DHCP Features Configuration

This chapter describes how to configure the DHCP server port-based address allocation features on the Router.

Table 1: Feature History

Feature Name	Release	Description
DHCP Snooping	Cisco IOS XE Amsterdam 17.3.1	The Dynamic Host Configuration Protocol (DHCP) Snooping is a DHCP security feature that provides network securityby filtering untrusted DHCP messages and by building and maintaining a DHCP Snooping binding database, DHCP snooping acts like a firewall between untrusted hosts and DHCP servers.DHCP Snooping is used to differentiate untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another router. This feature is supported on the Cisco NCS 520 Router

Limitations and Restrictions on the Cisco NCS 520 Router

- DCHP over xconnect and local connect is supported.
- DHCP smart relay supports a maximum of 16 local addresses configured on a BDI or an interface.

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.

DHCP Server

The DHCP server assigns IP addresses from specified address pools on a switch or router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

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 egress interfaces.

DHCP relay is supported on these variants of the Cisco NCS 520 Series Ethernet Access Device:

- N520-4G4Z-A (Base)
- N520-X-4G4Z-A (Premium)
- N520-X-4G4Z-D (Premium)
- N520-20G4Z-A (Base)
- N520-20G4Z-D (Base)
- N520-X-20G4Z-A (Premium)
- N520-X-20G4Z-D (Premium)

Note DHCP option-82 is not supported, when the DHCP relay agent is enabled and by simultaneously disabling the DHCP snooping.

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. For more information about this database, see the Displaying DHCP Snooping Information, on page 15.

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 router 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 bridge-domain 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 bridge-domain 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 router 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.

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

Option-82 Data Insertion

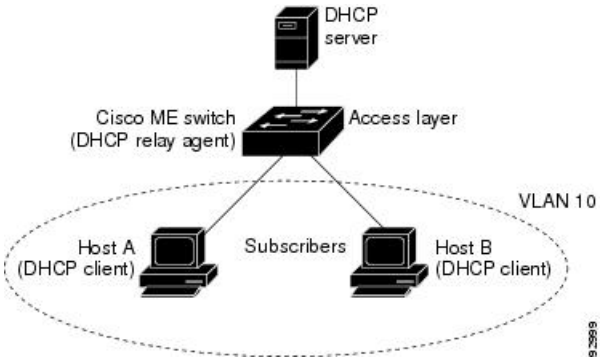
In residential, metropolitan Ethernet-access environments, DHCP can centrally manage the IP address assignments for a large number of subscribers. When the DHCP option-82 feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in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

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

Note DHCP Client will not receive the IP address if DHCP server is connected via relay and when snooping is globally enabled along with BDI IP configured for snooping enabled BD.

Figure below is an example of a metropolitan Ethernet network in which a centralized DHCP server assigns IP addresses to subscribers connected to the switch 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 Cisco Router) 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 switch, this sequence of events occurs:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- When the switch receives the DHCP request, it adds the option-82 information in the packet. By default, the remote-ID suboption is the switch MAC address, and the circuit-ID suboption is the port identifier from which the packet is received. You can also configure the remote ID and circuit ID. For information on configuring these suboptions, see the Enabling DHCP Snooping and Option 82, on page 12.
- If the IP address of the relay agent is configured, the switch adds this IP address in the DHCP packet.
- The switch 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 switch if the request was relayed to the server by the switch. The switch verifies that it originally inserted the option-82 data by inspecting the remote ID and possibly the circuit ID fields. The switch 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 in figure below do not change:

- 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 circuit ID type

Figure below 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 DHCP snooping is globally enabled and when the ip dhcp snooping information option global configuration command is entered.

