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry is 77 bytes, followed by a space, a checksum value, and the EOL symbol.

Use the DHCP snooping database agent to retain bindings when the switch reloads. If the agent is disabled, dynamic ARP inspection or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When the switch reloads, it reads the binding file to build the DHCP snooping binding database. The switch updates the file when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The switch uses the DHCP snooping binding database to store information about untrusted interfaces when DHCP snooping is enabled. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

Binding file format

This is the format of the file with bindings:

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

Each entry in the file is tagged with a checksum value, which the switch uses to verify the entries when it reads the file. The initial-checksum entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

Binding file example

This is an example of a binding file:

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
10.1.1.1 512 001.0001.0005 3EBE2881 Gi1/1                                e5e1e733
10.1.1.1 512 001.0001.0002 3EBE2881 Gi1/1                                4b3486ec
10.1.1.1 1536 001.0001.0004 3EBE2881 Gi1/1                               f0e02872
10.1.1.1 1024 001.0001.0003 3EBE2881 Gi1/1                               ac41adf9
10.1.1.1 1 001.0001.0001 3EBE2881 Gi1/1                                  34b3273e
END
```

When the switch starts, and the calculated checksum value equals the stored checksum value, the switch reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The switch ignores an entry when one of these situations occurs:

- The switch reads the entry and the calculated checksum value does not equal the stored checksum value. The entry and the ones following it are ignored.
- An entry has an expired lease time, although the switch may not remove the entry when the lease time expires.
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.

DHCP gleaning

DHCP gleaning is a read-only DHCP snooping functionality that:

- extracts location information from DHCP messages,
- differentiates an untrusted device port connected to an end user from a trusted port connected to a DHCP server, and
- registers and gleans only DHCP version 4 packets.

Gleaning helps extract location information from DHCP messages when messages are forwarded by a DHCP relay agent. The process does not block or modify DHCP packets, making it passive. DHCP gleaning is

supported only on Layer 2 ports. By default, gleaning is disabled, though enabling a device sensor automatically activates it. It functions on all active interfaces where DHCP snooping is deactivated. For private VLAN interaction, ensure gleaning is active on the secondary VLAN, even if snooping is disabled on the primary VLAN.

Note On Cisco C9350 Series Smart Switches, private VLAN destination lookup forwarding is based on the primary VLAN.

Trusted and untrusted sources

A trusted source is an entity or component that is considered reliable for network communications, provides authenticated data transmissions, and is verified to be part of the network infrastructure.

An untrusted DHCP message is a message that is received through an untrusted interface. By default, the switch considers all interfaces untrusted. So, the switch must be configured to trust some interfaces to use DHCP Snooping. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer's switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, an example of an interface you might configure as trusted is one connected to a port on a device in the same network. An example of an untrusted interface is one that is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet that is received on an untrusted interface, has a source MAC address and a DHCP client hardware address that do not match.
- The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.
- DHCP snooping exceeds the queue size limit of 1000.

When an aggregation switch with DHCP snooping connects to an edge switch inserting DHCP option-82, packets with option-82 are dropped if received on an untrusted interface. If DHCP Snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the **ip dhcp snooping information option allow-untrusted** global configuration command, the aggregation switch accepts packets with option-82 information from the edge switch. The aggregation switch learns the bindings for hosts connected through an untrusted switch interface. The DHCP security features, such as Dynamic ARP Inspection or IP Source Guard, can still be enabled on the aggregation switch while the switch receives packets with option-82 information on untrusted input interfaces to which hosts are connected. The port on the edge switch that connects to the aggregation switch must be configured as a trusted interface.

Default settings for DHCP snooping

Table 1: Default DHCP snooping configuration

Feature	Default Setting
DHCP snooping	Disabled
DHCP snooping information option	Enabled
DHCP snooping option to accept packets on untrusted input interfaces[1]	Disabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping VLAN	Disabled
DHCP snooping MAC address verification	Enabled
DHCP snooping binding database agent	Enabled in Cisco IOS software, requires configuration. This feature is operational only when a destination is configured.

[1] Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.

Prerequisites for DHCP snooping

These prerequisites apply to DHCP snooping:

- You must be familiar with DHCP before you configure DHCP snooping.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces, as untrusted DHCP messages will be forwarded only to trusted interfaces. In a service-provider network, a trusted interface is connected to a port on a device in the same network.
- You must configure the switch to use the Cisco IOS DHCP server binding database to use it for DHCP snooping.

- To use the DHCP snooping option of accepting packets on untrusted inputs, the switch must be an aggregation switch that receives packets with option-82 information from an edge switch.
- The following prerequisites apply to DHCP snooping binding database configuration:
  - You must configure a destination on the DHCP snooping binding database to use the switch for DHCP snooping.
  - Because both NVRAM and the flash memory have limited storage capacity, we recommend that the binding file be stored on a TFTP server.
  - You must create an empty file at the configured network-based URLs (such as TFTP and FTP) before the switch can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.
  - To ensure the accuracy of the lease time in the database, we recommend that you enable and configure Network Time Protocol (NTP).
  - If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

Configure DHCP snooping

This section provides information about the various tasks to configure DHCP snooping.

Enable DHCP Snooping

Beginning in privileged EXEC mode, follow these steps to enable DHCP snooping on the switch:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp snooping** [**acl** | **database** | **glean** | **information** | **track** | **verify** | **vlan** | **wireless**] **Example:** `Device(config)# ip dhcp snooping`	Enables DHCP snooping globally. The **no** option disables DHCP snooping. Additionally, you can enable these optional keywords:

	Command or Action	Purpose
		• **acl**: Enables DHCP snooping on the specified ACL. • **database**: Enables DHCP snooping for the database agent or the binding file • **glean**: Enables read–only DHCP snooping function. • **information**: Enables the insertion and removal of Option 82 information for DHCP packets. • **track**: Enables DHCP server tracking when multiple DHCP servers are in the network. • **verify**: Verifies packets received on client associated address or gateway address which are part of DHCP snoop lookup. • **vlan**: Enables DHCP snooping on the specified VLANs. • **wireless**: Enables bootstrap protocol broadcast support in wireless DHCP.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Enable the DHCP snooping binding database agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the switch:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**ip dhcp snooping database** {**flash** [*number*] **:** */filename* | **ftp:**//*user* **:** *password* **@** *host* */filename* | **http:**//[[*username* **:** *password*] **@**] {*hostname* | *host-ip*} [*/directory*] */image-name***.tar** | **rcp:**//*user* **@** *host*/*filename* | **scp:**//*user***@***host*/*filename* | **tftp:**//*hostfilename*} **Example:** `Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2`	Specifies the URL for the database agent or the binding file by using one of these forms: • **flash**[*number*]**:**/*filename* • **ftp:**//*user***:***password***@***host*/*filename* • **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** • **rcp:**//*user***@***host*/*filename* • **scp:**//*user***@***host*/*filename* **Note** Before you configure SCP, you need to set the line console 0 transport output to *ssh* or *all*. • **tftp:**//*host*/*filename*
Step 4	**ip dhcp snooping database timeout** *seconds* **Example:** `Device(config)# ip dhcp snooping database timeout 300`	Specifies (in seconds) how long to wait for the database transfer process to finish before stopping the process. The default is 300 seconds. The range is 0 to 86400. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely.
Step 5	**ip dhcp snooping database write-delay** *seconds* **Example:** `Device(config)# ip dhcp snooping database write-delay 15`	Specifies the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds* **Example:** `Device# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5`	(Optional) Adds binding entries to the DHCP snooping binding database. The *vlan-id* range is from 1 to 4904. The *seconds* range is from 1 to 4294967295. Enter this command for each entry that you add. Use this command when you are testing or debugging the switch.

	Command or Action	Purpose
	`interface gigabitethernet 1/1/0 expiry 1000`	
Step 8	**show ip dhcp snooping database** [**detail**] **Example:** `Device# show ip dhcp snooping database detail`	Displays the status and statistics of the DHCP snooping binding database agent.

Configure an interface as a trusted or an untrusted source for DHCP gleaning

You can enable or disable DHCP gleaning on a device. You can configure an interface as a trusted or untrusted source of DHCP messages. Verify that no DHCP packets are dropped when DHCP gleaning is enabled on an untrusted interface or on a device port.

Note By default, DHCP gleaning is disabled, and all interfaces are untrusted.

You can configure DHCP trust on the following types of interfaces:

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces
- Layer 2 access and trunk interfaces

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp snooping glean** **Example:** `Device(config)# ip dhcp snooping glean`	Enables DHCP gleaning.
Step 4	**interface** *type number* **Example:** `Device(config)# interface gigabitEthernet 1/0/1`	Enters interface configuration mode, where *type number* is the Layer 2 Ethernet interface which you want to configure as trusted or untrusted for DHCP snooping.

	Command or Action	Purpose
Step 5	[**no**] **ip dhcp snooping trust** **Example:** `Device(config-if)# ip dhcp snooping trust`	Configures the interface as a trusted interface for DHCP snooping. The **no** option configures the port as an untrusted interface.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**show ip dhcp snooping statistics** **Example:** `Device# show ip dhcp snooping statistics`	Displays packets that were dropped on the device port configured as an untrusted interface.
Step 8	**show ip dhcp snooping** **Example:** `Device# show ip dhcp snooping`	Displays DHCP snooping configuration information, including information about DHCP gleaning.

Monitor DHCP snooping information

Table 2: Commands for displaying DHCP information

Command	Purpose
show ip dhcp snooping	Displays general information about DHCP snooping.
show ip dhcp snooping binding	Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.
show ip dhcp snooping database	Displays the DHCP snooping binding database status and statistics.
show ip dhcp snooping statistics	Displays the DHCP snooping statistics in summary or detail form.
show ip source binding	Display the dynamically and statically configured bindings.

Note If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.