Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 14

Configuring DHCP Snooping

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on an NX-OS device.

This chapter includes the following sections:

Information About 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.

Dynamic ARP inspection (DAI) and IP Source Guard also use 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 a range of VLANs.

Trusted and Untrusted Sources

Note

DHCP Snooping Binding Database

Note

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 message from the host.

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.

"Clearing the DHCP Snooping Binding Database" section on page 14-17.

DHCP Relay Agent

Packet Validation

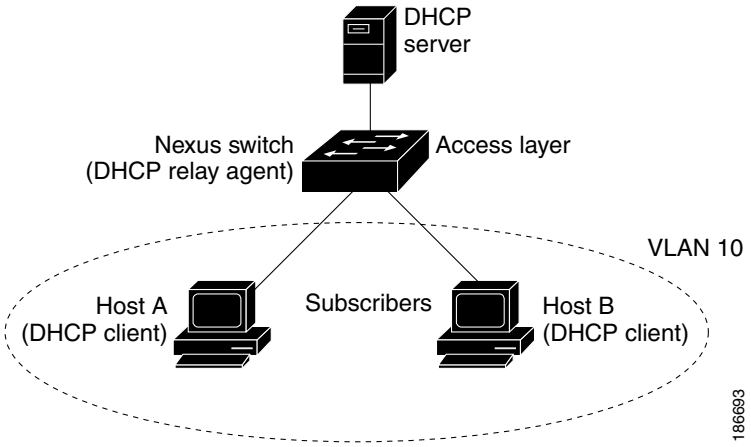
-
-
-
- The device receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0.

DHCP Snooping Option-82 Data Insertion

assignments for a large number of subscribers. When you enable option 82, the device identifies a subscriber device that connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can connect to the same port on the access device and are uniquely identified.

Figure 14-1 shows an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the device at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

Figure 14-1 DHCP Relay Agent in a Metropolitan Ethernet Network



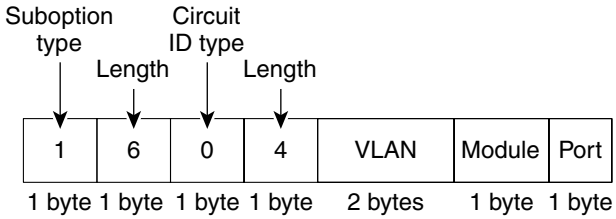
When you enable option 82 on the NX-OS device, the following sequence of events occurs:

1.
2.
3.
4.
5.
6.

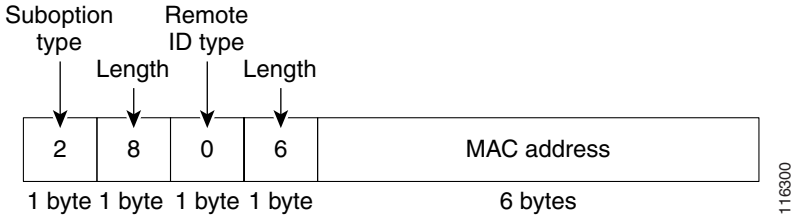
-
  -
  -
  -
  -
  -
  -
  -
  -

Figure 14-2 Suboption Packet Formats

Circuit ID Suboption Frame Format



Remote ID Suboption Frame Format



Virtualization Support for DHCP Snooping

-
-

Licensing Requirements for DHCP Snooping

Product	License Requirement
	Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0

Guidelines and Limitations

- **feature dhcp**
  approximately 30 seconds before the I/O modules receive DHCP snooping or DAI configuration. This delay occurs regardless of the method that you use to change from a configuration with DHCP snooping disabled to a configuration with DHCP snooping enabled. For example, if you use the Rollback feature to revert to a configuration that enables DHCP snooping, the I/O modules receive DHCP snooping and DAI configuration approximately 30 seconds after you complete the rollback.

  The DHCP snooping database can store 2000 bindings.

  DHCP snooping is not active until you enable the feature, enable DHCP snooping globally, and enable DHCP snooping on at least one VLAN.

  Before globally enabling DHCP snooping on the device, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.

  Access-control list (ACL) statistics are not supported if the DHCP snooping feature is enabled.

This section includes the following topics:

Minimum DHCP Snooping Configuration

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

Enabling or Disabling the DHCP Snooping Feature

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2. [ ]
   show running-config dhcp
   copy running-config startup-config

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	
	[ ] **feature dhcp** **Example:** switch(config)# feature dhcp	
	show running-config dhcp **Example:** switch(config)# show running-config dhcp	
	copy running-config startup-config **Example:** switch(config)# copy running-config startup-config	

Enabling or Disabling DHCP Snooping Globally

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.

Enabling or Disabling DHCP Snooping on a VLAN

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2. **vlan** *vlan-list*

dhcp snooping vlan *vlan-list* `switch(config)# ip dhcp snooping vlan 100,200,250-252`	
`switch(config)# show running-config dhcp`	
`switch(config)# copy running-config startup-config`	

dhcp snooping verify mac-address

show running-config dhcp

copy running-config startup-config

	Command	Purpose
Step 1	switch# config t switch(config)#	
Step 2	[ ]	
	switch(config)# ip dhcp snooping verify mac-address	
	switch(config)# show running-config dhcp	
	switch(config)# copy running-config startup-config	

Enabling or Disabling Option-82 Data Insertion and Removal

Note

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.

/port

channel-number

slot/*port* switch(config)# interface ethernet 2/1 switch(config-if)#	
channel-number	

BOOTREQUEST packet arrives on the interface, the relay agent forwards the packet to all DHCP server IP address specified. The relay agent forwards replies from all DHCP servers to the host that sent the request. In Cisco NX-OS Release 4.0.2 and earlier, you can configure only one DHCP server IP address on an interface.

By default, there is no DHCP server IP address configured on an interface.

Ensure that the DHCP server is correctly configured.

Determine the IP address for each DHCP server that you want to .

Ensure that DHCP snooping is enabled. For more information, see the "Enabling or Disabling the DHCP Snooping Feature" section on page 14-7.

[.

interface vlan

interface port-channel

ip dhcp relay address *IP-address*

DETAILED STEPS

	Command	Purpose
Step 1		

Step 2	.
	
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`	

	vlan-id	

	channel-id
	
	`switch(config)# interface port-channel 7`
	`switch(config-if)#`	

	IP-address `10.132.7.120`	
	`switch(config-if)# show running-config dhcp`	
	`switch(config-if)# copy running-config startup-config`	

Verifying DHCP Snooping Configuration

Series NX-OS Security Command Reference, Release 4.0

Displaying DHCP Bindings

Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 4.0

Clearing the DHCP Snooping Binding Database

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.

DETAILED STEPS

	Command	Purpose
Step 1	**clear ip dhcp snooping binding** **Example:** switch# clear ip dhcp snooping binding	
	switch# ip dhcp snooping binding	

Example Configuration for DHCP Snooping

```
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet2/5
  ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```

```
feature dhcp
ip dhcp snoop
service dhcp
ip dhcp relay information option

interface Ethernet2/3
  ip dhcp relay address 10.132.7.120
```

Table 14-1 Default DHCP Snooping Parameters

	Default

Related Documents

Related Topic	Document Title

Standards

Standards	Title
	Dynamic Host Configuration Protocol
	DHCP Relay Agent Information Option

Feature History for DHCP Snooping

Feature Name	Releases	Feature Information