IP Addressing Services Configuration Guide, Cisco IOS Release 15.2(7)Ex (Catalyst 2960-L Switches)

Revised: April 25, 2022

Configuring DHCP

Prerequisites for Configuring DHCP

The section describes the prerequisites for DHCP Snooping and Option 82:

- You must globally enable DHCP snooping on the device.
- Before globally enabling DHCP snooping on the device, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- If you want the device to respond to DHCP requests, it must be configured as a DHCP server.
- Before configuring the DHCP snooping information option on your device, be sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.
- For DHCP snooping to function properly, all DHCP servers must be connected to the device through trusted interfaces. In a service-provider network, a trusted interface is connected to a port on a device in the same network.
- You must configure the device to use the Cisco IOS DHCP server binding database to use it for DHCP snooping.
- To use the DHCP snooping option of accepting packets on untrusted inputs, the device must be an aggregation device that receives packets with option-82 information from an edge device.
- The following prerequisites apply to DHCP snooping binding database configuration:
    - You must configure a destination on the DHCP snooping binding database to use the device for DHCP snooping.
    - Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store the binding file on a TFTP server.
    - For network-based URLs (such as TFTP and FTP), you must create an empty file at the configured URL before the device can write bindings to the binding file at that URL. See the documentation for your TFTP server to determine whether you must first create an empty file on the server; some TFTP servers cannot be configured this way.
    - To ensure that the lease time in the database is accurate, we recommend that you enable and configure Network Time Protocol (NTP).
    - If NTP is configured, the device writes binding changes to the binding file only when the device system clock is synchronized with NTP.
- Before configuring the DHCP relay agent on your device, make sure to configure the device that is acting as the DHCP server. You must specify the IP addresses that the DHCP server can assign or exclude, configure DHCP options for devices, or set up the DHCP database agent.
- For a device to relay DHCP packets, the IP address of the DHCP server must be configured on the device virtual interface (SVI) of the DHCP client.
- If a switch port is connected to a DHCP server, configure a port as trusted by entering the **ip dhcp snooping trust interface** configuration command.

- If a switch port is connected to a DHCP client, configure a port as untrusted by entering the **no ip dhcp snooping trust** interface configuration command.

Restrictions for Configuring DHCP

This section describes the restrictions for DHCP Snooping and Option 82:

- The DHCP option-82 feature is supported only when DHCP snooping is globally enabled and on the VLANs to which subscriber devices using this feature are assigned.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- When configuring a large number of circuit IDs on a device, consider the impact of lengthy character strings on the NVRAM or the flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.
- If the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.
- Do not enter the **ip dhcp snooping information option allow-untrusted** command on an aggregation device to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.
- Only one IP address can be assigned per port.
- Reserved addresses (preassigned) cannot be cleared by using the **clear ip dhcp binding** global configuration command.
- Preassigned addresses are automatically excluded from normal dynamic IP address assignment. Preassigned addresses cannot be used in host pools, but there can be multiple preassigned addresses per DHCP address pool.
- If DHCP snooping is enabled on RSPAN VLANs, DHCP packets might not reach the RSPAN destination port.
- The DHCP server port-based address allocation feature is only supported on a Cisco IOS DHCP server and not a third-party server.
- The following scenario is not supported:

  A non-DHCP snooping VLAN, and the SVI of the non-DHCP snooping VLAN is configured on a device. The SVI of the non-DHCP snooping VLAN is configured with the status of *no shutdown*. In this scenario, the DHCP packets in the non-DHCP snooping VLAN are not forwarded to the trusted ports.

  If the SVI of the non-DHCP snooping VLAN is not configured or is configured with the *shutdown* status, DHCP packets are forwarded to the trusted ports, and DHCP clients can obtain IP address from the DHCP server.

Information About Configuring DHCP

DHCP Server

The DHCP server assigns IP addresses from specified address pools on a device to DHCP 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. The device can act as a DHCP server.

DHCP Relay Agent

A DHCP relay agent is a Layer 3 device that forwards DHCP packets between clients and servers. Relay agents forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces.

DHCP Snooping

DHCP snooping is a DHCP security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table.

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 device.

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

An untrusted DHCP message is a message that is received through an untrusted interface. By default, the device considers all interfaces untrusted. So, the device must be configured to trust some interfaces to use DHCP Snooping. 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 device. 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 device. It does not have information regarding hosts interconnected with a trusted interface.

