CHAPTER 12

Configuring DHCP Snooping

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping and includes the following sections:

Information About DHCP Snooping

This section includes the following topics:

Overview

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers by doing the following:

- Validates DHCP messages received from untrusted sources and filters out invalid response messages from DHCP servers.
- 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.

Dynamic ARP inspection (DAI) and IP Source Guard also use information stored in the DHCP snooping binding database. For more information about these features, see Chapter 13, "Configuring Dynamic ARP Inspection" and Chapter 14, "Configuring IP Source Guard."

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

Trusted and Untrusted Sources

DHCP snooping identifies ports as trusted or untrusted. When you enable DHCP snooping, by default all vEthernet ports are untrusted and all ethernet ports (uplinks), port channels, special vEthernet ports (used by other features, such as VSD, for their operation) are trusted.You can configure whether DHCP trusts traffic sources.

In an enterprise network, a trusted source is a device that is under your administrative control. Any device beyond the firewall or outside the network is an untrusted source. Generally, host ports are treated as untrusted sources.

In a service provider environment, any device that is not in the service provider network is an untrusted source (such as a customer switch). Host ports are untrusted sources.

In the Cisco Nexus 1000V, you indicate that a source is trusted by configuring the trust state of its connecting interface. Uplink ports, as defined with the uplink capability on port profiles, are trusted and cannot be configured to be untrusted. This restriction prevents the uplink from being shut down for not conforming to rate limits or DHCP responses.

You can also configure other interfaces as trusted if they connect to devices (such as switches or routers) inside your network or if the administrator is running the DHCP server in a VM. You usually do not configure host port interfaces as trusted.

Note For DHCP snooping to function properly, all DHCP servers must be connected to the device through trusted interfaces.

DHCP Snooping Binding Database

Using information extracted from intercepted DHCP messages, DHCP snooping dynamically builds and maintains a database on each VEM. The database contains an entry for each untrusted host with a leased IP address if the host is associated with a VLAN that has DHCP snooping enabled. The database does not contain entries for hosts connected through trusted interfaces.

Note The DHCP snooping binding database is also referred to as the DHCP snooping binding table.

DHCP snooping updates the database when the device receives specific DHCP messages. For example, the feature adds an entry to the database when the device receives a DHCPACK message from the server. The feature removes the entry in the database when the IP address lease expires or the device receives a DHCPRELEASE or DHCP DECLINE from the DHCP client or a DHCPNACK from the DHCP server.

Each entry in the DHCP snooping binding database includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.

You can remove dynamically added entries from the binding database by using the **clear ip dhcp snooping binding** command. For more information, see the "Clearing the DHCP Snooping Binding Database" section on page 12-13.

Relay Agent Information Option

You can configure DHCP to add the VSM MAC address and vEthernet port in the DHCP packet. This is called the DHCP Relay Agent Information Option, or Option 82, and is inserted by the DHCP relay agent when forwarding DHCP packets. Server administrators may use the information to implement IP address assignment policies.

The relay agent identifies the following:

Information Option	Description
circuit ID	vEthernet port name
remote ID	VSM MAC address

For detailed information about the Relay Agent Information Option, see *RFC-3046, DHCP Relay Agent Information Option.*

To configure the relay agent, see the "Relaying Switch and Circuit Information in DHCP" procedure on page 12-15.

High Availability

The DHCP snooping binding table and all database entries created on the VEM are exported to the VSM and are persistent across VSM reboots.

Prerequisites for DHCP Snooping

DHCP snooping has the following prerequisites:

- You must be familiar with DHCP to configure DHCP snooping.

Guidelines and Limitations

DHCP snooping has the following configuration guidelines and limitations:

- A DHCP snooping database is stored on each VEM and can contain up to 1024 bindings.
- For seamless DHCP snooping, Virtual Service Domain (VSD) service VM ports are trusted ports by default. If you configure these ports as untrusted, this setting is ignored.
- If the VSM uses the VEM for connectivity (that is, the VSM has its VSM AIPC, management, and inband ports on a particular VEM), these virtual Ethernet interfaces must be configured as trusted interfaces.
- The connecting interfaces on a device upstream from the Cisco Nexus 1000V must be configured as trusted if DHCP snooping is enabled on the device.
- If you are configuring more than 128 ACLs (MAC and IP ACLs combined) then make sure the VSM RAM is set to be 3GB (3072 Mb). The procedure to change the RAM to 3GB is explained at Setting the VSM RAM size to 3072 Mb (hyperlink).

Default Settings

Table 12-1 lists the defaults for DHCP snooping.

