Configuring DHCP Snooping

This chapter contains the following sections:

- Information About DHCP Snooping, page 1
- DHCP Overview, page 2
- BOOTP Packet Format, page 4
- Trusted and Untrusted Sources, page 6
- DHCP Snooping Binding Database, page 7
- DHCP Snooping Option 82 Data Insertion, page 7
- Licensing Requirements for DHCP Snooping, page 9
- Prerequisites for DHCP Snooping, page 10
- Guidelines and Limitations for DHCP Snooping, page 10
- Default Settings for DHCP Settings, page 11
- Configuring DHCP Snooping, page 11
- Verifying the DHCP Snooping Configuration, page 23
- Monitoring DHCP Snooping , page 24
- Configuration Example for DHCP Snooping, page 24
- Configuration Example for Trust Configuration and DHCP Server Placement in the Network, page 26
- Standards, page 28
- Feature History for DHCP Snooping, page 28

Information About DHCP Snooping

DHCP snooping functions 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.

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.

DHCP Overview

The Dynamic Host Configuration Protocol (DHCP) provides the configuration parameters to Internet hosts. DHCP does the following:

- Delivers host-specific configuration parameters from a DHCP server to a host.
- Allocates network addresses to hosts.

DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

By default, DHCP supports the following mechanisms for IP address allocation:

- Automatic allocation—- DHCP assigns a permanent IP address to a client.
- Dynamic allocation—DHCP assigns an IP address to a client for a limited period of time (or until the client explicitly relinquishes the address).
- Manual allocation—The network administrator assigns an IP address to a client and DHCP is used to convey the assigned address to the client.

The format of DHCP messages is based on the format of Bootstrap Protocol (BOOTP) messages. This format supports BOOTP relay agent functionality and interoperability between BOOTP clients and DHCP servers. With BOOTP relay agents, you do not need to deploy a DHCP server on each physical network segment.

DHCP uses the two ports assigned by IANA for BOOTP. The destination UDP port 67 sends data to the server, and UDP port 68 sends data to the client.

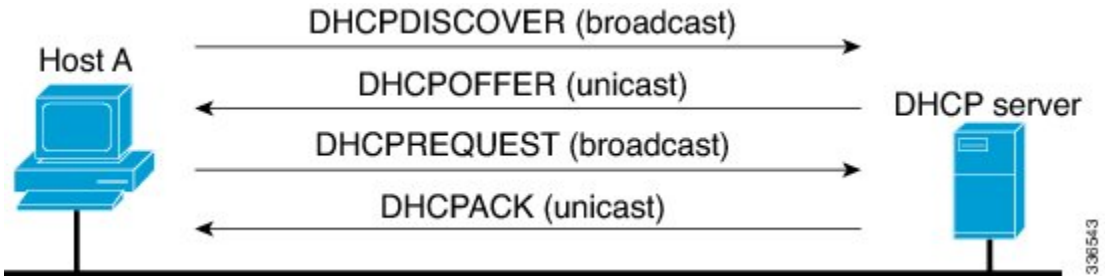
DHCP operations are categorized into four basic phases:

- IP Discovery
- IP Lease Offer
- IP Request
- IP Lease Acknowledgement

Note The DHCP operations phases are often abbreviated as DORA (Discovery, Offer, Request, and Acknowledgement).

The following figure shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server. The client, Host A, sends a DHCPDISCOVER broadcast message to locate a Cisco IOS DHCP server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message.

Figure 1: DHCP Request for an IP Address from a DHCP Server



The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message. The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

BOOTP Packet Format

BOOTP requests and replies are encapsulated in UDP datagrams as shown in the following figure and table.