Figure 2: Suboption Packet Formats

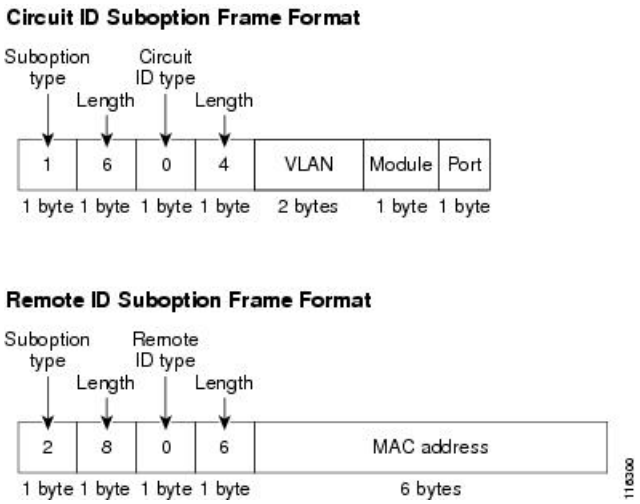


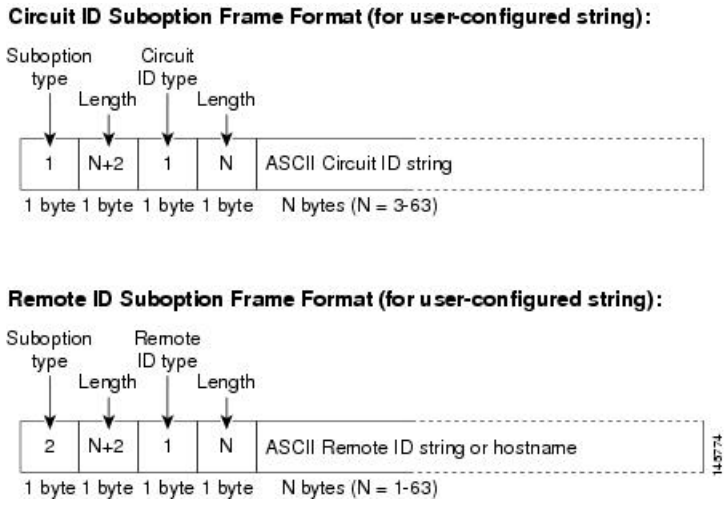
Figure below shows the packet formats for user-configured remote-ID and circuit-ID suboptions The switch uses these packet formats when you globally enable DHCP snooping and enter the ip dhcp snooping information option format remote-id global configuration command and the ip dhcp snooping bridge-domain information option format-type circuit-id string interface configuration command.

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



Note In scenarios where **no ip dhcp snooping information option** is configured (i.e when the server does not support DHCP information option) then use **ip dchp snooping track host** command. This is because the MAC to port mapping is only available in DHCP optoin 82. If the information options has been disabled then to know the MAC to port mapping **ip dhcp snooping track host** command must be enabled.

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. For more information about manual and automatic address bindings, see the IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S .

DHCP Snooping Binding Database

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 8192 bindings.

Note DHCP snooping database read event will **not** retrieve entries for 10G and PC interface

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 bridge-domain 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* value that accounts for 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 switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP inspection, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

When reloading, the router reads the binding file to build the DHCP snooping binding database. The switch keeps the file current by updating it when the database changes.

When a router learns of new bindings or when it loses bindings, the router immediately updates the entries in the database. The router 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 that has the 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 router 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 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
```

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

- The router 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 router 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.

Configuring DHCP Features

Default DHCP Configuration

Table below shows the default DHCP configuration.

Table 2: 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)[3]
DHCP relay agent forwarding policy	Replace the existing relay agent information[4]
DHCP snooping enabled globally	Disabled
DHCP snooping information option	Enabled
DHCP snooping option to accept packets on untrusted ingress interfaces[5]	Disabled
DHCP snooping limit rate	None configured
DHCP snooping trust	Untrusted
DHCP snooping bridge-domain	Disabled
DHCP snooping MAC address verification	Enabled

Feature	Default Setting
Cisco IOS DHCP server binding database	Enabled in Cisco IOS software, requires configuration. **Note** The router 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 router responds to DHCP requests only if it is configured as a DHCP server.
[2] The router relays DHCP packets only if the IP address of the DHCP server is configured on the BDI of the DHCP client.
[3] The router relays DHCP packets only if the IP address of the DHCP server is configured on the BDI of the DHCP client.
[4] The router relays DHCP packets only if the IP address of the DHCP server is configured on the BDI of the DHCP client.
[5] Use this feature when the router is an aggregation switch that receives packets with option-82 information from an edge switch.

DHCP Snooping Configuration Guidelines

- You must globally enable DHCP snooping on the router.
- DHCP snooping is not active until DHCP snooping is enabled on a bridge-domain.
- Before globally enabling DHCP snooping on the router, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- Before configuring the DHCP snooping information option on your router, be sure to configure the device that is acting as the DHCP server. For example, you must specify the IP addresses that the DHCP server can assign or exclude, or you must configure DHCP options for these devices.
- When configuring a large number of circuit IDs on a router, 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.
- Before configuring the DHCP relay agent on your router, make sure to configure the device that is acting as the DHCP server. For example, 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.
- If the DHCP relay agent is enabled but DHCP snooping is disabled, the DHCP option-82 data insertion feature is not supported.
- 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.

Follow these guidelines when configuring the DHCP snooping binding database:

- 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 router 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 NTP is enabled and configured.
- If NTP is configured, the router writes binding changes to the binding file only when the router system clock is synchronized with NTP.
- Do not enter the ip dhcp snooping information option allowed-untrusted command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