Note When configuring DHCP snooping to block unauthorized IP address using the **ip verify source prot-security** command on an interface, the **switchport port-security** command should also be configured.

In a service-provider network, an example of an interface you might configure as trusted is one connected to a port on a device in the same network. An example of an untrusted interface is one that is connected to an untrusted interface in the network or to an interface on a device that is not in the network.

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

The device 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 device 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 device is an aggregation device supporting DHCP snooping and is connected to an edge device that is inserting DHCP option-82 information, the device 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 device does not learn the DHCP snooping bindings for connected devices and cannot build a complete DHCP snooping binding database.

When an aggregation device can be connected to an edge device through an untrusted interface and you enter the **ip dhcp snooping information option allow-untrusted** command, the aggregation device accepts packets with option-82 information from the edge device. The aggregation device learns the bindings for hosts connected through an untrusted device interface. The DHCP security features, such as dynamic ARP inspection or IP source guard, can still be enabled on the aggregation device while the device receives packets with option-82 information on untrusted input interfaces to which hosts are connected. The port on the edge device that connects to the aggregation device must be configured as a trusted interface.

Normally, it is not desirable to broadcast packets to wireless clients. So, DHCP snooping replaces destination broadcast MAC address (ffff.ffff.ffff) with unicast MAC address for DHCP packets that are going from server to wireless clients. The unicast MAC address is retrieved from CHADDR field in the DHCP payload. This processing is applied for server to client packets such as DHCP OFFER, DHCP ACK, and DHCP NACK messages. The **ip dhcp snooping wireless bootp-broadcast enable** can be used to revert this behavior. When the wireless BOOTP broadcast is enabled, the broadcast DHCP packets from server are forwarded to wireless clients without changing the destination MAC address.

Default DHCP Snooping Configuration

Table 1: Default DHCP Configuration

Feature	Default Setting
DHCP server	Enabled in Cisco IOS software, requires configuration[1]
DHCP relay agent	Enabled[2]
DHCP packet forwarding address	None configured
Checking the relay agent information	Enabled (invalid messages are dropped)
DHCP relay agent forwarding policy	Replace the existing relay agent information
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. **Note** The switch gets network addresses and configuration parameters only from a device configured as a DHCP server.

Feature	Default Setting
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 Binding Database

When DHCP snooping is enabled, the device uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 64,000 bindings.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database agent stores the bindings in a file at a configured location. At the end of each entry is a checksum that accounts for all the bytes from the start of the file through all the bytes associated with the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the device reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP inspection or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the device loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the device does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the device reads the binding file to build the DHCP snooping binding database. The device updates the file when the database changes.

When a device learns of new bindings or when it loses bindings, the device immediately updates the entries in the database. The device also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

This is the format of the file with bindings:

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

Each entry in the file is tagged with a checksum value that the device uses to verify the entries when it reads the file. The initial-checksum entry on the first line distinguishes entries associated with the latest file update from entries associated with a previous file update.

This is an example of a binding file:

```
2bb4c2a1
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
192.1.168.1 3 0003.47d8.c91f 2BB6488E Gi1/0/4 21ae5fbb
```

```
192.1.168.3 3 0003.44d6.c52f 2BB648EB Gi1/0/4 1bdb223f
192.1.168.2 3 0003.47d9.c8f1 2BB648AB Gi1/0/4 584a38f0
END
```

When the device starts and the calculated checksum value equals the stored checksum value, the device reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The device ignores an entry when one of these situations occurs:

- The device reads the entry and the calculated checksum value does not equal the stored checksum value. The entry and the ones following it are ignored.
- An entry has an expired lease time (the device might not remove a binding entry when the lease time expires).
- The interface in the entry no longer exists on the system.
- The interface is a routed interface or a DHCP snooping-trusted interface.

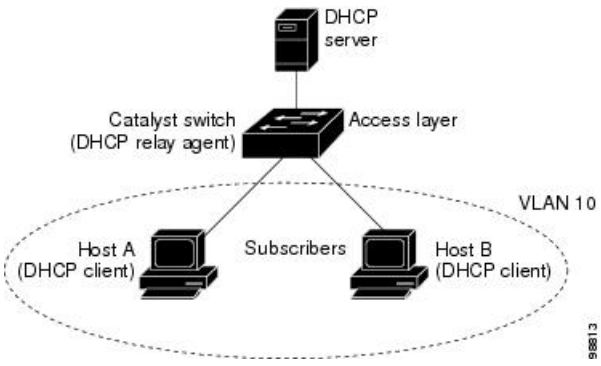
Option-82 Data Insertion

In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the device, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access device and are uniquely identified.

