



CHAPTER 33

Configuring DHCP Snooping and IP Source Guard

This chapter describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping and IP source guard on the Catalyst 6500 series switches.

This chapter consists of these sections:

- [Understanding How DHCP Snooping Works, page 33-1](#)
- [Configuring DHCP Snooping on a VLAN, page 33-2](#)
- [Specifying the DHCP-Snooping Binding Limit on a Per-Port Basis, page 33-11](#)
- [Specifying the DHCP-Snooping IP Address-to-MAC Address Binding on a Per-Port Basis, page 33-12](#)
- [Displaying DHCP-Snooping Information, page 33-12](#)
- [Storing DHCP-Snooping Binding Entries to a Flash Device, page 33-15](#)
- [Understanding How IP Source Guard Works, page 33-16](#)
- [Enabling IP Source Guard on a Port, page 33-17](#)
- [Displaying the IP Source Guard Information, page 33-18](#)



Note

For complete syntax and usage information for the switch commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* and related publications at http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/command/reference/cmd_ref.html

Understanding How DHCP Snooping Works

DHCP snooping provides the security against the Denial-Of-Service (DoS) attacks that are launched using the DHCP messages by filtering the DHCP packets and building and maintaining a DHCP-snooping binding table. DHCP snooping uses both trusted and untrusted ports.

The DHCP packets that are received from a trusted port are forwarded without validation. Typically, the trusted ports are used to reach a DHCP server or relay agent. When the switch receives the DHCP packets from an untrusted port, DHCP snooping validates that only the DHCP packets from the clients are allowed and verifies that no spoofing of information is occurring.

The DHCP-snooping binding table contains the MAC address, IP address, lease time in seconds, and VLAN port information for the DHCP clients on the untrusted ports of a switch. The information that is contained in a DHCP-snooping binding table is removed from the binding table once its lease expires or DHCP snooping is disabled in the VLAN.

**Note**

In software release 8.6(1) and later releases, you can enable DHCP snooping on a per-port basis.

These DHCP messages are used to build the DHCP binding table:

- DHCPACK—Adds a new dynamic DHCP binding entry if the binding entry does not already exist.
- DHCPNAK—Deletes an existing DHCP binding entry.
- DHCPRELEASE—Deletes a dynamic DHCP binding entry if the binding entry exists.
- DHCPDECLINE—Deletes a dynamic DHCP binding entry if the binding entry exists.

Each switch maintains a DHCP-snooping binding table for only the local untrusted ports. The table does not store information about the DHCP-snooping binding table for the hosts that are directly connected to other switches, and it does not contain information about the hosts that are connected through a trusted port. A trusted port has an entity, such as a relay agent or DHCP server, that is directly connected or is the forwarding path to such an entity. Any path to a relay agent or DHCP server should be trusted.

DHCP Snooping Configuration Guidelines

This section describes the guidelines for configuring DHCP snooping in your network:

- In software release 8.6(1) and later releases, you can enable DHCP snooping on a per-port basis.
- If you do a non-high availability switchover with DHCP snooping enabled, you will lose the contents of the DHCP-snooping binding table. We do not recommend using this configuration.
- DHCP snooping is supported on the Policy Feature Card (PFC) and later versions.
- The DHCP-snooping binding table is limited to 16,384 entries. Once the limit is reached, no new entries can be added until the lease time is reached on the older entries.
- 802.1X-DHCP and DHCP snooping are mutually exclusive. You should not configure a VLAN for both 802.1X-DHCP and DHCP snooping. If you configure both 802.1X and DHCP snooping in your ACL, the feature that is positioned higher up in the ACL overrides the other feature.
- We recommend that you enable high availability when using dynamic ARP inspection (DAI), DHCP snooping, and IP source guard. If high availability is not enabled, the clients have to renew their IP addresses for these features to work after a switchover. For configuration details on DAI, see the [“Dynamic ARP Inspection” section on page 15-39](#).