Table 12-1 Default DHCP Snooping Parameters

Parameters	Default
DHCP feature	Disabled
DHCP snooping global	Disabled
DHCP snooping VLAN	Disabled
DHCP snooping MAC address verification	Enabled
DHCP snooping trust	Trusted for Ethernet interfaces, vEthernet interfaces, and port channels, in the VSD feature. Untrusted for vEthernet interfaces not participating in the VSD feature.

Configuring DHCP Snooping

This section includes the following topics:

Minimum DHCP Snooping Configuration

The minimum configuration for DHCP snooping is as follows:

Step 1 Enable the DHCP feature. For more information, see the "Enabling or Disabling the DHCP Feature" section on page 12-5.

Step 2 Enable DHCP snooping globally. For more information, see the "Enabling or Disabling DHCP Snooping Globally" section on page 12-6.

Step 3 Enable DHCP snooping on at least one VLAN. For more information, see the "Enabling or Disabling DHCP Snooping on a VLAN" section on page 12-7.

By default, DHCP snooping is disabled on all VLANs.

Step 4 Ensure that the DHCP server is connected to the device using a trusted interface. For more information, see the "Configuring an Interface as Trusted or Untrusted" section on page 12-9.

Enabling or Disabling the DHCP Feature

Use this procedure to globally enable or disable the DHCP feature.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- By default, DHCP is disabled.

SUMMARY STEPS

1. **config t**
2. **feature dhcp**
3. **show feature**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**feature dhcp** **Example:** n1000v(config)# feature dhcp **Example:** n1000v(config)# no feature dhcp	Enables DHCP snooping globally. The **no** option disables DHCP snooping but preserves an existing DHCP snooping configuration.
Step 3	**show feature** **Example:** n1000v(config)# show feature Feature Name Instance State -------------------- -------- -------- dhcp-snooping 1 enabled http-server 1 enabled lacp 1 enabled netflow 1 disabled port-profile-roles 1 enabled private-vlan 1 disabled sshServer 1 enabled tacacs 1 enabled telnetServer 1 enabled n1000v(config)#	Shows the state (enabled or disabled) of each available feature.
Step 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Enabling or Disabling DHCP Snooping Globally

Use this procedure to globally enable or disable the DHCP snooping.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- By default, DHCP snooping is globally disabled.
- If DHCP snooping is globally disabled, all DHCP snooping stops and no DHCP messages are relayed.
- If you configure DHCP snooping and then globally disable it, the remaining configuration is preserved.

SUMMARY STEPS

1. **config t**

2. **[no] ip dhcp snooping**
3. **show running-config dhcp**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**[no] ip dhcp snooping** **Example:** n1000v(config)# ip dhcp snooping	Enables DHCP snooping globally. The **no** option disables DHCP snooping but preserves an existing DHCP snooping configuration.
Step 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	Shows the DHCP snooping configuration.
Step 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Enabling or Disabling DHCP Snooping on a VLAN

Use this procedure to enable or disable DHCP snooping on one or more VLANs.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- By default, DHCP snooping is disabled on all VLANs.

SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp snooping vlan** *vlan-list*
3. **show running-config dhcp**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	[**no**] **ip dhcp snooping vlan** *vlan-list* **Example:** n1000v(config)# ip dhcp snooping vlan 100,200,250-252	Enables DHCP snooping on the VLANs specified by *vlan-list*. The **no** option disables DHCP snooping on the VLANs specified.
Step 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	Shows the DHCP snooping configuration.
Step 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Enabling or Disabling DHCP Snooping MAC Address Verification

Use this procedure to enable or disable DHCP snooping MAC address verification. If the device receives a packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, address verification causes the device to drop the packet.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- MAC address verification is enabled by default.

SUMMARY STEPS

1. **config t**
2. [**no**] **ip dhcp snooping verify mac-address**
3. **show running-config dhcp**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**[no] ip dhcp snooping verify mac-address** **Example:** n1000v(config)# ip dhcp snooping verify mac-address	Enables DHCP snooping MAC address verification. The **no** option disables MAC address verification.
Step 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp	Shows the DHCP snooping configuration.
Step 4	**copy running-config startup-config** **Example:** n1000v(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring an Interface as Trusted or Untrusted

Use this procedure to configure whether a virtual interface is a trusted or untrusted source of DHCP messages. You can configure DHCP trust on the following:

