CHAPTER 19

DHCP, DAI, and IPSG

This chapter describes how to identify and resolve problems related to the following security features:

- Dynamic Host Configuration Protocol (DHCP) Snooping
- Dynamic ARP Inspection (DAI)
- IP Source Guard (IPSG)

This chapter includes the following sections:

- Information About DHCP Snooping, page 19-1
- Information About Dynamic ARP Inspection, page 19-2
- Information About IP Source Guard, page 19-2
- Guidelines and Limitations for Troubleshooting, page 19-2
- Problems with DHCP Snooping, page 19-3
- Troubleshooting Dropped ARP Responses, page 19-4
- Problems with IP Source Guard, page 19-5
- Collecting and Evaluating Logs, page 19-5
- DHCP, DAI, and IPSG Troubleshooting Commands, page 19-6

Information About DHCP Snooping

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 detailed information about configuring DHCP snooping, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.

Information About Dynamic ARP Inspection

DAI is used to validate ARP requests and responses as follows:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that a packet has a valid IP-to-MAC address binding before updating the ARP cache or forwarding the packet.
- Drops invalid ARP packets.

DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a Dynamic Host Configuration Protocol (DHCP) snooping binding database. This database is built by DHCP snooping when it is enabled on the VLANs and on the device. It may also contain static entries that you have created.

For detailed information about configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.

Information About IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches the IP and MAC address bindings of dynamic or static IP source entries in the Dynamic Host Configuration Protocol (DHCP) snooping binding table.

For detailed information about configuring IP Source Guard, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.

Guidelines and Limitations for Troubleshooting

The following guidelines and limitations apply when troubleshooting DHCP snooping, Dynamic ARP Inspection, or IP Source Guard:

- A maximum of 2000 DHCP entries can be snooped and learned system-wide in the DVS. This is a combined total for both entries learned dynamically and entries configured statically.
- Rate limits on interfaces must be set to high values for trusted interfaces such as VSD SVM ports or vEthernet ports connecting to DHCP servers.

For detailed guidelines and limitations used in configuring these features, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.

Problems with DHCP Snooping

The following are symptoms, possible causes, and solutions for problems with DHCP snooping.

Symptom	Possible Causes	Solution
With snooping configured, DHCP client is not able to obtain an IP address from the server.	IP address was not added to binding database. Faulty connection between DHCP server and client.	1. Verify the connection between the DHCP server(s) and the host connected to the client. **vmkping** 2. If the connection between DHCP server and the host is broken, do the following: – Check the configuration in the upstream switch, for example, verifying that the VLAN is allowed, etc. – Make sure the server itself is up and running.
	The interface of the DHCP server(s) connected to the DVS as a VM is not trusted.	1. On the VSM, verify that the interface is trusted. **show ip dhcp snooping** 2. On the VSM, verify the vEthernet interface attached to the server is trusted. **module vem** *mod#* **execute vemcmd show dhcps interfaces**
	DHCP requests from the VM are not reaching the server for acknowledgement.	On the DHCP server, log in and use a packet capture utility to verify requests and acknowledgements in packets.
	DHCP requests and acknowledgements are not reaching the Cisco Nexus 1000V.	• From the client vEthernet interface, SPAN the packets to verify they are reaching the client. • On the host connected to the client, enable VEM packet capture to verify incoming requests and acknowledgements in packets.
	The Cisco Nexus 1000V is dropping packets.	On the VSM, verify DHCP statistics. **show ip dhcp snooping statistics** **module vem** *mod#* **execute vemcmd show dhcps stats**

Troubleshooting Dropped ARP Responses

The following are possible causes, and solutions for dropped ARP responses.

Possible Causes	Solution
ARP inspection is not configured on the VSM	On the VSM, verify that ARP inspection is configured as expected. **show ip arp inspection** For detailed information about configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*
DHCP snooping is not enabled globally on the VSM, or is not enabled on the VLAN.	On the VSM, verify the DHCP snooping configuration. **show ip dhcp snooping** For detailed information about enabling DHCP, and configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.
DHCP snooping is not enabled on the VEM, or is not enabled on the VLAN.	1. From the VSM, verify the VEM DHCP snooping configuration. **module vem** *mod#* **execute vemcmd show dhcps vlan** 2. Do one of the following: – Correct any errors in the VSM DHCP configuration. For detailed information, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*. – If the configuration appears correct on the VSM but fails on the VEM, capture and analyze the error logs from both VSM and the VEM to identify the reason for the failure.
If snooping is disabled, the binding entry is not statically configured in the binding table.	1. On the VSM, display the binding table. **show ip dhcp snooping binding** 2. Correct any errors in the static binding table. For detailed information about clearing entries from the table, enabling DHCP, and configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.
The binding corresponding to the VM sending the ARP response is not present in the binding table.	1. On the VSM, display the binding table. **show ip dhcp snooping binding** 2. Correct any errors in the static binding table. For detailed information about clearing entries from the table, enabling DHCP, and configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*. 3. If all configurations are correct, make sure to turn on DHCP snooping before DAI or IPSG. This is to make sure the Cisco Nexus 1000V has enough time to add the binding in the snooping database. For more information, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*.

Problems with IP Source Guard

The following are symptoms, possible causes, and solutions for problems with IP Source Guard.