Configuring DHCP Snooping on a VLAN

Typically, DHCP snooping is used at the access-level network, such as a wiring closet. When you enable DHCP snooping on a VLAN, it builds a table of IP addresses to MAC-address bindings for the DHCP clients on that VLAN.

**Note**

In software release 8.6(1) and later releases, you can enable DHCP snooping on a per-port basis.

**Note**

In software release 8.5(1) and later releases, you can enable DHCP snooping on the management VLANs sc0 and sc1.

These sections describe how to configure DHCP snooping:

- [Default Configuration for DHCP Snooping, page 33-4](#)
- [Enabling DHCP Snooping, page 33-4](#)
- [Enabling DHCP Snooping on a Private VLAN, page 33-5](#)
- [Enabling the DHCP-Snooping Host-Tracking Information Option, page 33-5](#)
- [Enabling the DHCP Snooping MAC-Address Matching Option, page 33-6](#)
- [Configuration Examples for DHCP Snooping, page 33-7](#)

Default Configuration for DHCP Snooping

DHCP snooping is disabled by default. [Table 33-1](#) shows the default configuration values for each DHCP-snooping option. If you want to change the default configuration values, see the “[Enabling DHCP Snooping](#)” section on page 33-4.

Table 33-1 Default Configuration Values for DHCP Snooping

Option	Default Value/State
DHCP-snooping host tracking information option	Disabled.
DHCP-snooping limit rate	1000 pps shared with ARP inspection and 802.1X-DHCP. Rate limiting is supported on PFC2 and later versions.
DHCP-snooping trust on a port	Untrusted.
DHCP snooping on a VLAN	Disabled.
DHCP-snooping bindings-database auto-save option	Disabled.
DHCP-snooping bindings-database storage device and filename	bootflash:dhcp-snooping-bindings-database

Enabling DHCP Snooping

DHCP snooping is enabled on the VLANs through the security VLAN access control lists (VACLs). DHCP snooping is enabled on a VLAN by adding a DHCP-snooping access control entry (ACE) to a new or existing security ACL. You must determine where to position DHCP snooping in the ACL depending on your policy for the DHCP packets. For example, if you want to deny the DHCP packets that come from a certain host and perform DHCP snooping for the other DHCP packets, then you must place a deny ACE before the DHCP-snooping ACE.

To enable DHCP snooping on a VLAN, perform this task in privileged mode:

	Task	Command
Step 1	Add DHCP snooping to the VACL.	set security acl ip <i>acl_name</i> permit dhcp-snooping
Step 2	Configure the VACL to allow DHCP snooping from all hosts.	set security acl ip <i>acl_name</i> permit ip any any

	Task	Command
Step 3	Save the VACL.	<code>commit security acl <i>acl_name</i></code>
Step 4	Add an ACL to a VLAN.	<code>set security acl map <i>acl_name</i> 10</code>

This example shows how to configure DHCP snooping on a VLAN:

```

Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to save
changes.
Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

ACL dhcpsnoop successfully mapped to VLAN 10.
Console> (enable)

```



Note

If you create a VACL just for enabling DHCP snooping, the VACL has an implicit deny at the end and no other packets are allowed unless there is an explicit permit for those packets.



Note

802.1X-DHCP and DHCP snooping are mutually exclusive. Do not configure a VLAN with both features.

Enabling DHCP Snooping on a Private VLAN

You must enable DHCP snooping separately on the primary and secondary (isolated or community) private VLANs (PVLANS). The DHCP-snooping binding table contains binding information about the primary VLAN only and not the secondary VLANs. If you enable DHCP snooping on a PVLAN and not on the secondary VLAN, the DHCP-snooping binding table entries are not added, even though the packet is seen on the PVLAN.