- Layer 2 vEthernet interfaces
- Port Profiles for Layer 2 vEthernet interfaces

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- By default, vEthernet interfaces are untrusted. The only exception is the special vEthernet ports used by other features such as VSD which are trusted
- Ensure that the vEthernet interface is configured as a Layer 2 interface.
- For seamless DHCP snooping, DAI, and IP Source Guard, Virtual Service Domain (VSD) service VM ports are trusted ports by default. If you configure these ports as untrusted, this setting is ignored.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *interface-number*

   port-profile *profilename*
3. **[no] ip dhcp snooping trust**
4. **show running-config dhcp**

5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**interface vethernet** *interface-number*
	
	Example:
	`n1000v(config)# interface vethernet 3`
	`n1000v(config-if)#`
		Enters interface configuration mode, where *interface-number* is the vEthernet interface that you want to configure as trusted or untrusted for DHCP snooping.

	port-profile *profilename*
	
	Example:
	`n1000v(config)# port-profile vm-data`
	`n1000v(config-port-prof)#`
		Enters port profile configuration mode for the specified port profile, where *profilename* is a unique name of up to 80 characters.

Step 3	[**no**] **ip dhcp snooping trust** **Example:** `n1000v(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 4	**show running-config dhcp** **Example:** `n1000v(config-if)# show running-config dhcp`	Shows the DHCP snooping configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring the Rate Limit for DHCP Packets

Use this procedure to configure a limit for the rate of DHCP packets per second received on each port.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Ports are put into an errdisabled state if they exceed the limit you set in this procedure for rate of DHCP packets per second.
- You can configure the rate limit on either the interface or port profile.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *interface-number*

port-profile *profilename*

3. **[no] ip dhcp snooping limit rate** *rate*
4. **show running-config dhcp**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**interface vethernet** *interface-number* **Example:** n1000v(config)# interface vethernet 3 n1000v(config-if)#	Enters interface configuration mode, where *interface-number* is the vEthernet interface for which you want to configure the DHCP packets per second limit.
	port-profile *profilename* **Example:** n1000v(config)# port-profile vm-data n1000v(config-port-prof)#	Enters port profile configuration mode for the specified port profile, where *profilename* is a unique name of up to 80 characters.
Step 3	[**no**] **ip dhcp snooping limit rate** *rate* **Example:** n1000v(config-port-prof)# ip dhcp snooping limit rate 30	Configures the limit for the rate of DHCP packets per second (1 - 2048). The **no** option removes the rate limit.
Step 4	**show running-config dhcp** **Example:** n1000v(config-if)# show running-config dhcp	Shows the DHCP snooping configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Detecting Ports Disabled for DHCP Rate Limit Violation

Use this procedure to globally configure detection of ports disabled for exceeding the DHCP rate limit.

BEFORE YOU BEGIN

Before beginning this procedures, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- A failure to conform to the set rate causes the port to be put into an errdisable state.
- You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from the error-disabled state.

SUMMARY STEPS

1. **config t**
2. **[no] errdisable detect cause dhcp-rate-limit**
3. **show running-config dhcp**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**[no] errdisable detect cause dhcp-rate-limit** **Example:** `n1000v(config)# errdisable detect cause dhcp-rate-limit`	Enables DHCP error-disabled detection. The **no** option disables DHCP error-disabled detection.
Step 3	**show running-config dhcp** **Example:** `n1000v(config)# show running-config dhcp`	Shows the DHCP snooping configuration.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Recovering Ports Disabled for DHCP Rate Limit Violations

Use this procedure to globally configure automatic recovery of ports disabled for violating the DHCP rate limit.

BEFORE YOU BEGIN

Before beginning this procedures, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Ports that rate causes the port to be put into an errdisable state.
- You must enter the **shutdown** command and then the **no shutdown** command to recover an interface manually from the error-disabled state.

SUMMARY STEPS

1. **config t**
2. **[no] errdisable recovery cause dhcp-rate-limit**
3. **errdisable recovery interval** *timer-interval*

4. **show running-config dhcp**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Enters global configuration mode.

Step 2	**[no] errdisable recovery cause dhcp-rate-limit** **Example:** `n1000v(config)# errdisable detect cause dhcp-rate-limit`	Enables DHCP error-disabled recovery. The **no** option disables DHCP error-recovery.
Step 3	**errdisable recovery interval** *timer-interval* **Example:** `n1000v(config)# errdisable recovery interval 30`	Sets the DHCP error-disabled recovery interval, where *timer-interval* is the number of seconds (30-65535).
Step 4	**show running-config dhcp** **Example:** `n1000v(config)# show running-config dhcp`	Shows the DHCP snooping configuration.
Step 5	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Clearing the DHCP Snooping Binding Database

This section includes the following procedures:

Clearing All Binding Entries

Use this procedure to remove all entries from the DHCP snooping binding database.

