CHAPTER 21

Configuring DHCP Features and IP Source Guard

This chapter describes how to configure DHCP snooping and option-82 data insertion, and the DHCP server port-based address allocation features on the switch. It also describes how to configure the IP source guard feature.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for this release, and see the "DHCP Commands" section in the *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2* **Documentation > Cisco IOS Software 12.2 Mainline Command References**

This chapter consists of these sections:

- Understanding DHCP Features, page 21-1

Configuring DHCP Features, page 21-7

Displaying DHCP Snooping Information, page 21-15

Understanding IP Source Guard, page 21-15

Configuring IP Source Guard, page 21-16

Displaying IP Source Guard Information, page 21-18

Understanding DHCP Server Port-Based Address Allocation, page 21-18

Configuring DHCP Server Port-Based Address Allocation, page 21-19

Displaying DHCP Server Port-Based Address Allocation, page 21-22

Understanding DHCP Features

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts; only those hosts that are connected to the network consume IP addresses.

These sections contain this information:

DHCP Server, page 21-2

DHCP Relay Agent, page 21-2

DHCP Snooping, page 21-2

Option-82 Data Insertion, page 21-3

-
-

Configuring DHCP *IP Addressing and Services* *Cisco IOS IP Configuration Guide, Release 12.2* **Configuration Guides**

DHCP Server

clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator.

DHCP Relay Agent

DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch.

Note For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

An untrusted DHCP message is a message that is received from outside the network or firewall. When you use DHCP snooping in a service-provider environment, an untrusted message is sent from a device that is not in the service-provider network, such as a customer's switch. Messages from unknown devices are untrusted because they can be sources of traffic attacks.

The DHCP snooping binding database has the MAC address, the IP address, the lease time, the binding type, the VLAN number, and the interface information that corresponds to the local untrusted interfaces of a switch. It does not have information regarding hosts interconnected with a trusted interface.

In a service-provider network, a trusted interface is connected to a port on a device in the same network. An untrusted interface is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN in which DHCP snooping is enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet.

The switch drops a DHCP packet when one of these situations occurs:

A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.

A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.

The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.

A DHCP relay agent forwards a DHCP packet that includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.

If the switch is an aggregation switch supporting DHCP snooping and is connected to an edge switch that is inserting DHCP option-82 information, the switch drops packets with option-82 information when packets are received on an untrusted interface. If DHCP snooping is enabled and packets are received on a trusted port, the aggregation switch does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

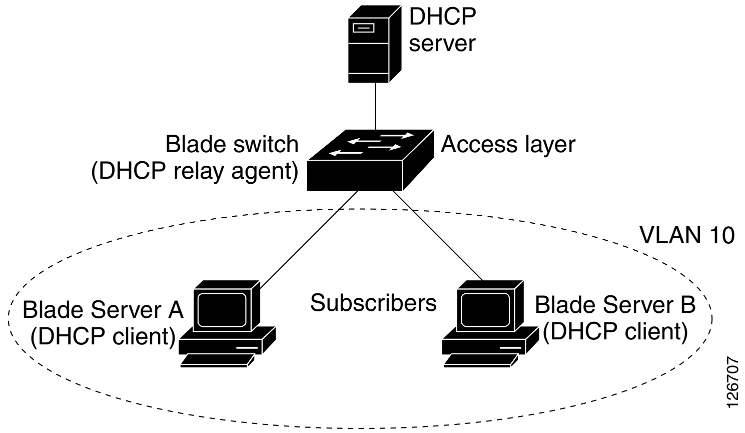
You cannot configure IP source guard and dynamic Address Resolution Protocol (ARP) inspection on the switch unless you use static bindings or ARP access control lists (ACLs).

When an aggregation switch can be connected to an edge switch through an untrusted interface and you enter the **ip dhcp snooping information option allow-untrusted**

Option-82 Data Insertion

Note

Figure 21-1 DHCP Relay Agent in a Metropolitan Ethernet Network



When you enable the DHCP snooping information option 82 on the switch, this sequence of events occurs:

The Blade Server (DHCP client) generates a DHCP request and broadcasts it on the network.