Figure 2: BOOTP Packet Format

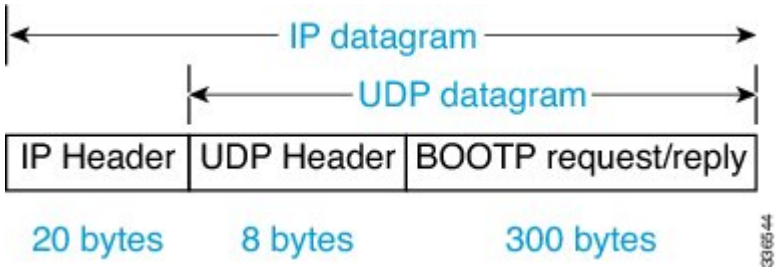


Figure 3: 300-Byte BOOTP Request and Reply Format

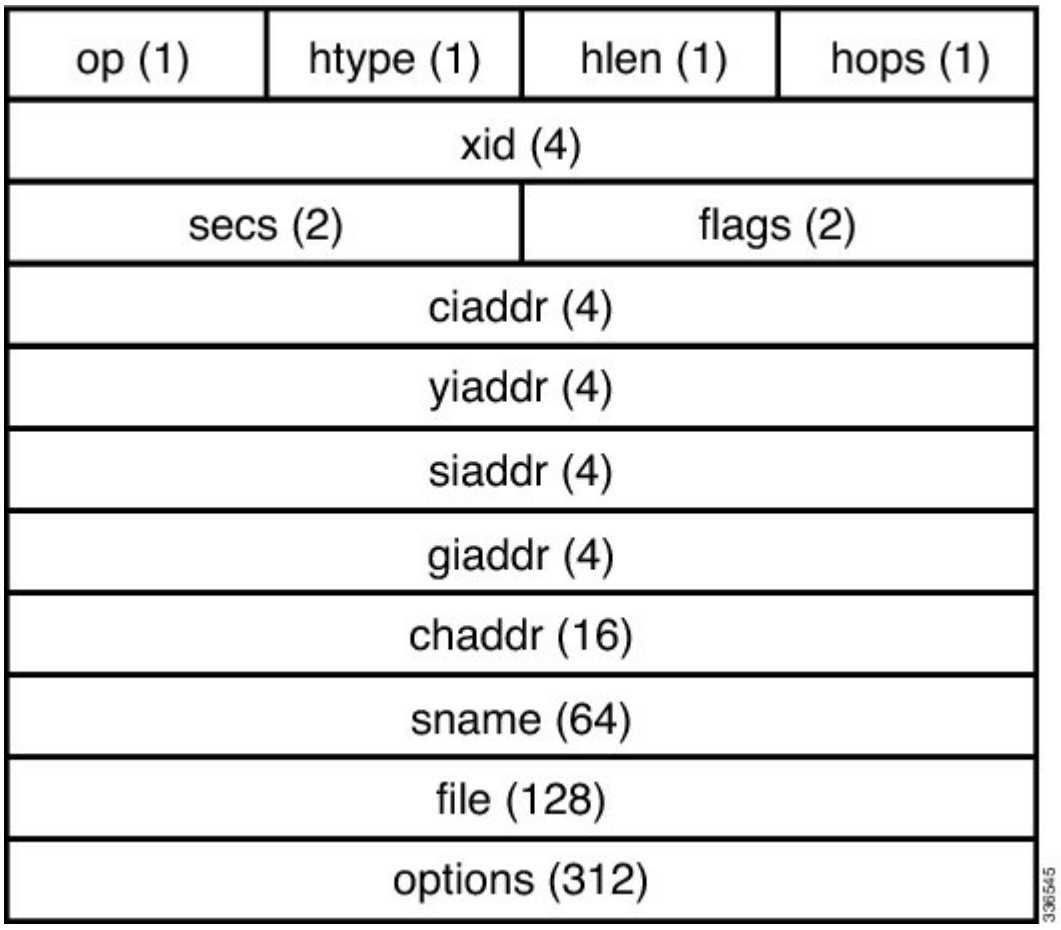


Table 1: BOOTP Request and Reply Format

Field	Bytes	Name	Description
op	1	OpCode	Identifies the packet as a request or reply. 1=BOOTREQUEST and 2=BOOTREPLY.
htype	1	Hardware Type	Specifies the network hardware type.
hlen	1	Hardware Length	Specifies the length hardware address length.
hops	1	Hops	The client sets the value to zero and the value increments if the request is forwarded across a router.
xid	4	Transaction ID	A random number that is chosen by the client. All DHCP messages exchanged for a given DHCP transaction use the ID (xid).
secs	2	Seconds	Specifies number of seconds since the DHCP process started.
flags	2	Flags	Indicates whether the message will be broadcast or unicast.
ciaddr	4	Client IP Address	Used when the client is aware of the IP address as in the case of the Bound, Renew, or Rebinding states.
yiaddr	4	Your IP Address	If the client IP address is 0.0.0.0, the DHCP server places the offered client IP address in this field.

Field	Bytes	Name	Description
siaddr	4	Server IP Address	If the client knows the IP address of the DHCP server, this field is populated with the DHCP server address. Otherwise, it is used in DHCPOFFER and DHCPACK from the DHCP server.
giaddr	4	Router IP Address	The gateway IP address, filled in by the DHCP/BootP Relay Agent.
chaddr	16	Client MAC Address	The DHCP client MAC address.
sname	64	Server Name	The optional server hostname.
File	128	Boot Filename	The boot filename.
Options	Variable	Option Parameters	The optional parameters that can be provided by the DHCP server. RFC 2132 lists all possible options.

Trusted and Untrusted Sources

DHCP snooping identifies ports as trusted or untrusted sources. When you enable DHCP snooping, by default, all vEthernet (vEth) ports are untrusted and all Ethernet ports (uplinks), port channels, special vEth ports (used by other features, such as the Virtual Service Domain (VSD) are trusted.

In an enterprise network, a trusted source is a device that is under your administrator's control. Any device beyond the firewall or outside the network is an untrusted source. Client ports are generally treated as untrusted sources.

In the Cisco Nexus 1000V switch, 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.

DHCP snooping does the following and acts like a firewall between untrusted clients and trusted DHCP servers:

- Only DHCP messages that come from a server that is connected to a trusted port are accepted. Any DHCP message on UDP port 68 that is data from the server to the client that is received on an untrusted port is dropped.
- Builds and maintains the DHCP snooping binding database, which contains information about clients with leased IP addresses.
- Uses the DHCP snooping binding database to validate subsequent requests from clients.

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

DHCP Snooping Binding Database

By using the information that is extracted from intercepted DHCP messages, DHCP snooping dynamically builds and maintains a database on each Virtual Ethernet Module (VEM). The database contains an entry for each untrusted client 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 that are 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, with DHCP snooping, you can add an entry to the database when the device receives a DHCPACK message from the server. DHCP snooping also allows you to remove an 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.

To remove dynamically added entries from the binding database, use the **clear ip dhcp snooping binding** command.

DHCP Snooping Option 82 Data Insertion

DHCP can centrally manage the IP address assignments for a large number of subscribers. When you enable option 82, the device identifies a subscriber device that connects to the network using the vEthernet number to which the client is connected and the Virtual Supervisor Module (VSM) to which the client belongs (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.

When you enable option 82 on the Cisco Nexus 1000V, the following sequence of events is displayed:

1. The host (DHCP client) generates a DHCP request and broadcasts it on the network.
2. When the Cisco Nexus 1000V Virtual Ethernet Module (VEM) receives the DHCP request, it adds the option 82 information in the packet. The option 82 information contains the device MAC address (the remote ID suboption), the port identifier, and the vEth number from which the packet is received (the circuit ID suboption).