```
Router# show ip dhcp snooping binding

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface

------------------  ---------------  ----------  -------------  ----  --------------------


AA:00:11:13:00:01   40.0.0.2         117         dhcp-snooping  100   Port-channel100+Efp7
```

Configuring the DHCP Server

The router can act as a DHCP server. By default, the Cisco IOS DHCP server and relay agent features are enabled on your router but are not configured. These features are not operational.

For procedures to configure the router as a DHCP server, see the IP Addressing Configuration Guide Library, Cisco IOS XE Release 3S.

Configuring the DHCP Relay Agent

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**service dhcp**	Enable the DHCP relay agent on your router. By default, this feature is enabled.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To disable the DHCP relay agent, use the **no service dhcp** global configuration command.

Specifying the Packet Forwarding Address

If the DHCP server and the DHCP clients are on different networks or subnets and the router is running the metro IP access image, you must configure the router 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.

Note To remove the DHCP packet forwarding address, use the **no ip helper-address***address* interface configuration command.

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface bridge-domain id**	Create a switch virtual interface by entering a bridge-domain ID, and enter interface configuration mode.
Step 3	**ip address ip-address subnet-mask**	Configure the interface with an IP address and an IP subnet.
Step 4	**ip helper-address address**	Specify 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 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enabling DHCP Snooping and Option 82

Beginning in the privileged EXEC mode, follow these steps to enable DHCP snooping on the switch:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp snooping**	Enable DHCP snooping globally.
Step 3	**ip dhcp snooping bridge-domain id**	Enable DHCP snooping on a bridge-domain
Step 4	**ip dhcp snooping information option**	Enable the router 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 5	**ip dhcp snooping information option format remote-id [string ASCII-string | hostname]**	(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 router **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 router MAC address.
Step 6	**ip dhcp snooping information option allowed-untrusted**	(Optional) If the router is acting as an aggregation switch connected to an edge switch, enable the router to accept incoming DHCP snooping packets with option-82 information from the edge switch. The default is disabled. **Note** Enter this command only on aggregation switches that are connected to trusted devices.
Step 7	**interface interface-id**	Specify the interface to be configured, and enter interface configuration mode.
Step 8	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled.
Step 9	**ip dhcp snooping trust**	Configure the interface as trusted or untrusted. You can use the **no** keyword to configure an

	Command or Action	Purpose
		interface to receive messages from an untrusted client. The default is untrusted.
Step 10	**ip dhcp snooping limit rate rate**	(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. **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 bridge-domain on which DHCP snooping is enabled.
Step 11	**exit**	Return to global configuration mode.
Step 12	**ip dhcp snooping verify mac-address**	(Optional) Configure the router 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.
Step 13	**end**	Return to privileged EXEC mode.
Step 14	**show running-config**	Verify your entries.
Step 15	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enabling the Cisco IOS DHCP Server Database

For procedures to enable and configure the Cisco IOS DHCP server database, see the *IP Addressing: DHCP Configuration Guide*.

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 router:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command or Action	Purpose
Step 2	**ip dhcp snooping database {flash:/filename | ftp://user:password@host/filename | http://[[username:password]@]{hostname | host-ip}[/directory] /image-name.tar | rcp://user@host/filename}| tftp://host/filename**	Specify the URL for the database agent or the binding file by using one of these forms: • **flash:**/*filename* • **ftp:**//*user:password@host/filename* • **http:**//[[*username:password]@]{hostname | host-ip}[/directory]/image-name***.tar*** • **rcp:**//*user@host/filename* • **tftp:**//*host/filename*