When the blade switch receives the DHCP request, it adds the option-82 information in the packet. By default, the The remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier, **vlan-mod-port**

–

–

–

–

–

–

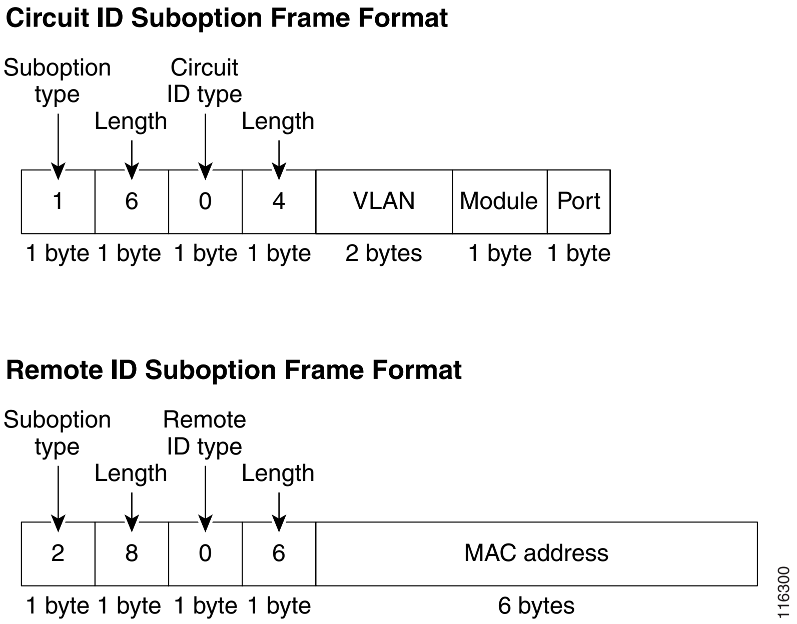
–

–

Blade Switch 3020 for HP, which as 24 ports, port 1 is the Gigabit Ethernet 0/1 port, port 2 is the Gigabit Ethernet 0/2 port, port 3 is the Gigabit Ethernet 0/3 port, and so on. Ports 17 to 20 are dual-purpose SFP module/RJ-45 copper Ethernet uplink ports Gi0/17 to Gi0/20. Ports 21x and 22x are copper 10/100/1000BASE-T ports Gi0/21 and Gi0/22. Ports 23x and 24x are dual-purpose external/internal 10/100/1000BASET copper uplink ports Gi0/23 and Gi0/24.

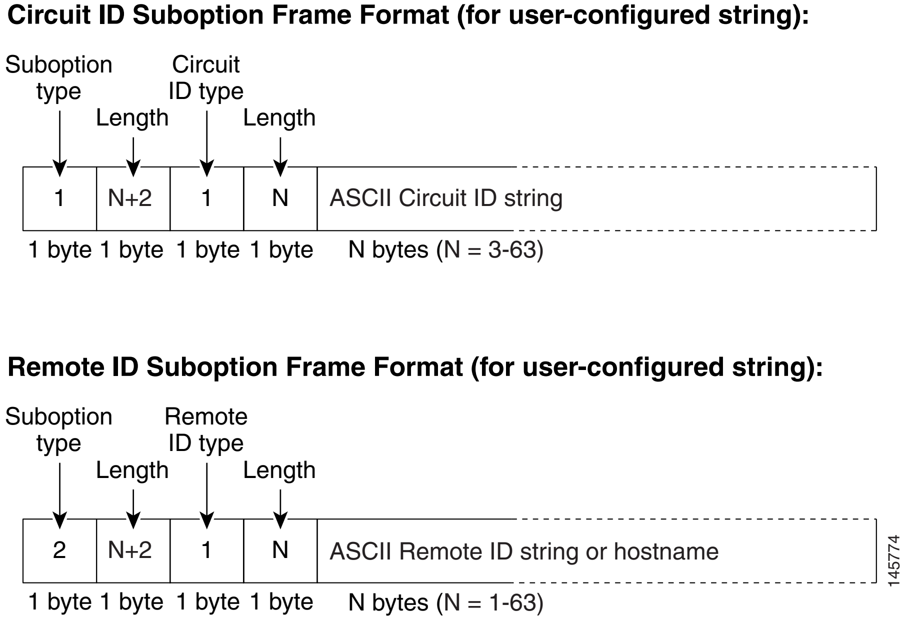
Figure 21-2 shows the packet formats for the remote-ID suboption and the circuit-ID suboption when the default suboption configuration is used.The switch uses the packet formats when you globally enable DHCP snooping and enter the global configuration command.