3 The device forwards the DHCP request that includes the option 82 field to the DHCP server.

4 The DHCP server receives the packet. If the server is option 82 capable, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. The DHCP server echoes the option 82 field in the DHCP reply.

5 The DHCP server sends the reply to the Cisco Nexus 1000V. The Cisco Nexus 1000V verifies that it originally inserted the option 82 data by inspecting the remote ID and the circuit ID fields. The Cisco Nexus 1000V VEM removes the Option 82 field and forwards the packet to the interface that connects to the DHCP client that sent the DHCP request.

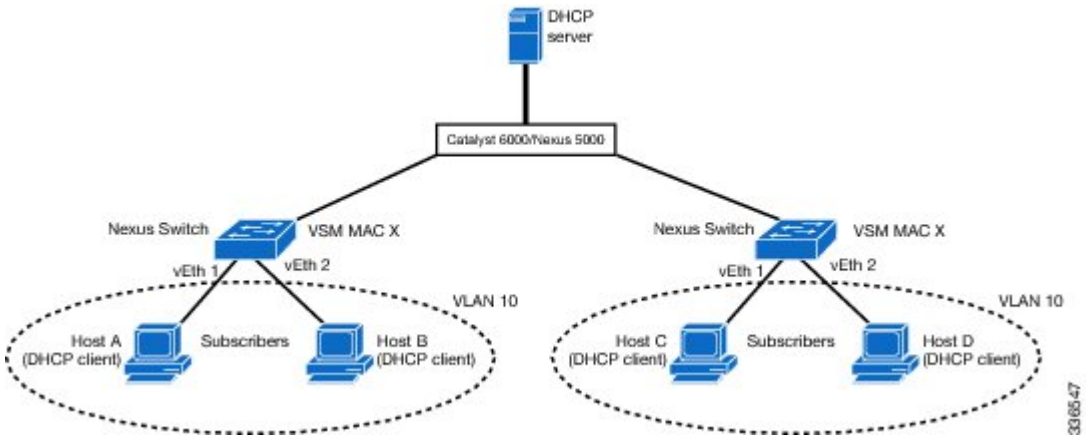
Option 82 Insertion

The following figure describes a typical use case of option 82 insertion. Host A and Host B are part of Cisco Nexus 1000V with the VSM MAC address on VLAN 10. Similarly, Host C and Host D are part of the Cisco Nexus 1000 V with the VSM MAC address also on VLAN 10. All the clients receive an IP address from the common DHCP server that is connected to the upstream switch.

Option 82 insertion enables you to assign specific IP addresses to Host C and Host A. These hosts are both part of VLAN 10 and have the same vEth numbers (vEthernet1). You can also assign IP addresses to Hosts D and Host B (vEthernet 2) by using the VSM MAC address in the DHCP packet.

DHCP packets from Hosts A and B on the first Cisco Nexus 1000V have the VSM MAC address in the Remote ID field. Requests from Hosts C and D have the VSM MAC address in the Remote ID field. Based on the remote IDs, you can configure the DHCP server with pools to assign separate set of IPs to clients on each Cisco Nexus 1000V even though the clients are part of the same VLAN (VLAN 10).

Figure 4: Option 82 Insertion Topology



Suboption Packet Formats

The following figure shows the packet formats for the remote ID suboption and the circuit ID suboption. The Cisco Nexus 1000V uses these packet formats when you globally enable DHCP snooping and when you enable option 82 data insertion and removal. For the circuit ID suboption, the circuit ID string is the name of

the vEth port to which the client is connected. For the Remote ID suboption, the MAC address is the Asynchronous Inter-process Communication (AIPC) interface on the Cisco Nexus 1000V.

Figure 5: Remote ID Suboption Frame Format

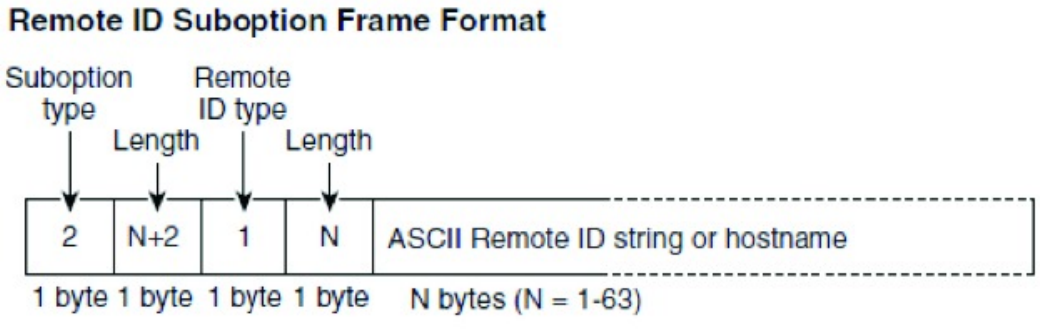
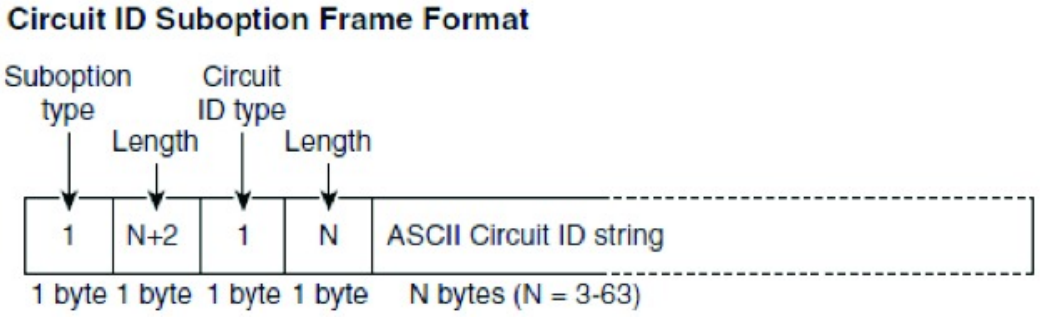


