DHCP, DAI, and IPSG

This chapter describes how to identify and resolve problems related to Dynamic Host Configuration Protocol, Dynamic ARP Inspection, and IP Source Guard. This chapter contains the following sections:

Information About DHCP Snooping

Dynamic Host Configuration Protocol (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 (IPSG) 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*.

Information About DAI

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 DHCP snooping binding database. This database is built by DHCP snooping when it is enabled on the VLANs and on the device. It might also contain static entries that you have created.

For detailed information about configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide*.

Information About IPSG

IPSG 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 DHCP snooping binding table.

For detailed information about configuring IP Source Guard, see the *Cisco Nexus 1000V Security Configuration Guide*.

Guidelines and Limitations for Troubleshooting DHCP Snooping, DAI, or IPSG

The following guidelines and limitations apply when troubleshooting DHCP snooping, DAI, or IPSG:

- A maximum of 12,000 DHCP entries can be snooped and learned system-wide in the DVS. This combined total is 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 that connect to DHCP servers.
- Rate limits for trusted interfaces will be ignored.
- A maximum of 2000 DHCP entries per host can be learned dynamically and configured statically.
- A maximum of 1000 static DHCP entries per interface can be configured.

For detailed guidelines and limitations used in configuring these features, see the *Cisco Nexus 1000V Security Configuration Guide*.

Problems with DHCP Snooping

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

Symptom	Possible Causes	Solution
With snooping configured, the DHCP client is not able to obtain an IP address from the server.	The IP address was not added to the binding database. A faulty connection is between the DHCP server and client.	1. Verify the connection between the DHCP server(s) and the host connected to the client by using the **vmkping** command. 2. If the connection between the DHCP server and the host is broken, do the following: 1. Check the configuration in the upstream switch, for example, verifying that the VLAN is allowed. 2. Make sure that the server is up and running.
	The interface of the DHCP server(s) connected to the DVS as a VM is not trusted.	Do the following on the VSM: 1. Verify that the interface is trusted by using the **show ip dhcp snooping** command. 2. Verify that the vEthernet interface attached to the server is trusted by using the **module vem** *module-number* **execute vemcmd show dhcps interfaces** command.
	DHCP requests from the VM are not reaching the server for acknowledgment.	On the DHCP server, log in and use a packet capture utility to verify requests and acknowledgments in packets.
	DHCP requests and acknowledgments are not reaching 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 acknowledgments in packets.
	Cisco Nexus 1000V is dropping packets.	On the VSM, verify DHCP statistics by using the following commands: • **show ip dhcp snooping statistics** • **module vem** *module-number* **execute vemcmd show dhcps interfaces**

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 by using the **show ip arp inspection** command. For detailed information about configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide*.

Possible Causes	Solution
DHCP snooping is not enabled globally on the VSM or is not enabled on the VLAN.	On the VSM, verify the DHCP snooping configuration by using the **show ip dhcp snooping** command. For detailed information about enabling DHCP and configuring DAI, see the *Cisco Nexus 1000V Security Configuration Guide*.
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 by using the **module vem** *module-number* **execute vemcmd show dhcps vlan** command. **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*. • If the configuration appears correct on the VSM but fails on the VEM, capture and analyze the error logs from both the 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 by using the **show ip dhcp snooping binding** command. **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*.
The binding that corresponds to the VM sending the ARP response is not present in the binding table.	**1.** On the VSM, display the binding table by using the **show ip dhcp snooping binding** command. **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*. **3.** If all configurations are correct, make sure to turn on DHCP snooping before DAI or IPSG 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*.

Problems with IP Source Guard

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

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

Collecting and Evaluating Logs

VSM Logging Commands

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

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

Host Logging Commands

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

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 data path debug logging and captures logs for the data packets sent between the client and the server.
vemlog debug sfdhcps_pod all	Captures Port Opaque Data (POD) logging for the feature.
vemlog debug sfdhcps_config all	Enables data path debug logging and captures logs for configuration coming from the VSM.
vemlog debug sfdhcps_binding_table all	Enables data path debug logging and captures logs that correspond 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 IPSG.

