

Configuring DHCP Snooping

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on Catalyst 4500 series switches. It provides guidelines, procedures, and configuration examples.

This chapter consists of the following major sections:

- [Overview of DHCP Snooping, page 19-1](#)
- [Configuring DHCP Snooping on the Switch, page 19-2](#)
- [Displaying DHCP Snooping Information, page 19-4](#)

**Note**

For complete syntax and usage information for the switch commands used in this chapter, refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_12/index.htm

Overview of DHCP Snooping

DHCP snooping is a DHCP security feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An untrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

**Note**

In order to enable DHCP snooping on a VLAN, you must enable DHCP snooping on the switch.

You can configure DHCP snooping for switches and VLANs. When you enable DHCP snooping on a switch, the interface acts as a Layer 2 bridge, intercepting and safeguarding DHCP messages going to a Layer 2 VLAN. When you enable DHCP snooping on a VLAN, the switch acts as a Layer 2 bridge within a VLAN domain.

**Note**

For DHCP server configuration information, refer to “Configuring DHCP” in the *Cisco IOS IP and IP Routing Configuration Guide* at the following URL: 05 Aug 2007 - www.cisco.com/en/US/docs/ios/12_1/iproute/configuration/guide/1cdindx.html

Configuring DHCP Snooping on the Switch

When you configure DHCP snooping on your switch, you are enabling the switch to differentiate untrusted interfaces from trusted interfaces. You must enable DHCP snooping globally before you can use DHCP snooping on a VLAN. You can enable DHCP snooping independently from other DHCP features.

Once you have enabled DHCP snooping, all the DHCP relay information option configuration commands are disabled; this includes the following commands:

- **ip dhcp relay information check**
- **ip dhcp relay information policy**
- **ip dhcp relay information option**
- **ip dhcp relay information trusted**
- **ip dhcp relay information trust-all**

These sections describe how to configure DHCP snooping:

- [Default Configuration for DHCP Snooping](#)
- [Enabling DHCP Snooping](#)
- [Enabling DHCP Snooping on Private VLAN, page 19-4](#)
- [Configuring DHCP Snooping on Private VLAN, page 19-4](#)

Default Configuration for DHCP Snooping

DHCP snooping is disabled by default. [Table 19-1](#) shows all the default configuration values for each DHCP snooping option.

Table 19-1 Default Configuration Values for DHCP Snooping

Option	Default Value/State
DHCP snooping	Disabled
DHCP snooping information option	Enabled
DHCP snooping limit rate	Infinite (functions as if rate limiting were disabled)
DHCP snooping trust	Untrusted
DHCP snooping vlan	Disabled

If you want to change the default configuration values, see the “[Enabling DHCP Snooping](#)” section.

Enabling DHCP Snooping

To enable DHCP snooping, perform this task:

	Command	Purpose
Step 1	Switch(config)# ip dhcp snooping	Enables DHCP snooping globally. You can use the no keyword to disable DHCP snooping.
Step 2	Switch(config)# ip dhcp snooping vlan <i>number</i> <i>[number]</i>	Enables DHCP snooping on your VLANs.
Step 3	Switch(config)# ip dhcp snooping information option	Enables DHCP Option 82 data insertion.
Step 4	Switch(config-if)# ip dhcp snooping trust	Configures the interface as trusted or untrusted. You can use the no keyword of to configure an interface to receive only messages from within the network.
Step 5	Switch(config-if)# ip dhcp snooping limit rate <i>rate</i>	Configures the number of DHCP packets per second (pps) that an interface can receive. Note You may not want to configure untrusted rate limiting to more than 100 pps. Normally, the rate limit applies to untrusted interfaces. If you want to set up rate limiting for trusted interfaces, keep in mind that trusted interfaces aggregate all DHCP traffic in the switch, and you will need to adjust the rate limit to a higher value.
Step 6	Switch(config)# end	Exits configuration mode.
Step 7	Switch# show ip dhcp snooping	Verifies the configuration.

You can configure DHCP snooping for a single VLAN or a range of VLANs. To configure a single VLAN, enter a single VLAN number. To configure a range of VLANs, enter a beginning and an ending VLAN number.

This example shows how to enable DHCP snooping on VLANs 10 through 100:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 100
Switch(config)# ip dhcp snooping information option
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config)# end
Switch# show ip dhcp snooping
DHCP Snooping is configured on the following VLANs:
 10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted           Rate limit (pps)
-----
FastEthernet2/1     yes              10
FastEthernet2/2     yes              none
FastEthernet3/1     no               20
Switch#
```

Enabling DHCP Snooping on Private VLAN

DHCP snooping can be enabled on private VLANs, which provide isolation between Layer 2 ports within the same VLAN. If DHCP snooping is enabled (or disabled), the configuration is propagated to both the primary VLAN and its associated secondary VLANs; you cannot enable (or disable) DHCP snooping on a primary VLAN without reflecting this configuration change on the secondary VLANs.

Configuring DHCP snooping on a secondary VLAN is still allowed, but it will not take effect if the associated primary VLAN is already configured. If this is the case, the effective DHCP snooping mode on the secondary VLAN is derived from the corresponding primary VLAN. Manually configuring DHCP snooping on a secondary VLAN will cause the switch to issue the error message:

```
DHCP Snooping configuration may not take effect on secondary vlan XXX
```

The command **show ip dhcp snooping** will display all VLANs with DHCP snooping enabled, including both primary VLANs and their corresponding secondary VLANs.

Configuring DHCP Snooping on Private VLAN

DHCP snooping, IPSG, and DAI are Layer 2 based security features that can be enabled and disabled on an individual VLAN, including auxiliary/voice VLAN. This means that you need to enable DHCP snooping on a voice VLAN for a Cisco IP phone to function properly.

Displaying DHCP Snooping Information

You can display a DHCP snooping binding table and configuration information for all interfaces on a switch.

Displaying a Binding Table

The DHCP snooping binding table for each switch contains binding entries that correspond to untrusted ports. It does not contain information about hosts interconnected with a trusted port, because each interconnected switch will have its own DHCP snooping binding table.

This example shows how to display the DHCP snooping binding information for a switch.

```
Switch# show ip dhcp snooping binding
MacAddress      IP Address      Lease (seconds)  Type      VLAN      Interface
-----
0000.0100.0201  10.0.0.1        1600             dynamic   100       FastEthernet2/1
Switch#
```

Table 19-2 describes the fields in the **show ip dhcp snooping binding** command output.

Table 19-2 show ip dhcp snooping binding Command Output

Field	Description
Mac Address	Client hardware MAC address
IP Address	Client IP address assigned from the DHCP server
Lease (seconds)	IP address lease time

Table 19-2 *show ip dhcp snooping binding Command Output*

Field	Description
Type	Binding type; statically configured from CLI or dynamically learned
VLAN	VLAN number of the client interface
Interface	Interface that connects to the DHCP client host

Displaying the DHCP Snooping Configuration

This example shows how to display the DHCP snooping configuration for a switch.

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
  10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted           Rate limit (pps)
-----
FastEthernet2/1     yes              10
FastEthernet3/1     yes              none
GigabitEthernet1/1 no                20
Switch#
```