Figure 6: Circuit ID Suboption Frame Format



Licensing Requirements for DHCP Snooping

The following table shows the licensing requirements for this feature:

Feature	License Requirement
DHCP snooping	Starting with Release 4.2(1)SV2(1.1), a tier-based licensing approach is adopted for the Cisco Nexus 1000V. The Cisco Nexus 1000V is shipped in two editions: Essential and Advanced. When the switch edition is configured as the Advanced edition, DHCP snooping, Dynamic ARP Inspection (DAI), and IP Source Guard (IPSG) are available as advanced features that require licenses. **Note** Starting with Release 4.2(1)SV2(1.1), you can enable DHCP snooping on the Cisco Nexus 1000V by using the **feature dhcp** command. If the switch edition is Essential, the **feature** command fails. See the *Cisco Nexus 1000V License Configuration Guide* for more information about the licensing requirements for the Cisco Nexus 1000V.

Prerequisites for DHCP Snooping

- You must be familiar with DHCP to configure DHCP snooping.
- See the Licensing Requirements section for information about the licensing requirements of this feature.

Guidelines and Limitations for DHCP Snooping

- A DHCP snooping database is stored on each VEM and can contain up to 2048 bindings. The combined number of DHCP bindings entries from all VEMs is a maximum of 2048.
- 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 Asynchronous Inter-process Communication (AIPC), management, and inband ports on a particular VEM), you must configure these virtual Ethernet interfaces as trusted interfaces.
- You must configure connecting interfaces on a device upstream from the Cisco Nexus 1000V as trusted if DHCP snooping is enabled on the device.
- Enabling DHCP snooping on the primary VLAN enables snooping on all its corresponding secondary VLANs. Enabling DHCP snooping only on a secondary VLAN is not a valid configuration.
- If you are configuring more than 128 access control lists (ACL) (MAC and IP ACLs combined), make sure that the VSM RAM is set at 3 GB (3072 MB).

Default Settings for DHCP Settings

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.
DHCP snooping limit rate	None

Configuring DHCP Snooping

Process for DHCP Snooping Configuration

1. Enable the DHCP feature.
2. Enable DHCP snooping globally.
3. Enable DHCP snooping on at least one VLAN.

   By default, DHCP snooping is disabled on all VLANs.
4. Ensure that the DHCP server is connected to the device using a trusted interface.

Enabling or Disabling the DHCP Feature

By default, DHCP is disabled.

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature dhcp**	Enables DHCP snooping globally. The **no** option disables DHCP snooping but saves an existing DHCP snooping configuration. DHCP snooping is available as an advanced feature that requires a license. See the *Cisco Nexus 1000V License Configuration Guide* for more information about the licensing requirements for the Cisco Nexus 1000V.
Step 3	switch(config)# **show feature**	(Optional) Displays the state (enabled or disabled) of each available feature.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to enable DHCP:

```
switch# configure terminal
switch(config)# feature dhcp
switch(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
switch(config)# copy running-config startup-config
```

Enabling or Disabling DHCP Snooping Globally

Be sure you know the following information about DHCP snooping:

- 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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature dhcp**	Enables DHCP globally. DHCP snooping is available as an advanced feature that requires a license.
Step 3	switch(config)# [**no**] **ip dhcp snooping**	Enables IP DHCP snooping. The **no** option disables DHCP snooping but saves an existing DHCP snooping configuration.
Step 4	switch(config)# **show running-config dhcp**	(Optional) Displays the DHCP snooping running configuration.
Step 5	switch(config)# **show ip dhcp snooping**	(Optional) Displays the DHCP snooping IP configuration.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to enable or disable DHCP snooping globally:

```
switch# configure terminal
switch(config)# ip dhcp snooping
switch(config)# show running-config dhcp
feature dhcp ip dhcp snooping
switch (config)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:none
DHCP snooping is operational on the following VLANs:none
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted        Pkt Limit
------------          -------        ---------
Vethernet1            No              Unlimited
Vethernet2            No              Unlimited
Vethernet3            No              Unlimited
Vethernet4            No              Unlimited
Vethernet5            No              Unlimited

switch(config)# copy running-config startup-config
```

Enabling or Disabling DHCP Snooping on a VLAN

By default, DHCP snooping is disabled on all VLANs.

Note Enabling DHCP snooping on the primary VLAN enables snooping on all its corresponding secondary VLANs. Enabling DHCP snooping only on a secondary VLAN is not a valid configuration.

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature dhcp**	Enables DHCP globally. DHCP snooping is available as an advanced feature that requires a license.
Step 3	switch(config)# [**no**] **ip dhcp snooping vlan vlan-list**	Enables DHCP snooping on the VLANs specified by the VLAN-list. The **no** option disables DHCP snooping on the VLANs specified.
Step 4	switch(config)# **show running-config dhcp**	(Optional) Displays the DHCP snooping running configuration.
Step 5	switch(config)# **show ip dhcp snooping**	(Optional) Displays the DHCP snooping IP configuration.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to enable or disable DHCP snooping on a VLAN:

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)# show running-config dhcp
feature dhcp
ip dhcp snooping
ip dhcp snooping vlan 100,200,250-252
switch(config)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface            Trusted        Pkt Limit
------------         -------        ---------
Vethernet1           No              Unlimited
Vethernet2           No              Unlimited
Vethernet3           No              Unlimited
Vethernet4           No              Unlimited
Vethernet5           No              Unlimited


switch(config)# copy running-config startup-config
```

Enabling or Disabling DHCP Snooping for MAC Address Verification

You can enable or disable DHCP snooping for 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. MAC address verification is enabled by default.

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **ip dhcp snooping verify mac-address**	Enables the DHCP snooping for MAC address verification. The **no** option disables MAC address verification.
Step 3	switch(config)# **show running-config dhcp**	(Optional) Displays the DHCP snooping running configuration.
Step 4	switch(config)# **show ip dhcp snooping**	(Optional) Displays the DHCP snooping IP configuration.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to enable DHCP snooping for MAC address verification:

```
switch# configure terminal
switch(config)# ip dhcp snooping verify mac-address
switch(config)# show running-config dhcp
feature dhcp
ip dhcp snooping
ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is disabled
Verification of MAC address is disabled
DHCP snooping trust is configured on the following interfaces:
Interface            Trusted        Pkt Limit
------------         -------        ---------
Vethernet1           No              Unlimited
Vethernet2           No              Unlimited
Vethernet3           No              Unlimited
Vethernet4           No              Unlimited
Vethernet5           No              Unlimited
switch(config)# copy running-config startup-config
```

Configuring an Interface as Trusted or Untrusted

You can configure whether a virtual Ethernet (vEth) interface is a trusted or untrusted source of DHCP messages. You can configure DHCP trust using one of the following methods:

- Layer 2 vEthernet interfaces
- Port profiles for Layer 2 vEthernet interfaces

By default, vEth interfaces are untrusted. The only exception is the special vEth ports that are used by other features, such as Virtual Service Domain (VSD), are trusted

For seamless DHCP snooping, Dynamic ARP Inspection (DAI), IP Source Guard, VSD service VM ports are trusted ports by default. If you configure these ports as untrusted, this setting is ignored.

Before You Begin

- Log in to the CLI in EXEC mode.
- Know that the vEthernet interface is configured as a Layer 2 interface.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Places you in interface configuration mode for the specified vEthernet interface. Use this command to configure an interface as a trusted interface using an interface configuration.
Step 3	switch(config)# **port-profile** *profilename*	Places you in port profile configuration mode for the specified port profile. Configures an interface as a trusted interface using a port profile configuration.
Step 4	switch(config-if)# [**no**] **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 5	switch(config-if)# **show running-config dhcp**	(Optional) Displays the DHCP snooping running configuration.
Step 6	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure an interface as trusted or untrusted:

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip dhcp snooping trust
```

```
switch(config)# port-profile vm-data
switch(config-port-profile)#  ip dhcp snooping trust
switch(config-port-profile)#  show running-config dhcp
feature dhcp
interface Vethernet1
  ip dhcp snooping trust
interface Vethernet3
  ip dhcp snooping trust
interface Vethernet10
  ip dhcp snooping trust
interface Vethernet11
  ip dhcp snooping trust
interface Vethernet12
  ip dhcp snooping trust
interface Vethernet13
  ip dhcp snooping trust
ip dhcp snooping
no ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config-port-profile)#  copy running-config startup-config
```

Configuring the Rate Limit for DHCP Packets

You can configure a limit for the rate of DHCP packets per second received on each port.

Before You Begin

Log in to the CLI in EXEC mode.

You should know the following information:

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vethernet** *interface-number*	Places you in interface configuration mode for the specified vEthernet interface.
Step 3	switch(config)# **port-profile** *profilename*	Places you in port profile configuration mode for the specified port profile.
Step 4	switch(config-if)# [**no**] **ip dhcp snooping limit rate** *rate*	Configures the limit for the rate of DHCP packets per second (1 to 2048). The **no** option removes the rate limit.
Step 5	switch(config-if)# **show running-config dhcp**	(Optional) Displays the DHCP snooping running configuration.

	Command or Action	Purpose
Step 6	switch(config-if)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a rate limit for DHCP packets:

```
switch# configure terminal
switch(config)# interface vethernet 3
switch(config-if)# ip dhcp snooping limit rate 15
switch(config-if)# show running-config dhcp
switch(config-if)# copy running-config startup-config

switch(config)# port-profile vm-data
switch(config-port-profile)#  ip dhcp snooping limit rate 15
switch(config-port-profile)#  show running-config dhcp
feature dhcp
interface Vethernet3
  ip dhcp snooping trust
  ip dhcp snooping limit rate 15
ip dhcp snooping
no ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config-port-profile)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted        Pkt Limit
------------          -------        ---------
Vethernet1            No              Unlimited
Vethernet2            No              Unlimited
Vethernet3            Yes              15
Vethernet4            No              Unlimited
Vethernet5            No              Unlimited
switch(config-port-profile)#  copy running-config startup-config
```

Detecting Disabled Ports for DHCP Rate Limit Violations

You can globally detect the disabled ports that exceed the DHCP rate limit.

To recover an interface manually from the error-disabled state, you must enter the **shutdown** command and then the **no shutdown** command.

Note A failure to conform to the set rate causes the port to be put into an errdisable state.

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **feature dhcp**	Enables DHCP globally. DHCP snooping is available as an advanced feature that requires a license.
Step 3	switch(config)# [**no**] **errdisable detect cause dhcp-rate-limit**	Enables DHCP error-disabled detection. The **no** option disables DHCP error-disabled detection.
Step 4	switch(config)# **show running-config dhcp**	(Optional) Displays the DHCP snooping running configuration.
Step 5	switch(config)# **show errdisable detect**	(Optional) Displays the reasons for the port to be in the error-disabled state.
Step 6	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to detect disabled ports for DHCP rate limit violation:

```
switch# configure terminal
switch(config)# errdisable recovery cause dhcp-rate-limit
switch(config)# show running-config dhcp
switch(config)# show errdisable detect
ErrDisable Reason            Timer Status
-----------------            ------------
link-flap                    enabled
dhcp-rate-limit              enabled
arp-inspection               enabled
ip-addr-conflict             enabled
switch(config)# copy running-config startup-config
```

Recovering Disabled Ports for DHCP Rate Limit Violations

You can globally configure the automatic recovery of disabled ports for violating the DHCP rate limit.