Command	Description
show running-config dhcp	Displays the DHCP snooping, DAI, and IPSG configuration. See show running-config dhcp, on page 7.
show ip dhcp snooping	Displays general information about DHCP snooping. See show ip dhcp snooping, on page 7.
show ip dhcp snooping binding	Displays the contents of the DHCP snooping binding table. See show ip dhcp snooping binding, on page 7.
show feature	Displays the features available, such as DHCP, and whether they are enabled. See show feature, on page 7.
show ip arp inspection	Displays the status of DAI. See show ip arp inspection, on page 8.
show ip arp inspection interface vethernet *interface-number*	Displays the trust state and ARP packet rate for a specific interface. See show ip arp inspection interface vethernet, on page 8.
show ip arp inspection vlan *vlan-ID*	Displays the DAI configuration for a specific VLAN. See show ip arp inspection vlan, on page 8.

Command	Description
show ip verify source	Displays the IP-MAC address bindings and the interfaces where IPSG is enabled. See show ip verify source, on page 8.
show system internal dhcp {event-history | mem-stats | msgs}	Debugs any issues in the filter-mode configuration. See show system internal dhcp, on page 9.
debug dhcp all	Enables debug all for DHCP configuration flags on the VSM.

Command Examples

show running-config dhcp

```
switch# 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

switch#
```

show ip dhcp snooping

```
switch# 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

switch#
```

show ip dhcp snooping binding

```
switch# 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
switch#
```

show feature

```
switch# 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
switch#
```

show ip arp inspection

```
switch(config)# show ip arp inspection

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

Filter Mode(for static bindings): IP-MAC

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

Vlan : 40
-----------
Configuration : Disabled
Operation State : Inactive
```

show ip arp inspection interface vethernet

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

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

show ip arp inspection vlan

```
switch# show ip arp inspection vlan 13

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

switch#
```

show ip verify source

```
switch# show ip verify source
Filter Mode(for static bindings): IP-MAC
IP source guard is enabled on the following interfaces:
---------------------------------------------------
Vethernet11
```

```
IP source guard operational entries:
-----------------------------------
Interface Filter-mode IP-address Mac-address Vlan
------------ ----------- ---------- -------------- ----
Vethernet11 active 205.2.5.80 00:50:56:a4:38:ec 5
```