Note The DHCP option-82 feature is supported only when DHCP snooping is globally enabled on the VLANs to which subscriber devices using option-82 are assigned.

The following illustration shows a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the device at the access layer. Because the DHCP clients and their associated DHCP server do not reside on the same IP network or subnet, a DHCP relay agent (the Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

Figure 1: DHCP Relay Agent in a Metropolitan Ethernet Network



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

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the device receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the device MAC address, and the circuit-ID suboption is the port identifier, **vlan-mod-port**, from which the packet is received.You can configure the remote ID and circuit ID.

- If the IP address of the relay agent is configured, the device adds this IP address in the DHCP packet.
- The device forwards the DHCP request that includes the option-82 field to the DHCP server.
- 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. Then the DHCP server echoes the option-82 field in the DHCP reply.
- The DHCP server unicasts the reply to the device if the request was relayed to the server by the device. The device verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The device removes the option-82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

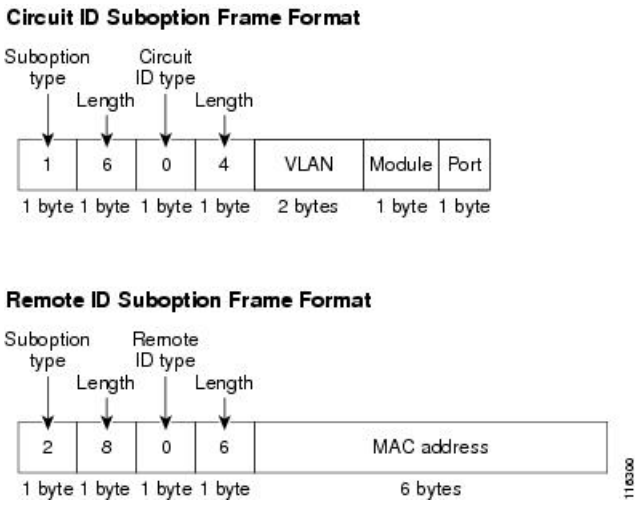
In the default suboption configuration, when the described sequence of events occurs, the values in these fields do not change (see the illustration,*Suboption Packet Formats*):

- Circuit-ID suboption fields
    - Suboption type
    - Length of the suboption type
    - Circuit-ID type
    - Length of the circuit-ID type
- Remote-ID suboption fields
    - Suboption type
    - Length of the suboption type
    - Remote-ID type
    - Length of the remote-ID type

In the port field of the circuit ID suboption, the port numbers start at 3. For example, on a device with 24 10/100/1000 ports and four small form-factor pluggable (SFP) module slots, port 3 is the GigabitEthernet 1/0/1 port, port 4 is the GigabitEthernet 1/0/2 port, and so forth. Port 27 is the SFP module slot Gigabit Ethernet1/0/25, and so forth.

The illustration, *Suboption Packet Formats*. shows the packet formats for the remote-ID suboption and the circuit-ID suboption when the default suboption configuration is used. The device uses the packet formats when you globally enable DHCP snooping and enter the **ip dhcp snooping information option** command.

Figure 2: Suboption Packet Formats

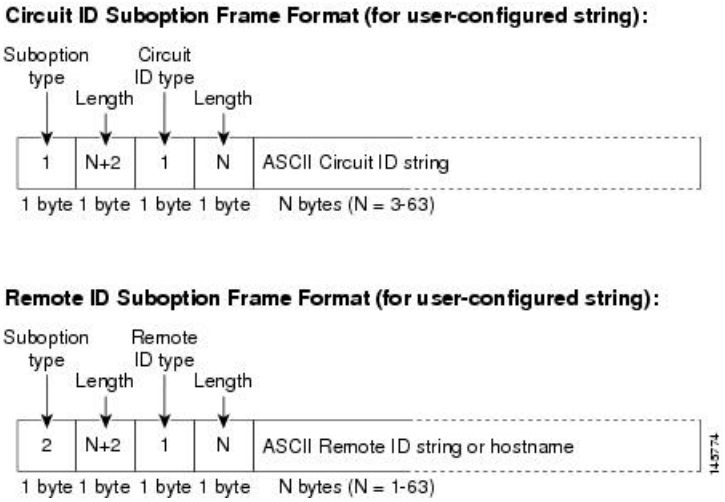


The illustration, *User-Configured Suboption Packet Formats,* shows the packet formats for user-configured remote-ID and circuit-ID suboptions The device uses these packet formats when DHCP snooping is globally enabled and when the **ip dhcp snooping information option format remote-id** command and the **ip dhcp snooping vlan information option format-type circuit-id string** command are entered.