Enabling the DHCP-Snooping Host-Tracking Information Option

If you enable the host-tracking information option, the DHCP relay agent information option (option 82) is added to the client packets that are being forwarded. The relay agent option contains the agent circuit ID and the agent remote ID information. The circuit ID suboption contains the port and the VLAN number of the client. The remote ID suboption contains the MAC address of the switch. Before inserting the host-tracking information, the switch verifies that the DHCP messages do not have an existing relay information option or a nonzero giaddr field. Before removing the host-tracking information, the switch verifies that the DHCP reply messages are from a trusted port and that the MAC address of the remote ID and the local switch match. If the packet comes from a trusted port and the addresses do not match, the packet is forwarded.

To configure the host-tracking information option for DHCP snooping, perform this task in privileged mode:

	Task	Command
Step 1	Enable the DHCP-snooping host-tracking information option.	set dhcp-snooping information host-tracking enable
Step 2	Display the MAC address for the host-tracking information option.	show dhcp-snooping config

This example shows how to configure the DHCP-snooping host-tracking information option:

```

Console> (enable) set dhcp-snooping information host-tracking enable
DHCP Snooping Information Option Enabled.
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is enabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> (enable)

```

Enabling the DHCP Snooping MAC-Address Matching Option

If you enable the MAC-address matching option, the source MAC address in the Ethernet header is matched with the chaddr field in the DHCP payload for the DHCP packets that are coming from the untrusted ports. If the match fails, the packets are dropped and the counter for the packets that are dropped on the untrusted ports is incremented. This feature is enabled by default.

To configure the MAC-address matching option for DHCP snooping, perform this task in privileged mode:

	Task	Command
Step 1	Enable the DHCP-snooping MAC-address matching option.	set dhcp-snooping match-mac enable
Step 2	Display the DHCP-snooping configuration.	show dhcp-snooping config

This example shows how to configure the DHCP-snooping MAC-address matching option:

```

Console> (enable) set dhcp-snooping match-mac enable
DHCP Snooping MAC address matching enabled.
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is enabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> (enable)

```

Configuration Examples for DHCP Snooping

These configuration examples show how to enable DHCP snooping.

Example 1: Enabling DHCP Snooping

This example shows how to enable DHCP snooping for VLAN 10 with a DHCP server on port 1/2:

```
Console> (enable) set security acl ip dhcp snooping permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcp-snoop. Use 'commit' command to
save changes.
Console> (enable) set security acl ip dhcp snooping permit ip any any
dhcp-snoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcp-snoop
ACL commit in progress.
```

```
ACL 'dhcp-snoop' successfully committed.
Console> (enable) set security acl map dhcp-snoop 10
Mapping in progress.
```

```
ACL dhcp-snoop successfully mapped to VLAN 10.
Console> (enable) set port dhcp-snooping 1/2 trust enable
Port(s) 1/2 state set to trusted for DHCP Snooping.
Console> show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-d0-00-4c-1b-ff.
Console> show port dhcp-snooping 1/1-2
Port      Trust
----      -
1/1      untrusted
1/2      trusted
Console> (enable)
```

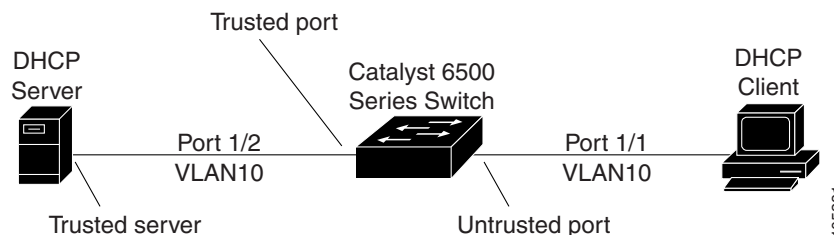


Note

If you want to configure DHCP-snooping host tracking after enabling DHCP snooping, enter the **set dhcp-snooping information-option host-tracking** command.

Figure 33-1 shows the typical topology that is used when you configure DHCP snooping in a client/server network.