To recover an interface manually from the error-disabled state, you must enter the **shutdown** command and then the **no shutdown** command.

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **errdisable recovery cause dhcp-rate-limit**	Enables DHCP error-disabled detection. The **no** option disables DHCP error-disabled detection.
Step 3	switch(config)# **errdisable recovery interval** *time interval*	Sets the DHCP error-disabled recovery interval, where *time interval* is the number of seconds from 30 to 65535.
Step 4	switch(config)# **show errdisable recovery**	(Optional) Displays the recovery interval for the vEth to recover from the error-disabled state.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to recover disabled ports for DHCP rate limit violations:

```
switch# configure terminal
switch(config)# errdisable detect cause dhcp-rate-limit
switch(config)# errdisable recovery interval 30
switch(config)# show running-config dhcp
switch(config)# show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            ------------
link-flap                    disabled
dhcp-rate-limit              enabled
arp-inspection               disabled
security-violation           disabled
psecure-violation            disabled
failed-port-state            enabled
ip-addr-conflict             disabled

        Timer interval: 30
switch(config)# copy running-config startup-config
```

Clearing the DHCP Snooping Binding Database

You can clear the DHCP snooping binding database.

Clearing All Binding Entries

Before You Begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **clear ip dhcp snooping binding**	Clears dynamically added entries from the DHCP snooping binding database.
Step 2	switch# **show ip dhcp snooping binding**	(Optional) Displays the DHCP snooping binding database.

This example shows how to clear all binding entries:

```
switch# clear ip dhcp snooping binding
switch# show ip dhcp snooping binding
```

Clearing Binding Entries for an Interface

Before You Begin

- Log in to the CLI in EXEC mode
- Collect the following information for the interface:
  - VLAN ID
  - IP address
  - MAC address

Procedure

	Command or Action	Purpose
Step 1	switch# **clear ip dhcp snooping binding** [{**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*} | **vlan** *vlan-id1* | **interface** *interface-id1*]	Clears dynamically added entries for an interface from the DHCP snooping binding database.
Step 2	switch# **show ip dhcp snooping binding**	Displays the DHCP snooping binding database.

This example shows how to clear binding entries for an interface:

```
switch# clear ip dhcp snooping binding vlan 10 mac EEEE.EEEE.EEEE ip 10.10.10.1 interface
vethernet 1
switch# show ip dhcp snooping binding
```

Relaying Switch and Circuit Information in DHCP

You can globally relay the VSM MAC address and vEthernet port information in DHCP packets.

Before You Begin

Log in to the CLI in EXEC mode.

Note In a HA pair setup, the MAC address inserted in the option 82 field of the DHCP packet is the AIPC interface of the current active VSM. The match criteria on the DHCP server must match the AIPC MAC address of both primary and secondary VSMs.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **ip dhcp snooping information option**	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	switch(config)# **show running-config dhcp**	(Optional) Displays the DHCP snooping running configuration.
Step 4	switch(config)# **show ip dhcp snooping**	(Optional) Displays the DHCP snooping IP configuration.
Step 5	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to relay switch and circuit information in DHCP:

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)# show running-config dhcp
feature dhcp
interface Vethernet3
  ip dhcp snooping trust
  ip dhcp snooping limit rate 15
ip dhcp snooping
ip dhcp snooping information option
no ip dhcp snooping verify mac-address
ip dhcp snooping vlan 100,200,250-252
switch(config)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100,200,250-252
DHCP snooping is operational on the following VLANs:
100,200,250-252
Insertion of Option 82 is enabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface            Trusted        Pkt Limit
------------         -------        ---------
Vethernet1           No              Unlimited
Vethernet2           No              Unlimited
Vethernet3           Yes              15
```

```
Vethernet4            No              Unlimited
Vethernet5            No              Unlimited
switch(config)# copy running-config startup-config
```

Adding or Removing a Static IP Entry

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# [**no**] **ip source binding** *ip address MAC address* **vlan** *vlanid* **interface vethernet** *interface-number*	Creates a static IP source entry for the current interface. Use the **no** option to remove the static IP source entry.
Step 3	switch(config)# **show ip dhcp snooping binding interface vethernet** *interface number*	(Optional) Displays IP-MAC address bindings for the interface specified, including static IP source entries. Static entries appear with the term static in the Type column.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

This example shows how to add or remove a static IP entry:

```
switch# configure terminal
switch(config)#  ip source binding 10.5.22.178 001f.28bd.0014 vlan 100 interface vethernet
 3
switch(config)# show ip dhcp snooping binding interface vethernet 3
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  --------------
00:1f:28:bd:00:14  10.5.22.178      infinite   static       100   Vethernet3
switch(config)# copy running-config startup-config
```

Verifying the DHCP Snooping Configuration

Use the following commands to verify the configuration:

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	Displays the contents of the DHCP snooping binding table.

Command	Purpose
show feature	Displays the features available, such as DHCP, and whether they are enabled.

Monitoring DHCP Snooping

Use the **show ip dhcp snooping statistics** command to monitor DHCP snooping statistics.