The values for these fields in the packets change from the default values when you configure the remote-ID and circuit-ID suboptions:

- Circuit-ID suboption fields
  - The circuit-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.
- Remote-ID suboption fields
  - The remote-ID type is 1.
  - The length values are variable, depending on the length of the string that you configure.

Figure 3: User-Configured Suboption Packet Formats



DHCP Server Port-Based Address Allocation

DHCP server port-based address allocation is a feature that enables DHCP to maintain the same IP address on an Ethernet switch port regardless of the attached device client identifier or client hardware address.

When Ethernet devices are deployed in the network, they offer connectivity to the directly connected devices. In some environments, such as on a factory floor, if a device fails, the replacement device must be working immediately in the existing network. With the current DHCP implementation, there is no guarantee that DHCP would offer the same IP address to the replacement device. Control, monitoring, and other software expect a stable IP address associated with each device. If a device is replaced, the address assignment should remain stable even though the DHCP client has changed.

When configured, the DHCP server port-based address allocation feature ensures that the same IP address is always offered to the same connected port even as the client identifier or client hardware address changes in the DHCP messages received on that port. The DHCP protocol recognizes DHCP clients by the client identifier option in the DHCP packet. Clients that do not include the client identifier option are identified by the client hardware address. When you configure this feature, the port name of the interface overrides the client identifier or hardware address and the actual point of connection, the switch port, becomes the client identifier.

In all cases, by connecting the Ethernet cable to the same port, the same IP address is allocated through DHCP to the attached device.

The DHCP server port-based address allocation feature is only supported on a Cisco IOS DHCP server and not a third-party server.

Default Port-Based Address Allocation Configuration

By default, DHCP server port-based address allocation is disabled.

Port-Based Address Allocation Configuration Guidelines

- By default, DHCP server port-based address allocation is disabled.
- To restrict assignments from the DHCP pool to preconfigured reservations (unreserved addresses are not offered to the client and other clients are not served by the pool), you can enter the **reserved-only** DHCP pool configuration command.

Cisco IOS DHCP Server Database

During the DHCP-based autoconfiguration process, the designated DHCP server uses the Cisco IOS DHCP server database. It has IP addresses, address bindings, and configuration parameters, such as the boot file.

An address binding is a mapping between an IP address and a MAC address of a host in the Cisco IOS DHCP server database. You can manually assign the client IP address, or the DHCP server can allocate an IP address from a DHCP address pool.

How to Configure DHCP

Configuring the DHCP Server

The device can act as a DHCP server.

Configuring the DHCP Relay Agent

Follow these steps to enable the DHCP relay agent on the switch:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**service dhcp** **Example:** `Device(config)# service dhcp`	Enables the DHCP server and relay agent on your switch. By default, this feature is enabled.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

What to do next

- Checking (validating) the relay agent information
- Configuring the relay agent forwarding policy

Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets, you must configure the device with the **ip helper-address** *address* interface configuration command. The general rule is to configure the command on the Layer 3 interface closest to the client. The address used in the **ip helper-address** command can be a specific DHCP server IP address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables any DHCP server to respond to requests.