Symptom	Possible Causes	Solution
Traffic disruptions	ARP inspection is not configured on the VSM.	On the VSM, verify that IP Source Guard is configured as expected. **show port-profile name** *profile_name* **show running interface** *if_ID* **show ip verify source** For detailed information about configuring IP Source Guard, see the *Cisco Nexus 1000V Security Configuration Guide, Release 4.2(1)SV1(5.1)*
	The IP address corresponding to the vEthernet interface is not in the snooping binding table.	1. On the VSM, display the binding table. **show ip dhcp snooping binding** 2. Configure the missing static entry or renew the lease on the VM. 3. On the VSM, display the binding table again to verify the entry is added correctly. **show ip dhcp snooping binding**

Collecting and Evaluating Logs

You can use the commands in this section from the VSM to collect and view logs related to DHCP, DAI, and IP Source Guard.

- VSM Logging, page 19-5
- Host Logging, page 19-6

VSM Logging

You can use the commands in this section from the VSM to collect and view logs related to DHCP, DAI, and IP Source Guard.

VSM Command	Description
debug dhcp all	Enable debug all for dhcp configuration flags
debug dhcp errors	Enable debugging of errors
debug dhcp mts-errors	Enable debugging of mts errors
debug dhcp mts-events	Enable debugging of mts events
debug dhcp pkt-events	Enable debugging of pkt events
debug dhcp pss-errors	Enable debugging of pss errors
debug dhcp pss-events	Enable debugging of pss events

Host Logging

You can use the commands in this section from the ESX host to collect and view logs related to DHCP, DAI, and IP Source Guard.

ESX Host Command	Description
echo "logfile enable" > /tmp/dpafifo	Enables DPA debug logging. Logs are output to /var/log/vemdpa.log file.
echo "debug sfdhcpsagent all" > /tmp/dpafifo	Enables DPA DHCP agent debug logging. Logs are output to /var/log/vemdpa.log file.
vemlog debug sfdhcps all	Enables datapath debug logging, and captures logs for the data packets sent between the client and the server.
vemlog debug sfdhcps_config all	Enables datapath debug logging, and captures logs for configuration coming from the VSM.
vemlog debug sfdhcps_binding_table all	Enables datapath debug logging, and captures logs corresponding to binding database changes.

DHCP, DAI, and IPSG Troubleshooting Commands

You can use the commands in this section to troubleshoot problems related to DHCP snooping, DAI, and IP Source Guard.

Command	Description
show running-config dhcp	Displays the DHCP snooping, DAI, and IP Source Guard configuration See Example 19-1 on page 19-7.
show ip dhcp snooping	Displays general information about DHCP snooping. See Example 19-2 on page 19-7.
show ip dhcp snooping binding	Display the contents of the DHCP snooping binding table. See Example 19-3 on page 19-7.
show feature	Displays the features available, such as DHCP, and whether they are enabled. See Example 19-4 on page 19-7.
show ip arp inspection	Displays the status of DAI. See Example 19-5 on page 19-8.
show ip arp inspection interface vethernet *interface-number*	Displays the trust state and ARP packet rate for a specific interface. See Example 19-6 on page 19-8.

Command	Description
show ip arp inspection vlan *vlan-ID*	Displays the DAI configuration for a specific VLAN. See Example 19-7 on page 19-8.
show ip verify source	Displays interfaces where IP source guard is enabled and the IP-MAC address bindings. See Example 19-8 on page 19-9.

Example 19-1 show running-config dhcp

```
n1000v# show running-config dhcp

!Command: show running-config dhcp
!Time: Wed Feb 16 14:20:36 2011

version 4.2(1)SV1(4)
feature dhcp

no ip dhcp relay

n1000v#
```

Example 19-2 show ip dhcp snooping

```
n1000v# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
vEthernet 3           Yes

n1000v#
```

Example 19-3 show ip dhcp snooping binding

```
n1000v# show ip dhcp snooping binding
MacAddress         IpAddress        LeaseSec  Type        VLAN  Interface
-----------------  ---------------  --------  ----------  ----  -------------
0f:00:60:b3:23:33  10.3.2.2         infinite  static      13    vEthernet 6
0f:00:60:b3:23:35  10.2.2.2         infinite  static      100   vEthernet 10
n1000v#
```

Example 19-4 show feature

```
n1000v# show feature
Feature Name          Instance  State
--------------------  --------  --------
dhcp-snooping         1         enabled
http-server           1         enabled
ippool                1         enabled
```

```
lacp                  1         enabled
lisp                  1         enabled
lisphelper            1         enabled
netflow               1         disabled
port-profile-roles    1         enabled
private-vlan          1         disabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
n1000v#
```

Example 19-5 show ip arp inspection

```
n1000v# show ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan : 1
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 5
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 100
-----------
Configuration          : Disabled
Operation State        : Inactive

Vlan : 101
-----------
Configuration          : Disabled
Operation State        : Inactive
n1000v#
```

Example 19-6 show ip arp inspection interface

```
n1000v# show ip arp inspection interface vethernet 6

 Interface        Trust State
 -------------    -----------
 vEthernet 6        Trusted
n1000v#
```

Example 19-7 show ip arp inspection vlan

```
n1000v# show ip arp inspection vlan 13

Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

n1000v#
```

Example 19-8 show ip verify source

```
n1000v# show ip arp inspection vlan 13
IP source guard is  enabled on the following interfaces:
---------------------------------------------------------------------------
     Vethernet1

Interface         Filter-mode     IP-address     Mac-address       Vlan
------------      -----------     ----------     --------------    ----
Vethernet11      active           25.0.0.128     00:50:56:88:00:20  25
```