Figure 33-1 DHCP Snooping Configured for a Client and Server



Example 2: Enabling DHCP Snooping with an MSFC as a DHCP Relay Agent

This example shows how to configure the Multilayer Switch Feature Card (MSFC) as a relay agent with the DHCP host tracking enabled.



Note

In this example, the client is untrusted and accesses the switch with the MSFC as a relay agent. The MSFC relay agent switch connects to the MSFC DHCP server switch through a trusted trunk port.

This example shows how to configure the MSFC as a DHCP relay agent:

```
service dhcp
on int vlan 810
  ip address 192.168.80.241 255.255.255.0
  ip helper-address 192.168.94.247
  ip dhcp relay information trusted
on int vlan 4094
  ip address 192.168.94.241 255.255.255.0
```

This example shows how to configure the MSFC as a DHCP server:

```
service dhcp
ip dhcp excluded-address 192.168.80.241
!
ip dhcp pool net810
  network 192.168.80.0 255.255.255.0
on int vlan 4094
  ip address 192.168.94.247 255.255.255.0
```

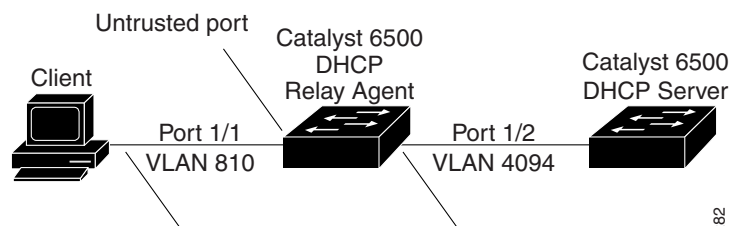


Note

The MSFC port is configured by the system as a DHCP-snooping trusted port.

Figure 33-2 shows the typical topology that is used when you configure the MSFC as a relay agent.

Figure 33-2 MSFC as a Relay Agent



Example 3: Enabling DHCP Snooping in Port-Based Mode

The following example shows how to enable DHCP snooping in port-based mode with a router as the MSFC. The DHCP-snooping ACL is mapped to the host VLAN.

```
Console> (enable) set security acl map dhcp 1/2
Mapping in progress.
ACL dhcp successfully mapped to port(s) 1/2
Console> (enable) set security acl map dhcp 16
Mapping in progress.
```

```
ACL dhcp successfully mapped to VLAN 16.
```

Enter the **show** command to display the security-acl mode:

```

Console> (enable) show port security-acl 1/2
Port Interface Type Interface Type Interface Merge Status
config runtime runtime
-----
1/2 port-based port-based not applicable

Config:
Port ACL name Type
-----
1/2 dhcp IP

Runtime:
Port ACL name Type
-----
1/2 dhcp IP

dhcp-snooping:
Port Trust Source-Guard Source-Guarded IP Addresses
-----
1/2 untrusted disabled

Port Binding Limit No. of Existing Bindings
-----
1/2 32 0

```

Enter the **show** command to verify the mapping:

```

Console> (enable) show security acl map config all
ACL Name Type Ports/Vlans
-----
dhcp IP 16
dhcp IP 1/2

```

The following example shows how to enable DHCP snooping in port-based mode with an external router configuration. DHCP snooping ACL is mapped to the host and the DHCP server port.



Note

Both the host and server ports are in port-based security ACL mode.

```

Console> (enable) set port security-acl 1/2 port-based
Warning: Vlan-based ACL features will be disabled on ports 1/2
ACL interface is set to port-based mode for port(s) 1/2.

```

```

Console> (enable) set port security-acl 5/2 port-based
Warning: Vlan-based ACL features will be disabled on ports 5/2
ACL interface is set to port-based mode for port(s) 5/2.