Suboption Packet Formats



information option format-type circuit-id string

Figure 21-3 User-Configured Suboption Packet Formats



Cisco IOS DHCP Server Database

address bindings

Cisco IOS IP Configuration Guide, Release 12.2

DHCP Snooping Binding Database

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-..-n>
END
```

initial-checksum

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Fa1/0/4 21ae5fbb
192.1.168.3 3 0003.44d6.c52f 2BB648EB Fa1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Fa1/0/4 584a38f0
END
```

Configuring DHCP Features

-
-
-
-
-

Enabling DHCP Snooping and Option 82, page 21-11

Enabling DHCP Snooping on Private VLANs, page 21-13

Enabling the Cisco IOS DHCP Server Database, page 21-13

Enabling the DHCP Snooping Binding Database Agent, page 21-14

Default DHCP Configuration

Table 21-1 Default DHCP Configuration

Feature	Default Setting
	[1]
DHCP relay agent	Enabled[2]
DHCP packet forwarding address	None configured
Checking the relay agent information	Enabled (invalid messages are dropped)[2]
DHCP relay agent forwarding policy	Replace the existing relay agent information[2]
DHCP snooping enabled globally	Disabled
DHCP snooping information option	Enabled
DHCP snooping option to accept packets on untrusted input interfaces[3]	Disabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping VLAN	Disabled
DHCP snooping MAC address verification	Enabled
Cisco IOS DHCP server binding database	Enabled in Cisco IOS software, requires configuration. The switch gets network addresses and configuration parameters only from a device configured as a DHCP server.
DHCP snooping binding database agent	Enabled in Cisco IOS software, requires configuration. This feature is operational only when a destination is configured.

[1] The switch responds to DHCP requests only if it is configured as a DHCP server.

[2] The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.

[3] Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.

DHCP Snooping Configuration Guidelines

•

•

•

•

– **ip dhcp relay information check**

ip dhcp relay information policy

ip dhcp relay information trust-all

ip dhcp relay information trusted

ip dhcp
snooping trust

no ip
dhcp snooping trust

ip dhcp snooping information option allow-untrusted

show ip dhcp snooping statistics user EXEC command, and you can clear the snooping statistics counters by entering the privileged EXEC command.

Do not enable Dynamic Host Configuration Protocol (DHCP) snooping on RSPAN VLANs. If DHCP snooping is enabled on RSPAN VLANs, DHCP packets might not reach the RSPAN destination port.

Configuring the DHCP Server

Configuring the DHCP Relay Agent

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

-
-

Specifying the Packet Forwarding Address

	Command	Purpose
Step 1		
Step 2		
Step 3	*ip-address subnet-mask*	

	Command	Purpose
Step 4		
Step 5	exit	
Step 6		
Step 7		
Step 8		
Step 9		
Step 10		
Step 11		

address

Enabling DHCP Snooping and Option 82

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		

Step 5	[|]	(Optional) Configure the remote-ID suboption. You can configure the remote ID to be: String of up to 63 ASCII characters (no spaces) Configured hostname for the switch If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration. The default remote ID is the switch MAC address.
		(Optional) If the switch is an aggregation switch connected to an edge switch, enable the switch to accept incoming DHCP snooping packets with option-82 information from the edge switch. The default setting is disabled. Enter this command only on aggregation switches that are connected to trusted devices.
		Specify the interface to be configured, and enter interface configuration mode.
		(Optional) Configure the circuit-ID suboption for the specified interface. Specify the VLAN and port identifier, using a VLAN ID in the range of 1 to 4094. The default circuit ID is the port identifier, in the format . You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces).
		(Optional) Configure the interface as trusted or untrusted. You can use the keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.
		(Optional) Configure the number of DHCP packets per second that an interface can receive. The range is 1 to 2048. By default, no rate limit is configured. We recommend an untrusted rate limit of not more than 100 packets per second. If you configure rate limiting for trusted interfaces, you might need to increase the rate limit if the port is a trunk port assigned to more than one VLAN on which DHCP snooping is enabled.
		Return to global configuration mode.
		(Optional) Configure the switch to verify that the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet. The default is to verify that the source MAC address matches the client hardware address in the packet.
		Return to privileged EXEC mode.
		Verify your entries.
		(Optional) Save your entries in the configuration file.

