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 Address Resolution Protocol (ARP) Inspection (DAI)
- IP Source Guard (IPSG)

Information About DHCP Snooping

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

- Validates DHCP messages that are 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 for Microsoft Hyper-V Security Configuration Guide*.

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 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 for Microsoft Hyper-V Security Configuration Guide*.

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 DHCP snooping binding table.

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

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 2048 DHCP entries can be snooped and learned system-wide in the distributed virtual switch (DVS). This total is for both entries learned dynamically and entries configured statically.
- Rate limits on interfaces that must be set to high values for trusted interfaces such as VSD SVM ports or vEthernet ports that connect to DHCP servers.
- If the Virtual Supervisor Module (VSM) uses the Virtual Ethernet Module (VEM) for connectivity (that is, the VSM has a VSM Asynchronous Inter-process Communication (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.

For detailed guidelines and limitations used in configuring these features, see the *Cisco Nexus 1000V for Microsoft Hyper-V 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.	IP address was not added to binding database. The connection is faulty between the DHCP server and client.	1. Verify the connection between the DHCP server(s) and the host connected to the client by entering the **vmkping** command. 2. If the connection between the DHCP server and the host is broken, do the following: – Check the configuration in the upstream switch. For example, verify that the VLAN is allowed, and so on. – Make sure that the server itself is up and running. – Make sure that global DHCP snooping (IP DHCP snooping) is configured on the VSM
	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 by entering the **show ip dhcp snooping** command. 2. On the VSM, verify that the vEthernet interface attached to the server is trusted by entering the **module vem** *module-number* **execute vemcmd show dhcps interfaces** command.
	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 that 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 by entering these commands. • **show ip dhcp snooping statistics** • **module vem** *module-number* **execute vemcmd show dhcps stats**

Dropped ARP Response Troubleshooting

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 entering the **show ip arp inspection** command. For detailed information about configuring DAI, see the *Cisco Nexus 1000V for Microsoft Hyper-V Security Configuration Guide*.
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 entering the **show ip dhcp snooping** command. For detailed information about enabling DHCP and configuring DAI, see the *Cisco Nexus 1000V for Microsoft Hyper-V 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 entering 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 for Microsoft Hyper-V Security Configuration Guide*. – 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 by entering 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 for Microsoft Hyper-V 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 entering 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 for Microsoft Hyper-V Security Configuration Guide*. 3. If all configurations are correct, make sure to turn on DHCP snooping before DAI or IPSG to make sure that the Cisco Nexus 1000V has enough time to add the binding in the snooping database. For more information, see the *Cisco Nexus 1000V for Microsoft Hyper-V Security Configuration Guide*.

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 by entering these commands: • **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 for Microsoft Hyper-V Security Configuration Guide*.
	The IP address corresponding to the vEthernet interface is not in the snooping binding table.	1. On the VSM, display the binding table by entering 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 the entry is added correctly by entering the **show ip dhcp snooping binding** command.

Collecting and Evaluating Logs

This section includes the following topics:

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	Enables debugging for all DHCP configuration flags.
debug dhcp errors	Enables debugging of DHCP 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

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.

Hyper-V Host Command	Description
vemcmd.exe dpa debug sfdhcpsagent all	Enables DPA DHCP agent debug logging. Enter the **vemlog.exe show all** command to view the log messages.
vemlog.exe debug sfdhcps all	Enables data-path debug logging, and captures logs for the data packets sent between the client and the server.
vemlog.exe debug sfdhcps_config all	Enables data-path debug logging, and captures logs for configuration that is coming from the VSM.
vemlog.exe 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 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 and whether option 82 is enabled. 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 Command

```
n1000v# show running-config dhcp

!Command: show running-config dhcp
!Time: Fri Feb  8 19:29:50 2013

version 5.2(1)SM1(5.1)
feature dhcp

no ip dhcp relayy

n1000v#
```

Example 19-2 show ip dhcp snooping Command

```
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 Command

```
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 Command

```
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 Command

```
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 Command

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

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

Example 19-7 show ip arp inspection vlan Command

```
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 Command

```
n1000v# show ip verify source
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
```