```

```

Console> (enable) set security acl map dhcp 1/2
Mapping in progress.
ACL dhcp successfully mapped to port(s) 1/2
Console> (enable) set security acl map dhcp 5/2
Mapping in progress.
ACL dhcp successfully mapped to port(s) 5/2

```

Enter the **show** command to display the security ACL mode:

```

Console> (enable) show port security-acl 1/2
Port Interface Type Interface Type Interface Merge Status
config runtime runtime
-----
1/2 port-based port-based not applicable

```

```

Config:
Port  ACL name                               Type
-----
1/2  dhcp                                     IP

Runtime:
Port  ACL name                               Type
-----
1/2  dhcp                                     IP

dhcp-snooping:
Port      Trust      Source-Guard      Source-Guarded IP Addresses
-----
1/2      untrusted    disabled

Port      Binding Limit      No. of Existing Bindings
-----
1/2      32                  0

Console> (enable) show port security-acl 5/2
Port  Interface Type Interface Type Interface Merge Status
config      runtime      runtime
-----
5/2      port-based   port-based       not applicable

Config:
Port  ACL name                               Type
-----
5/2  dhcp                                     IP

Runtime:
Port  ACL name                               Type
-----
5/2  dhcp                                     IP

dhcp-snooping:
Port      Trust      Source-Guard      Source-Guarded IP Addresses
-----
5/2      trusted    disabled

Port      Binding Limit      No. of Existing Bindings
-----
5/2      32                  0

```

Enter the **show** command to verify the ACL mappings:

```

Console> (enable) show security acl map config all
ACL Name                               Type Ports/Vlans
-----
dhcp                                     IP 1/2,5/2
No Mappings have been defined for any vlan yet.

```

Specifying the DHCP-Snooping Binding Limit on a Per-Port Basis

Use the **set port dhcp-snooping mod/port binding-limit count** command to specify the DHCP-snooping binding limit on a per-port basis. The minimum binding limit is 1, the maximum is 1024, and the default is 32. To specify the DHCP-snooping binding limit on a per-port basis, perform this task in privileged mode:

	Task	Command
Step 1	Specify the DHCP-snooping binding limit on a per-port basis.	set port dhcp-snooping mod/port binding-limit count
Step 2	Display the DHCP-snooping configuration.	show port dhcp-snooping [mod[/ports]]
Step 3	Display the static binding information.	show dhcp-snooping bindings
Step 4	Clear static bindings.	clear dhcp-snooping binding [port mod/port] [vlan vlanid] IP Address MAC Address

This example shows how to set the DHCP-snooping binding limit to 48 on port 5/9:

```
Console> (enable) set port dhcp-snooping 5/9 binding-limit 48
Port 5/9, DHCP Snooping binding limit set to 48
Console> (enable)
```

This example shows how to display the DHCP-snooping binding limit on port 5/9:

```
Console> (enable) show port dhcp-snooping 5/9
Port      Trust      Source-Guard      Source-Guarded IP Addresses
-----
5/9      untrusted    disabled

Port      Binding Limit
-----
5/9      48
Console> (enable)
```

This example shows how to display DHCP-snooping static bindings:

```
Console (enable) show dhcp-snooping bindings
MAC Address      IP Address      Lease(sec)      VLAN      Port
-----
00-01-7b-9b-05-3f  172.20.52.67    permanent       1         5/29
Console> (enable)
```

Specifying the DHCP-Snooping IP Address-to-MAC Address Binding on a Per-Port Basis

To specify the IP address-to-MAC address binding for the specified port, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address-to-MAC address binding for the specified port.	set port dhcp-snooping <i>mod/port add-binding ip-addr mac-addr [vlan]</i>
Step 2	Display the DHCP-snooping configuration.	show port dhcp-snooping [<i>mod[/ports]</i>]

This example shows how to specify the IP address-to-MAC address binding for the specified port:

```
Console> (enable) set port dhcp-snooping 5/29 add-binding 172.20.52.67 00-01-7b-9b-05-3f 1
DHCP Snooping Binding addition successful for Port 5/29, Vlan 1
IP addr 172.20.52.67, Mac Addr 00-01-7b-9b-05-3f.
Console> (enable)
```

Displaying DHCP-Snooping Information

You can display the DHCP-snooping binding table and configuration information using the commands in this section.

