DHCP Gleaning

This section provides information about DHCP Gleaning.

- Prerequisites for DHCP Gleaning, on page 1
- Information About DHCP Gleaning, on page 1
- Configuring an Interface as a Trusted or an Untrusted Source for DHCP Gleaning, on page 2
- Example: Configuring an Interface as a Trusted or an Untrusted Source for DHCP Gleaning, on page 3
- Additional References for DHCP Gleaning, on page 4
- Feature History for DHCP Gleaning, on page 4

Prerequisites for DHCP Gleaning

- Ensure that the interface to be configured is a Layer 2 interface.
- Ensure that global snooping is enabled.

Information About DHCP Gleaning

The following sections provide information about DHCP gleaning.

Overview of DHCP Gleaning

Gleaning helps extract location information from Dynamic Host Configuration Protocol (DHCP) messages when messages are forwarded by a DHCP relay agent; the process is a completely passive snooping functionality that neither blocks nor modifies DHCP packets. Additionally, gleaning helps to differentiate an untrusted device port that is connected to an end user from a trusted port connected to a DHCP server.

DHCP gleaning is a read–only DHCP snooping functionality that allows components to register and glean only DHCP version 4 packets. When you enable DHCP gleaning, it does a read-only snooping on all active interfaces on which DHCP snooping is disabled. You can add a secondary VLAN to a private VLAN. When add a secondary VLAN to a private VLAN, ensure that gleaning is enabled on the secondary VLAN, even though snooping is disabled on the primary VLAN. By default, the gleaning functionality is disabled. However, when you enable a device sensor, DHCP gleaning is automatically enabled.

DHCP Snooping

Dynamic Host Configuring Protocol (DHCP) snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and untrusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilizes 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.

Configuring 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.

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

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces

Note By default, all interfaces are untrusted.

Procedure

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

	Command or Action	Purpose
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 on an interface.
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.
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.

Example: Configuring an Interface as a Trusted or an Untrusted Source for DHCP Gleaning

This example shows how to enable Dynamic Host Configuration Protocol (DHCP) gleaning and configure an interface as a trusted interface:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping glean
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# ip dhcp snooping trust
Device(config-if)# end
```

Additional References for DHCP Gleaning

Standards and RFCs

Standard/RFC	Title
RFC-2131	*Dynamic Host Configuration Protocol*
RFC-4388	*DHCP Leasequery*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for DHCP Gleaning

This table provides release and related 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	Feature Information
Cisco IOS XE Dublin 17.10.1	DHCP Gleaning	DHCP gleaning is a read–only DHCP snooping functionality that allows components to register and glean only DHCP version 4 packets.

Use the Cisco Feature Navigator to find information about platform and software image support.