To disable DHCP snooping, use the global configuration command. To disable DHCP snooping on a VLAN or range of VLANs, use the global configuration command. To disable the insertion and removal of the option-82 field, use the global configuration command. To configure an aggregation switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, use the global configuration command.

This example shows how to enable DHCP snooping globally and on VLAN 10 and to configure a rate limit of 100 packets per second on a port:

```
Switch(config)# ip dhcp snooping
                ip dhcp snooping vlan 10
                ip dhcp snooping information option
                interface gigabitethernet0/1
                   ip dhcp snooping limit rate 100
```

Enabling DHCP Snooping on Private VLANs

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not take
effect on secondary vlan 200. DHCP Snooping configuration on secondary vlan is derived
from its primary vlan.
```

configure terminal	
ip dhcp snooping database { [ ]**:/** **ftp://** **:***password@host filename* *username password*]@]{ *me* | *host-ip*}[*/directory* *image-name* *user@host filename* *host filename*	*number* *filename* *number* *number* *user password@* **/** **http://** **:** **/** **.tar** **rcp://** **@** **/** **tftp://** **/**
ip dhcp snooping database timeout	
ip dhcp snooping database write-delay	
end	
ip dhcp snooping binding **vlan** **interface** **expiry**	
show ip dhcp snooping database **detail**	
copy running-config startup-config	

no ip dhcp snooping database **ip dhcp snooping database** **timeout** **ip dhcp snooping database write-delay**

clear ip dhcp snooping **database statistics** **renew ip dhcp snooping** **database**

no ip dhcp snooping **binding** **vlan** **interface**

Displaying DHCP Snooping Information

Commands for Displaying DHCP Information

Command	Purpose

Note

Understanding IP Source Guard

Source IP Address Filtering

Source IP and MAC Address Filtering

Configuring IP Source Guard

-
-
-

Default IP Source Guard Configuration

IP Source Guard Configuration Guidelines

-

Note

Enabling IP Source Guard

	Command	Purpose
Step 1		
Step 2		
Step 3		**Note**
Step 4		
Step 5		
Step 6		

	Command	Purpose
Step 7		
Step 8		
Step 9		

```
        configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config-if)# ip verify source port-security
                   exit
                ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet1/0/1
                ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
                end
```

Commands for Displaying IP Source Guard Information

Command	Purpose

Understanding DHCP Server Port-Based Address Allocation

Configuring DHCP Server Port-Based Address Allocation

-
-
-

Default Port-Based Address Allocation Configuration

Port-Based Address Allocation Configuration Guidelines

-
-
-

Enabling DHCP Server Port-Based Address Allocation

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		
Step 8		

	Command	Purpose
Step 1		
Step 2		
Step 3	*/prefix-length*	
	ip-address *string*	*string*—can be an ASCII value or a hexadecimal value.
		Return to privileged EXEC mode.
		Verify DHCP pool configuration.
		(Optional) Save your entries in the configuration file.

To disable DHCP port-based address allocation, use the global configuration command. To disable the automatic generation of a subscriber identifier, use the global configuration command. To disable the subscriber identifier on an interface, use the interface configuration command.

To remove an IP address reservation from a DHCP pool, use the DHCP pool configuration command.

In this example, a subscriber identifier is automatically generated, and the DHCP server ignores any client identifier fields in the DHCP messages and uses the subscriber identifier instead. The subscriber identifier is based on the short name of the interface and the client preassigned IP address 10.1.1.7.

```
        show running config


!
version 12.2
!
hostname switch
!
no aaa new-model
clock timezone EST 0
ip subnet-zero
ip dhcp relay information policy removal pad
no ip dhcp use vrf connected
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id "Et1/0" ascii
<output truncated>
```

```
switch#
Pool dhcp pool:
 Utilization mark (high/low) : 100 / 0
 Subnet size (first/next) : 0 / 0
 Total addresses : 254
 Leased addresses : 0
 Excluded addresses : 4
 Pending event : none
 1 subnet is currently in the pool:
 Current index   IP address range         Leased/Excluded/Total
 10.1.1.1        10.1.1.1 - 10.1.1.254     0     / 4 / 254
 1 reserved address is currently in the pool
 Address         Client
 10.1.1.7 Et1/0
```

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

To display the DHCP server port-based address allocation information, use one or more of the privileged EXEC commands in Table 21-4:

Table 21-4 Commands for Displaying DHCP Port-Based Address Allocation Information