Displaying the Binding Table

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

To display DHCP-snooping binding table information, perform this task in privileged mode:

Task	Command
Display the DHCP-snooping binding table information.	show dhcp-snooping bindings

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

```
Console# show dhcp-snooping bindings
MacAddress      IpAddress      Lease(sec)    VLAN   Port
-----
00-01-7b-9b-05-3f  192.168.80.221  86377        810   1/8
```

Table 33-2 describes the fields in the **show dhcp-snooping binding** command output.

Table 33-2 *show dhcp-snooping bindings 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.
VLAN	VLAN number of the client port.
Port	Port that connects to the DHCP-client host.

Displaying the DHCP-Snooping Configuration and Statistics

To display DHCP-snooping configuration information for a switch, perform this task in privileged mode:

Task	Command
Display the DHCP-snooping configuration for a switch.	show dhcp-snooping config

This example shows how to display the DHCP-snooping host tracking and match-MAC configuration:

```

Console# show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-01-64-41-60-ff.
DHCP Snooping auto save is disabled.
DHCP Snooping bindings storage file is bootflash:dhcp-snooping-bindings-databas.
DHCP Snooping global bindings limit 16384.
DHCP Snooping available global bindings limit 16383.
Console> (enable)

```

To display the DHCP-snooping statistics for a switch, perform this task in privileged mode:

Task	Command
Display the DHCP-snooping statistics for a switch.	show dhcp-snooping statistics

This example shows how to display the DHCP-snooping statistics for a switch:

```

Console# show dhcp-snooping statistics
Packets forwarded           =          125
Packets dropped             =           3
Packets dropped from untrusted ports =           0
Number of bindings entries  =           5
Console#

```

To display the DHCP-snooping port configuration for a switch, perform this task in privileged mode:

Task	Command
Display the DHCP-snooping port configuration for a switch.	show port dhcp-snooping

This example shows how to display the DHCP-snooping port configuration for a switch:

■ Displaying DHCP-Snooping Information

```

Console> (enable) show port dhcp-snooping
Port      Trust      Source-Guard  Source-Guarded IP Addresses
-----
5/1       untrusted  disabled
5/2       trusted   disabled
5/3       untrusted  disabled
5/4       untrusted  disabled
5/5       untrusted  disabled
5/6       untrusted  disabled
5/7       untrusted  disabled
5/8       untrusted  disabled
5/9       untrusted  disabled
5/10      untrusted  disabled
5/11      untrusted  disabled
5/12      untrusted  disabled
5/13      untrusted  disabled
5/14      untrusted  disabled
5/15      untrusted  disabled
5/16      untrusted  disabled
5/17      untrusted  disabled
5/18      untrusted  disabled
5/19      untrusted  disabled
5/20      untrusted  disabled
5/21      untrusted  disabled
5/22      untrusted  disabled
5/23      untrusted  disabled
5/24      untrusted  disabled

Port      Binding Limit      No. of Existing Bindings
-----
5/1       32                  0
5/2       32                  0
5/3       32                  0
5/4       32                  0
5/5       32                  0
5/6       32                  0
5/7       32                  0
5/8       32                  0
5/9       32                  0
5/10      32                  0
5/11      32                  0

```

```

5/12 32 0
5/13 32 0
5/14 32 0
5/15 32 0
5/16 32 0
5/17 32 0
5/18 32 0
5/19 32 0
5/20 32 0
5/21 32 0
5/22 32 0
5/23 32 0
5/24 32 0
Console> (enable)

```

Storing DHCP-Snooping Binding Entries to a Flash Device

The DHCP-snooping binding entries can be stored to a flash device so the bindings can be restored immediately after the switch is reset.