show system internal dhcp

```
switch# show system internal dhcp msgs
1) Event:E_DEBUG, length:75, at 409832 usecs after Mon Oct 8 20:57:48 2012
[16843009] Session close, handle -767541913, sess-id 0xff0101ba02812d08, state 3

2) Event:E_DEBUG, length:62, at 399944 usecs after Mon Oct 8 20:57:48 2012
[16843009] PPF session open session-id 0xff0101ba02812d08, msg_id 0

3) Event:E_DEBUG, length:30, at 399866 usecs after Mon Oct 8 20:57:48 2012
[16843009] PPF goto setting state 1

4) Event:E_DEBUG, length:23, at 682346 usecs after Mon Oct 8 20:57:11 2012
[16843009] Processed log-mts
...


VSM-N1k# show system internal dhcp mem-stats detail

Private Mem stats for UUID : Malloc track Library(103) Max types: 5
--------------------------------------------------------------------------------
TYPE NAME ALLOCS BYTES
CURR MAX CURR MAX
2 MT_MEM_mtrack_hdl 33 34 19236 19384
3 MT_MEM_mtrack_info 588 880 9408 14080
4 MT_MEM_mtrack_lib_name 882 1174 42246 56230
--------------------------------------------------------------------------------
Total bytes: 70890 (69k)
--------------------------------------------------------------------------------

Private Mem stats for UUID : Non mtrack users(0) Max types: 149
--------------------------------------------------------------------------------
TYPE NAME ALLOCS BYTES
CURR MAX CURR MAX
11 [r-xp]/isan/plugin/0/isan/lib/libavl.so 3421 3421 68360 68360
26 [r-xp]/isan/plugin/0/isan/lib/libddbcom 116 141 302445 308307
47 [r-xp]/isan/plugin/0/isan/lib/libindxob 6 6 456 456
50 [r-xp]/isan/plugin/0/isan/lib/libip.so. 1 1 212 212
64 [r-xp]/isan/plugin/0/isan/lib/libmpmts. 0 9 0 785
66 [r-xp]/isan/plugin/0/isan/lib/libmts.so 10 11 972 984
68 [r-xp]/isan/plugin/0/isan/lib/libnetsta 1 2 704 1350
81 [r-xp]/isan/plugin/0/isan/lib/libpss.so 158 262 101579 204281
85 [r-xp]/isan/plugin/0/isan/lib/libsdb.so 44 44 3914 3914
89 [r-xp]/isan/plugin/0/isan/lib/libsmm.so 3 3 216 216
111 [r-xp]/isan/plugin/0/isan/lib/libutils. 4 7 69 349
112 [r-xp]/isan/plugin/0/isan/lib/libvdc_mg 0 1 0 20
118 [r-xp]/isan/plugin/2/isan/bin/dhcp_snoo 0 2 0 64
121 [r-xp]/isan/plugin/2/isan/lib/libpdlser 4 29 208 1016
128 [r-xp]/lib/ld-2.3.3.so 33 33 5363 5371
131 [r-xp]/lib/tls/libc-2.3.3.so 51 51 1347 1637
134 [r-xp]/lib/tls/libpthread-2.3.3.so 1 1 33 33
138 [r-xp]/usr/lib/libglib-2.0.so.0.600.1 15 16 10372 10392
145 [r-xp]/isan/plugin/1/isan/lib/libvem_mg 0 1 0 1940
--------------------------------------------------------------------------------
Total bytes: 496250 (484k)
```

```
--------------------------------------------------------------------------------
...



switch# show system internal dhcp event-history msgs
1) Event:E_MTS_RX, length:60, at 809122 usecs after Mon Oct 8 20:59:08 2012
[RSP] Opc:MTS_OPC_PDL32(148511), Id:0X00F132AB, Ret:SUCCESS
Src:0x00000302/747, Dst:0x00000201/360, Flags:None
HA_SEQNO:0X00000000, RRtoken:0x00009498, Sync:UNKNOWN, Payloadsize:132
Payload:
0x0000: 00 00 00 03 00 00 00 01 00 00 00 64 00 00 00 07

2) Event:E_MTS_RX, length:60, at 809100 usecs after Mon Oct 8 20:59:08 2012
[RSP] Opc:MTS_OPC_PDL32(148511), Id:0X00E01555, Ret:SUCCESS
Src:0x00000502/747, Dst:0x00000201/360, Flags:None
HA_SEQNO:0X00000000, RRtoken:0x00009497, Sync:UNKNOWN, Payloadsize:132
Payload:
0x0000: 00 00 00 03 00 00 00 01 00 00 00 64 00 00 00 07

3) Event:E_MTS_RX, length:60, at 809079 usecs after Mon Oct 8 20:59:08 2012
[RSP] Opc:MTS_OPC_PDL32(148511), Id:0X006BE1FC, Ret:SUCCESS
Src:0x00000602/747, Dst:0x00000201/360, Flags:None
HA_SEQNO:0X00000000, RRtoken:0x00009496, Sync:UNKNOWN, Payloadsize:132
Payload:
0x0000: 00 00 00 03 00 00 00 01 00 00 00 64 00 00 00 07

4) Event:E_MTS_RX, length:60, at 809028 usecs after Mon Oct 8 20:59:08 2012
[RSP] Opc:MTS_OPC_PDL32(148511), Id:0X00F132AA, Ret:SUCCESS
Src:0x00000302/747, Dst:0x00000201/360, Flags:None
HA_SEQNO:0X00000000, RRtoken:0x00009474, Sync:UNKNOWN, Payloadsize:132
Payload:
0x0000: 00 00 00 03 00 00 00 01 00 00 00 64 00 00 00 07
contd.
```