```
switch(config)# show ip dhcp snooping statistics

Packets processed 0
Packets forwarded 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to service dhcp not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 0
Packets dropped due to max hops exceeded 0
```

Configuration Example for DHCP Snooping

This example shows how to enable DHCP snooping on VLAN 100, with vEthernet interface 5 trusted because the DHCP server is connected to that interface. This example shows how to configure a rate limit of 15 pps on the interface where the client is connected. The clients are using port-profile client-pp. When the rate limit is violated, the client port is put in the error-disabled state for 60 seconds before it is recovered. One of the clients has static DHCP IP assigned and one IP address has an infinite lease time assigned by the DHCP server:

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 100
switch(config)# interface veth 5
switch(config-if)# ip dhcp snooping trust
switch(config)# port-profile type vethernet client-pp
switch(config-port-prof)# ip dhcp snooping limit rate 15
switch(config)# errdisable detect cause dhcp-rate-limit
switch(config)# errdisable recovery interval 60
switch(config)# ip source binding 192.168.0.55  00:50:56:81:42:74 vlan 100 interface vethernet
 12

switch (config-if)# show feature
Feature Name          Instance      State
--------------------        -------       --------
cts                          1          disabled
dhcp-snooping                1          enabled
http-server                  1          enabled
lacp                         1          enabled
netflow                      1          enabled
network-segmentation         1          enabled
port-profile-roles           1          disabled
private-vlan                 1          enabled
segmentation                 1          enabled
sshServer                    1          enabled
tacacs                       1          disabled
telnetServer                 1          disabled
```

```
vtracker                    1         disabled

switch(config-if)# show run dhcp

feature dhcp

interface Vethernet1
  ip dhcp snooping limit rate 15

interface Vethernet5
  ip dhcp snooping trust

interface Vethernet10
  ip dhcp snooping limit rate 15

interface Vethernet11
  ip dhcp snooping limit rate 15

interface Vethernet12
  ip dhcp snooping limit rate 15

interface Vethernet13
  ip dhcp snooping limit rate 15
ip dhcp snooping
ip dhcp snooping vlan 100
ip source binding 192.168.0.55  00:50:56:81:42:74 vlan 100 interface vethernet 12

Note: Client interfaces Vethernet 1,10-13 are part of port-profile “client-pp”

swtich (config-if)# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
100
DHCP snooping is operational on the following VLANs:
100
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted              Pkt Limit
------------          -------        --------
Vethernet1            No                    15
Vethernet2            No                    Unlimited
Vethernet3            No                    Unlimited
Vethernet4            No                    Unlimited
Vethernet5            Yes                   Unlimited
Vethernet7            No                    Unlimited
Vethernet8            No                    Unlimited
Vethernet9            No                    Unlimited
Vethernet10           No                   15
Vethernet11           No                   15
Vethernet12           No                   15
Vethernet13           No                   15


switch# show ip dhcp snooping binding
MacAddress             IpAddress        LeaseSec  Type         VLAN  Interface
------------------     ---------------  ---------- ----------- ----- -------------
00:50:56:81:42:46      192.168.0.9      28570     dhcp-snoop  100    Vethernet1
00:50:56:81:42:59      192.168.0.69     28591     dhcp-snoop  100    Vethernet10
00:50:56:81:42:6d      192.168.0.251    28559     dhcp-snoop  100    Vethernet11
00:50:56:81:42:72      192.168.0.48     infinite  static      100    Vethernet12
00:50:56:81:42:74      192.168.0.55     infinite  dhcp-snoop  100    Vethernet13
```

Note An entry with an infinite lease time issued by the DHCP server has infinite in the Lease Sec column and will be of Type dhcp-snoop.

When client interfaces are part of a secondary VLAN, the DHCP binding table displays the entries on its corresponding primary VLAN.

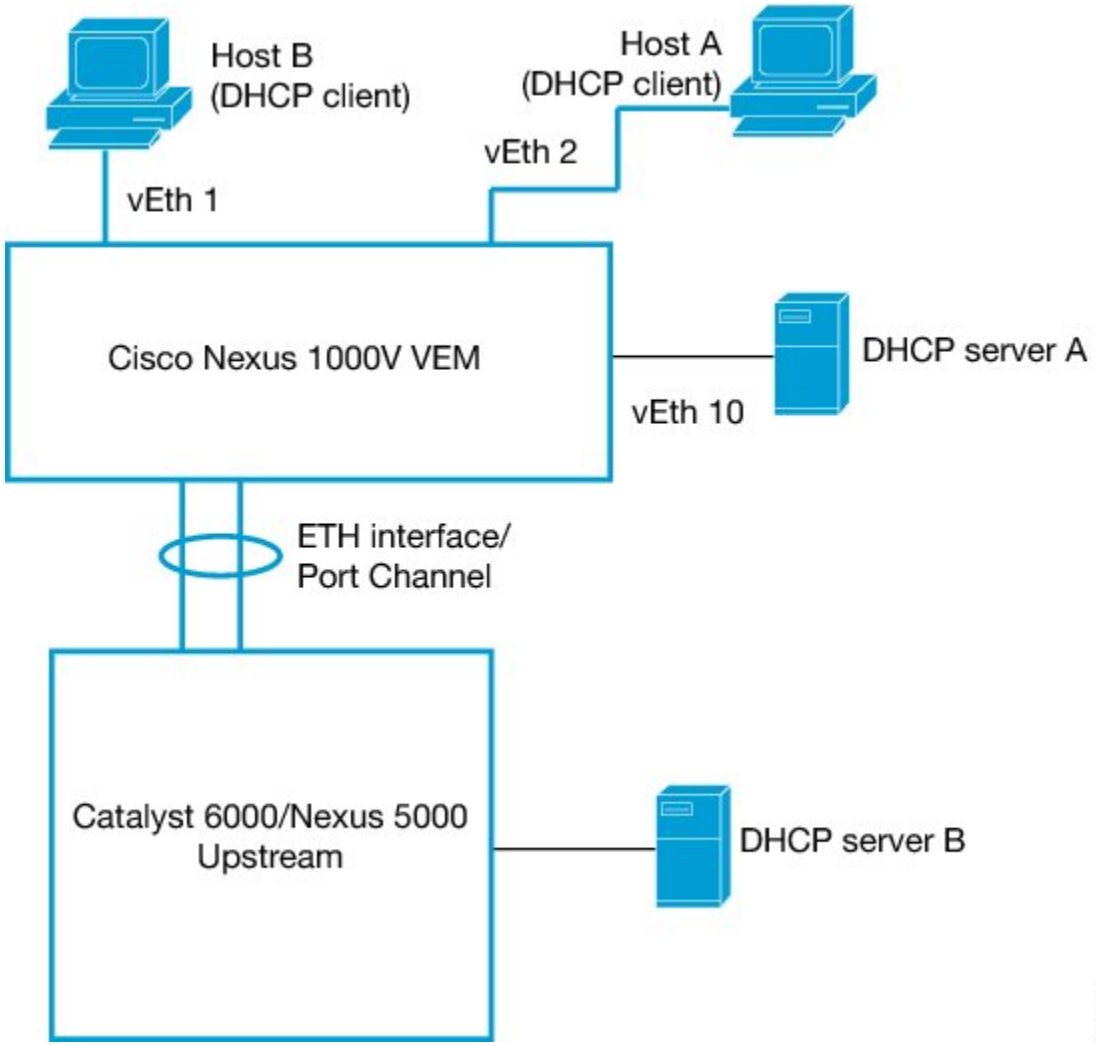
Configuration Example for Trust Configuration and DHCP Server Placement in the Network