The **auto-save** *interval* option is for configuring the auto-save interval for DHCP-snooping bindings. Valid ranges for the interval are 1 through 35000 minutes. Specifying a 0 disables the periodic saving of bindings on the flash device and deletes the bindings file stored in flash. Specifying a 0 does not clear a user-specified filename. The user-specified filename is cleared and returned to the default filename after the **clear config all** command is entered.

The *device:filename* option is for specifying the flash device and filename for storing the bindings. By default, the flash device is bootflash and the default filename is dhcp-snooping-bindings-database. If you have not configured a filename, the bindings are automatically saved with the default filename on the flash device.

To enable the **auto-save** option for DHCP-snooping binding entries and specify the interval to periodically save the bindings, perform this task in privileged mode:

Task	Command
Enable the auto-save option for DHCP-snooping binding entries and specify the interval to periodically save the bindings.	set dhcp-snooping bindings-database auto-save <i>interval</i>

This example shows how to enable the **auto-save** option for DHCP-snooping binding entries and specify an interval of 600 minutes to periodically save the bindings:

```

Console> (enable) set dhcp-snooping bindings-database auto-save 600
DHCP Snooping auto-save interval set to 600 minutes.
Console> (enable)

```

To specify the flash device and filename for storing the bindings, perform this task in privileged mode:

Task	Command
Specify the flash device and filename for storing the bindings.	set dhcp-snooping bindings-database device:[<i>filename</i>]

This example shows how to specify the flash device and filename for storing the bindings:

```

Console> (enable) set dhcp-snooping bindings-database disk1:dhcp-bindings

```

```
DHCP Snooping bindings storage file set to disk1:dhcp-bindings.
Console> (enable)
```

This example shows how to display the DHCP-snooping bindings-database configuration:

```
Console> (enable) show dhcp-snooping config
DHCP Snooping MAC address matching is enabled.
DHCP Snooping host-tracking information option is disabled.
Remote ID used in information option is 00-01-64-41-60-ff.
DHCP Snooping auto save interval is 600.
DHCP Snooping bindings storage file is disk1:dhcp-bindings.
Console> (enable)
```

Understanding How IP Source Guard Works

IP source guard prevents IP spoofing by allowing only the IP addresses that are obtained through DHCP snooping on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, a port access control list (PACL) is installed on the port that permits the traffic from the IP address. This process restricts the client IP traffic to those source IP addresses that are obtained from the DHCP server; any IP traffic with a source IP address other than that in the PACL's permit list is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address.



Note

If you enable IP source guard on a trunk port with a large number of VLANs that have DHCP snooping enabled, you might run out of the ACL hardware resources, and some clients that are connected to the ports may not be able to send the traffic. We do not recommend using this configuration because you are limited to ten IP addresses per port.



Note

In software releases prior to software release 8.6(1), you are limited to ten IP addresses per port. In software release 8.6(1) and later releases, you can have up to 48 IP addresses per port.

IP source guard uses source IP address filtering, which filters the IP traffic that is based on its source IP address. Only the IP traffic with a source IP address that matches the IP source binding entry is permitted.

A port's IP source address filter is changed when a new DHCP-snooping binding entry for a port is created or deleted. The port PACL is modified and reapplied in the hardware to reflect the IP source binding change. By default, if you enable IP source guard without any DHCP-snooping bindings on the port, a default PACL that denies all IP traffic is installed on the port. When you disable IP source guard, any IP source filter PACL is removed from the port.

IP Source Guard Configuration Guidelines

This section describes the guidelines for configuring IP source guard in your network:

- IP source guard is supported on PFC 3 and later versions.
- In software releases prior to software release 8.6(1), you are limited to ten IP addresses per port. In software release 8.6(1) and later releases, you can have up to 48 IP addresses per port.
- IP source guard is not recommended on trunk ports.