Beginning in privileged EXEC mode, follow these steps to specify the packet forwarding address:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface vlan** *vlan-id* **Example:** `Device(config)# interface vlan 1`	Creates a switch virtual interface by entering a VLAN ID, and enters interface configuration mode.
Step 4	**ip address** *ip-address subnet-mask* **Example:** `Device(config-if)# ip address 192.108.1.27 255.255.255.0`	Configures the interface with an IP address and an IP subnet.
Step 5	**ip helper-address** *address* **Example:** `Device(config-if)# ip helper-address 172.16.1.2`	Specifies the DHCP packet forwarding address. • The helper address can be a specific DHCP server address, or it can be the network address if other DHCP servers are on the destination network segment. Using the network address enables other servers to respond to DHCP requests. • If you have multiple servers, you can configure one helper address for each server.
Step 6	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 7	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 0/1`	Configures a single physical port that is connected to the DHCP client, and enters interface configuration mode.
Step 8	**switchport mode access** **Example:** `Device(config-if)# switchport mode access`	Defines the VLAN membership mode for the port.
Step 9	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 1`	Assigns the ports to the same VLAN as configured in Step 2.
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling DHCP Snooping and Option 82

Follow these steps to enable DHCP snooping on the device:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp snooping** **Example:** `Device(config)# ip dhcp snooping`	Enables DHCP snooping globally.
Step 4	**ip dhcp snooping vlan** *vlan-range* **Example:**	Enables DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094.

	Command or Action	Purpose
	`Device(config)# ip dhcp snooping vlan 10`	• You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.
Step 5	**ip dhcp snooping information option** **Example:** `Device(config)# ip dhcp snooping information option`	Enables the device to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages to the DHCP server. This is the default setting.
Step 6	**ip dhcp snooping information option format remote-id** [**string** *ASCII-string* | **hostname**] **Example:** `Device(config)# ip dhcp snooping information option format remote-id string acsiistring2`	(Optional) Configures the remote-ID option. You can configure the remote ID as: • String of up to 63 ASCII characters (no spaces) • Configured hostname for the device **Note** 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 device MAC address.
Step 7	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 0/1`	Specifies the interface to be configured, and enters interface configuration mode.
Step 8	**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id** [**override**] **string** *ASCII-string* **Example:** `Device(config-if)# ip dhcp snooping vlan 1 information option format-type circuit-id override string ovrride2`	(Optional) Configures 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 **vlan-mod-port**. • You can configure the circuit ID to be a string of 3 to 63 ASCII characters (no spaces). • (Optional) Use the **override** keyword when you do not want the circuit-ID suboption inserted in TLV format to define subscriber information.
Step 9	**ip dhcp snooping trust** **Example:** `Device(config-if)# ip dhcp snooping trust`	(Optional) Configures the interface as trusted or untrusted. Use the **no** keyword to configure an interface to receive messages from an untrusted client. The default setting is untrusted.

	Command or Action	Purpose
Step 10	**ip dhcp snooping limit rate** *rate* **Example:** `Device(config-if)# ip dhcp snooping limit rate 100`	(Optional) Configures 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. **Note** 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 with DHCP snooping.
Step 11	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 12	**ip dhcp snooping verify mac-address** **Example:** `Device(config)# ip dhcp snooping verify mac-address`	(Optional) Configures the device to verify that the source MAC address in a DHCP packet 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.
Step 13	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Monitoring DHCP Snooping Information

Table 2: Commands for Displaying DHCP Information

show ip dhcp snooping	Displays the DHCP snooping configuration for a device.
show ip dhcp snooping binding	Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.
show ip dhcp snooping database	Displays the DHCP snooping binding database status and statistics.
show ip dhcp snooping statistics	Displays the DHCP snooping statistics in summary or detail form.
show ip source binding	Display the dynamically and statically configured bindings.

Note If DHCP snooping is enabled and an interface changes to the down state, the device does not delete the statically configured bindings.

Enabling the Cisco IOS DHCP Server Database

For procedures to enable and configure the Cisco IOS DHCP server database, see the "DHCP Configuration Task List" section in the "Configuring DHCP" chapter of the Cisco IOS IP Configuration Guide, Release 12.4