BEFORE YOU BEGIN

Before beginning this procedures, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **clear ip dhcp snooping binding**

2. **show ip dhcp snooping binding**

DETAILED STEPS

	Command	Purpose
Step 1	**clear ip dhcp snooping binding** **Example:** `n1000v# clear ip dhcp snooping binding`	Clears dynamically added entries from the DHCP snooping binding database.
Step 2	**show ip dhcp snooping binding** **Example:** `n1000v# show ip dhcp snooping binding`	Displays the DHCP snooping binding database.

Clearing Binding Entries for an Interface

Use this procedure to remove binding entries for an interface from the DHCP snooping database.

BEFORE YOU BEGIN

Before beginning this procedures, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have the following information for the interface:
  - VLAN ID
  - IP address
  - MAC address

SUMMARY STEPS

1. **clear ip dhcp snooping binding** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} | **vlan** *vlan-id1* | **interface** *interface-id1*]
2. **show ip dhcp snooping binding**

DETAILED STEPS

	Command	Purpose
Step 1	**clear ip dhcp snooping binding** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} | **vlan** *vlan-id1* | **interface** *interface-id1*] **Example:** `n1000v# clear ip dhcp snooping binding vlan 10 mac EEEE.EEEE.EEEE ip 10.10.10.1 interface vethernet 1`	Clears dynamically added entries for an interface from the DHCP snooping binding database.
Step 2	**show ip dhcp snooping binding** **Example:** `n1000v# show ip dhcp snooping binding`	Displays the DHCP snooping binding database.

Relaying Switch and Circuit Information in DHCP

Use this procedure to globally configure relaying of the VSM MAC address and vEthernet port information in DHCP packets. This is also called Option 82 and Relay Agent Information Option.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- For more information, see the following:
  - "Relay Agent Information Option" section on page 12-3
  - *RFC-3046, DHCP Relay Agent Information Option.*

SUMMARY STEPS

1. **config t**
2. **[no] ip dhcp snooping information option**
3. **show runing-config dhcp**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**[no] ip dhcp snooping information option** **Example:** n1000v(config)# ip dhcp snooping information option n1000v(config)#	Configures DHCP to relay the VSM MAC address and vEthernet port information in DHCP packets. Use the **no** option to remove this configuration.
Step 3	**show running-config dhcp** **Example:** n1000v(config)# show running-config dhcp !Command: show running-config dhcp !Time: Fri Dec 17 11:30:22 2010 version 4.2(1)SV1(4) ip dhcp snooping information option service dhcp ip dhcp relay ip dhcp relay information option n1000v(config)#	(Optional) Displays the DHCP snooping configuration for verification.

	Command	Purpose
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the DHCP Snooping Configuration

To verify the DHCP snooping configuration, use the following commands:

Command	Purpose
show running-config dhcp	Displays the DHCP snooping configuration
show ip dhcp snooping	Displays general information about DHCP snooping.
show ip dhcp snooping binding	Display the contents of the DHCP snooping binding table.
show feature	Displays the features available, such as DHCP, and whether they are enabled.

For detailed information about these commands, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*.

Monitoring DHCP Snooping

Use the **show ip dhcp snooping statistics** command to monitor DHCP snooping statistics. For detailed information about this command, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*.

Example Configuration for DHCP Snooping

This example shows how to enable DHCP snooping on two VLANs, with vEthernet interface 5 trusted because the DHCP server is connected to that interface:

```
feature dhcp

interface vethernet 5
ip dhcp snooping trust
ip dhcp snooping vlan 1, 50
```

Additional References

For additional information related to implementing DHCP snooping, see the following sections:

- Related Documents, page 12-17
- Standards, page 12-17

Related Documents

Related Topic	Document Title
IP Source Guard	*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a)*, Chapter 14, "Configuring IP Source Guard"
Dynamic ARP Inspection	*Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(4a)*, Chapter 13, "Configuring Dynamic ARP Inspection"
DHCP snooping commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*

Standards

Standards	Title
RFC-2131	*Dynamic Host Configuration Protocol* (http://tools.ietf.org/html/rfc2131)
RFC-3046	*DHCP Relay Agent Information Option* (http://tools.ietf.org/html/rfc3046)

Feature History for DHCP Snooping

Table 12-2 lists the release history for this feature.

Table 12-2 Feature History for DHCP Snooping

Feature Name	Releases	Feature Information
Relay Agent (Option 82)	4.2(1)SV1(4)	You can configure relaying of VSM MAC and port information in DHCP packets.
feature dhcp command	4.2(1)SV1(4)	Command added for enabling DHCP feature globally.
DHCP snooping	4.0(4)SV1(2)	This feature was introduced.