- IP source guard cannot coexist with PACLs.
- IP source guard is not supported on EtherChannel-enabled ports, and EtherChannel is not supported on IP source guard-enabled ports.
- VLAN-based ACL features, such as static ARP inspection, are disabled when you enable IP source guard.
- We recommend that you enable high availability when using dynamic ARP inspection (DAI), DHCP snooping, and IP source guard. If high availability is not enabled, clients have to renew their IP addresses for these features to work after a switchover. For configuration details on DAI, see the [“Dynamic ARP Inspection” section on page 15-39](#).

Enabling IP Source Guard on a Port

To enable IP source guard, perform this task in privileged mode:

	Task	Command
Step 1	Configure the port as port based.	set port security-acl 3/1 port-based
Step 2	Enable IP source guard.	set port dhcp-snooping 3/1 source-guard enable
Step 3	Enable DHCP snooping.	set security acl ip dhcpsnoop permit dhcp-snooping
Step 4	Allow the port to forward other traffic.	set security acl ip dhcpsnoop permit ip any any
Step 5	Save the ACL configuration.	commit security acl dhcpsnoop
Step 6	Enable the ACL on the VLAN.	set security acl map dhcpsnoop 10
Step 7	Enable DHCP-snooping trust on a port.	set port dhcp-snooping 1/2 trust enable



Note

Before you can enable IP source guard, you must enable DHCP snooping on the VLAN to which the port belongs. You must configure the port as either port based or in merge mode for security ACLs. You should only enable IP source guard on DHCP-snooping untrusted ports.

This example shows how to enable IP source guard:

```

Console> (enable) set port security-acl 3/1 port-based
Warning:Vlan-based ACL features will be disabled on ports 3/1.
ACL interface is set to port-based mode for port(s) 3/1.
Console> (enable) set port dhcp-snooping 3/1 source-guard enable
IP Source Guard enabled on port(s) 3/1.

Console> (enable) set port dhcp-snooping 1/2 trust enable
Port(s) 1/2 state set to trusted for DHCP Snooping.
Console> (enable) set security acl ip dhcpsnoop permit dhcp-snooping
Successfully configured DHCP Snooping for ACL dhcpsnoop. Use 'commit' command to
save changes.

Console> (enable) set security acl ip dhcpsnoop permit ip any any
dhcpsnoop editbuffer modified. Use 'commit' command to apply changes.
Console> (enable) commit security acl dhcpsnoop
ACL commit in progress.

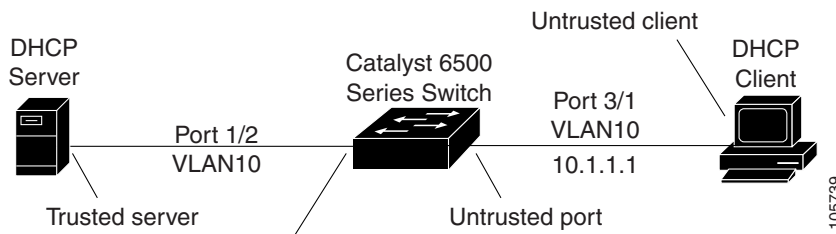
ACL 'dhcpsnoop' successfully committed.
Console> (enable) set security acl map dhcpsnoop 10
Mapping in progress.

```

```
ACL dhcp successfully mapped to port(s) 5/1.
Console>
```

Figure 33-3 shows the typical topology that is used when you configure IP source guard on an untrusted port.

Figure 33-3 IP Source Guard Enabled on an Untrusted Port



Displaying the IP Source Guard Information

You can display the information about IP source guard for all ports on a switch using the **show port dhcp-snooping** command. To display information about IP source guard on a module, perform this task in normal mode:

Task	Command
Display information about IP source guard on a port.	show port dhcp-snooping 4

This example shows how to display the configuration for IP source guard on a port:

```
Console> (enable) show port dhcp-snooping 3/25
Port      Trust      Source-Guard      Source-Guarded IP Addresses
-----
 3/25    untrusted      enabled           192.168.80.6, 192.168.80.5,
                                     192.168.80.4, 192.168.80.3,
                                     192.168.80.2, 192.168.80.1

Console> (enable)
```