DHCP Server Inside and Outside the Cisco Nexus 1000V Network and Clients on the Cisco Nexus 1000V

This example shows that there are two DHCP servers: server A on the Nexus 1000V and Server B on the upstream switch. Clients A and B can get the IP address from DHCP server B without any additional trust configuration because the Ethernet ports/port-channel interface on the Cisco Nexus 1000V are trusted by default.

The following figure shows that to use DHCP server A, you must configure trust on vEthernet 10 to which the server is connected.

Figure 7: DHCP Server Inside and Outside the Cisco Nexus 1000V Network and Clients on the Cisco Nexus 1000V

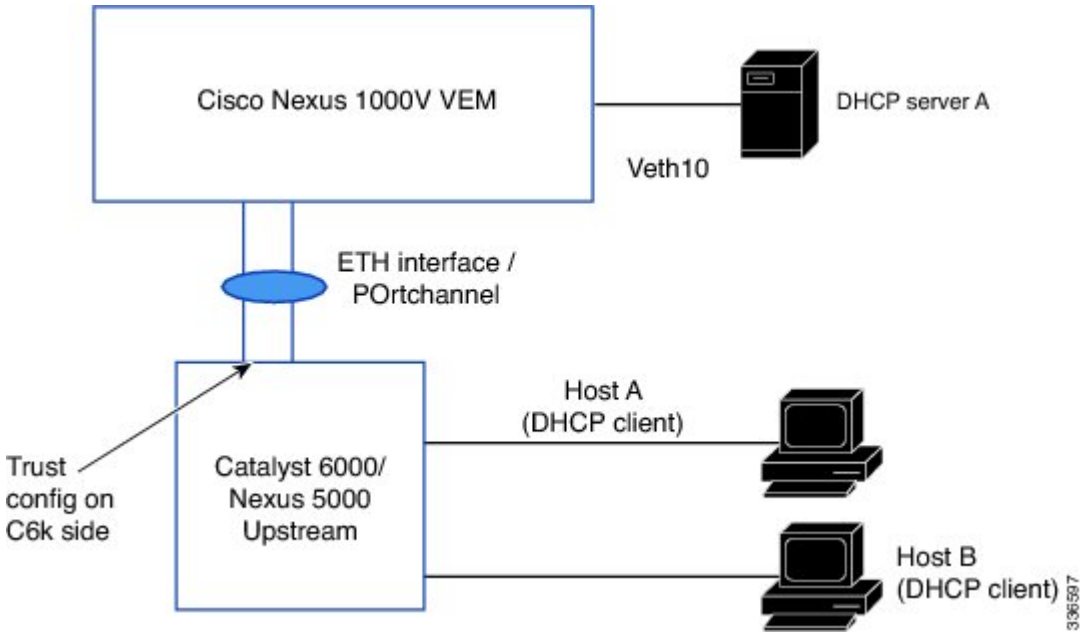


DHCP Server Inside the Cisco Nexus 1000V Network and Clients Outside the Cisco Nexus 1000V

You can configure interfaces on the upstream switch as trusted if the administrator is running the DHCP server on a Virtual Machine (VM) on the Cisco Nexus 1000V and clients are outside the Cisco Nexus 1000V.

In the following figure, server A is on the Cisco Nexus 1000V and clients A and B can get the IP address from server A only when trust is enabled on the ports on the upstream side.

Figure 8: DHCP Server Inside the Cisco Nexus 1000V Network and Clients Outside the Cisco Nexus 1000V



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

This table only includes updates for those releases that have resulted in additions to the feature.

Feature Name	Releases	Feature Information
Licensing changes	4.2(1)SV2(1.1)	DHCP snooping is available as an advanced feature. Use the **feature dhcp** command to enable the feature.

Feature Name	Releases	Feature Information
Enabling Source IP Based Filtering	4.2(1)SV2(1.1)	You can enable source IP-based filtering on the Cisco Nexus 1000V switch.
Relay Agent (option 82)	4.2(1)SV1(4)	You can configure relaying of the VSM MAC address and port information in DHCP packets.
feature dhcp command	4.2(1)SV1(4)	Command added for enabling the DHCP feature globally.
DHCP snooping	4.0(4)SV1(2)	This feature was introduced.