DHCP Gleaning

This document describes the Dynamic Host Configuration Protocol Gleaning feature.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

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

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, however, gleaning needs to be 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.

How to Configure DHCP Gleaning

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

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.

You can enable or disable DHCP gleaning on a device.

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping glean**
4. **interface fastethernet** *number*
5. **[no] ip dhcp snooping trust**
6. **end**
7. **show ip dhcp snooping statistics**

DETAILED STEPS

	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 on an interface.
Step 4	**interface fastethernet** *number* **Example:** Device(config)# interface fastEthernet 2 Device(config-if)#	Enters interface configuration mode, where *number* is the Layer 2 Ethernet interface where 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.

	Command or Action	Purpose
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.

Configuration Examples for 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 FastEthernet as a trusted interface:

```
ip dhcp snooping glean
interface fastethernet 5
 ip dhcp snooping trust
```

Additional References

Related Documents

Related Topic	Document Title
Master Commands List	Cisco IOS Master Commands List
DHCP Commands	Cisco IOS IP Addressing Services Command Reference
IP Source Guard	IP Source Guard
Dynamic ARP Inspection	Configuring Dynamic ARP Inspection

Standards and RFCs

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

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 Information for DHCP Gleaning

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for DHCP Gleaning

Feature Name	Releases	Feature Information
DHCP Gleaning	Cisco IOS 15.2E	This document describes the DHCP Gleaning feature. The following commands were introduced or modified for this feature:**ip dhcp snooping glean**, **show ip dhcp snooping glean**