Enabling the DHCP Snooping Binding Database Agent

Beginning in privileged EXEC mode, follow these steps to enable and configure the DHCP snooping binding database agent on the device:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp snooping database** {**flash**[*number*]**:**/*filename* | **ftp:**//*user***:***password***@***host*/*filename* | **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** | **rcp:**//*user***@***host*/*filename*}| **tftp:**//*host*/*filename* **Example:** `Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2`	Specifies the URL for the database agent or the binding file by using one of these forms: • **flash**[*number*]**:**/*filename* • **ftp:**//*user***:***password***@***host*/*filename* • **http:**//[[*username***:***password*]**@**]{*hostname* | *host-ip*}[/*directory*] /*image-name***.tar** • **rcp:**//*user***@***host*/*filename* • **tftp:**//*host*/*filename*
Step 4	**ip dhcp snooping database timeout** *seconds* **Example:** `Device(config)# ip dhcp snooping database timeout 300`	Specifies (in seconds) how long to wait for the database transfer process to finish before stopping the process. • The default is 300 seconds. The range is from 0 to 86400. Use 0 to define an infinite duration, which means to continue trying the transfer indefinitely.
Step 5	**ip dhcp snooping database write-delay** *seconds* **Example:** `Device(config)# ip dhcp snooping database write-delay 15`	Specifies the duration for which the transfer should be delayed after the binding database changes. • The default is 300 seconds (5 minutes). The range is from 15 to 86400 seconds.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id* **expiry** *seconds* **Example:** `Device# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gigabitethernet1/1 expiry 1000`	(Optional) Adds binding entries to the DHCP snooping binding database. • The *vlan-id* range is from 1 to 4904. The *seconds* range is from 1 to 4294967295. • Enter this command for each entry that you add. • Use this command when you are testing or debugging the device.
Step 8	**show ip dhcp snooping database** [**detail**] **Example:** `Device# show ip dhcp snooping database detail`	Displays the status and statistics of the DHCP snooping binding database agent.

Enabling DHCP Server Port-Based Address Allocation

Follow these steps to globally enable port-based address allocation and to automatically generate a subscriber identifier on an interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp use subscriber-id client-id** **Example:** `Device(config)# ip dhcp use subscriber-id client-id`	Configures the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.

	Command or Action	Purpose
Step 4	**ip dhcp subscriber-id interface-name** **Example:** `Device(config)# ip dhcp subscriber-id interface-name`	Automatically generates a subscriber identifier based on the short name of the interface. • A subscriber identifier configured on a specific interface takes precedence over this command.
Step 5	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet 0/1`	Specifies the interface to be configured, and enters interface configuration mode.
Step 6	**ip dhcp server use subscriber-id client-id** **Example:** `Device(config-if)# ip dhcp server use subscriber-id client-id`	Configures the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

What to do next

After enabling DHCP port-based address allocation on the device, use the **ip dhcp pool** global configuration command to preassign IP addresses and to associate them to clients.

Monitoring DHCP Server Port-Based Address Allocation

Table 3: Commands for Displaying DHCP Port-Based Address Allocation Information

Command	Purpose
show interface *interface id*	Displays the status and configuration of a specific interface.
show ip dhcp pool	Displays the DHCP address pools.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

Configuration Examples for DHCP

Example: Configuring the DHCP Relay Agent

This example shows how to configure the DHCP Relay Agent:

```
Device> enable
Device# configure terminal
```

```
Device(config)# service dhcp
Device(config)# end
```

Example: Specifying the Packet Forwarding Address

```
Device> enable
Device# configure terminal
Device(config)# interface vlan 1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip helper-address 172.16.1.2
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# end
```

Example: Enabling DHCP Snooping and Option 82

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping
Device(config)# ip dhcp snooping vlan 10
Device(config)# ip dhcp snooping information option
Device(config)# ip dhcp snooping information option format remote-id string acsiistring2
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ip dhcp snooping vlan 1 information option format-type
circuit-id override string ovrride2
Device(config-if)# ip dhcp snooping trust
Device(config-if)# ip dhcp snooping limit rate 100
Device(config-if)# exit
Device(config)# ip dhcp snooping verify mac-address
Device(config)# end
```

Example: Enabling the DHCP Snooping Binding Database Agent

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
Device(config)# ip dhcp snooping database timeout 300
Device(config)# ip dhcp snooping database write-delay 15
Device(config)# exit
Device# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5
interface gigabitethernet1/1 expiry 1000
```

Example: Enabling DHCP Server Port-Based Address Allocation

This example shows how to enable the DHCP server port-based address allocation:

```
Device> enable
Device# configure terminal
Device(config)# ip dhcp use subscriber-id client-id
Device(config)# ip dhcp subscriber-id interface-name
Device(config)# interface gigabitethernet 0/1
Device(config-if)# ip dhcp server use subscriber-id client-id
Device(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)E (Catalyst 2960-L Switches)

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for Configuring DHCP

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS Release 15.2(5)E	Configuring DHCP	DHCP server assigns IP addresses from specified address pools on a device to DHCP clients and manages them.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.