Step 3	**ip dhcp snooping database timeout seconds**	Specify when to stop the database transfer process after the binding database changes. The range is from 0 to 86400. Use 0 for an infinite duration. The default is 300 seconds (5 minutes).
Step 4	**ip dhcp snooping database write-delay seconds**	Specify the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**ip dhcp snooping binding [ip-address | mac-address | dynamic | static | bridge-domain id | interface interface]**	(Optional) Add binding entries to the DHCP snooping binding database. The *seconds* range is from 1 to 4294967295. Enter this command for each entry that you add. **Note** Use this command when you are testing or debugging the router.
Step 7	**show ip dhcp snooping database [detail]**	Display the status and statistics of the DHCP snooping binding database agent.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Stopping the Database Agent and Binding files

To stop using the database agent and binding files, use the no ip dhcp snooping database global configuration command.To reset the timeout or delay values, use the ip dhcp snooping database timeout seconds or the ip dhcp snooping database write-delay seconds global configuration command.

Clearing the Statistics of the DHCP Snooping Binding Database Agent

To clear the statistics of the DHCP snooping binding database agent, use the clear ip dhcp snooping database statistics privileged EXEC command. To renew the database, use the renew ip dhcp snooping database privileged EXEC command.

Deleting Binding Entries from the DHCP Snooping Binding Database

To delete binding entries from the DHCP snooping binding database, use the no ip dhcp snooping binding mac-address bridge-domain id ip-address interface interface-id privileged EXEC command. Enter this command for each entry that you delete.

Disabling DHCP Snooping

To disable DHCP snooping, use the **no ip dhcp snooping** global configurationcommand.

To disable DHCP snooping on a bridge-domain, use the **no ip dhcp snooping bridge-domain** *id* global configuration command.

To disable the insertion and removal of the option-82 field, use the **no ip dhcp snooping information option global** configuration command.

To configure an aggregation switch to drop incoming DHCP snooping packets with option-82 information from an edge switch, use the **no ip dhcp snooping information option allowed-untrusted** global configuration command.

Displaying DHCP Snooping Information

To display the DHCP snooping information, use one or more of the privileged EXEC commands as shown in below table:

Table 3: Commands for Displaying DHCP Information

Command	Purpose
show ip dhcp snooping	Displays the DHCP snooping configuration
show ip dhcp snooping binding*[ip-address* | *mac-address* | **dynamic | static | bridge-domain** *id* **| interface***interface]*	Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table.[6]
show ip dhcp snooping database	Displays the DHCP snooping binding database status and statistics.

[6] If DHCP snooping is enabled and an interface changes to the down state, the router does not delete the manually configured bindings.

Pre-assigned Address Reserved in the DHCP Pool

This example shows that the preassigned address was correctly reserved in the DHCP pool:

```
Router# show ip dhcp pool dhcppool
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
```

Automatic Generation of Subscriber Identifier

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.

```
Router# show running config
Building configuration...
Current configuration : 4899 bytes
!
hostname router
!
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#
```

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 switches 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 DH CP 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.

Configuring DHCP Server Port-Based Address Allocation

Before you begin

Default Port-Based Address Allocation Configuration

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

Port-Based Address Allocation Configuration Guidelines

These are the configuration guidelines for DH CP port-based address allocation:

- 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.
- 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.

Enabling DHCP Server Port-Based Address Allocation

Beginning in privileged EXEC mode, 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	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp use subscriber-id client-id**	Configure the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.
Step 3	**ip dhcp subscriber-id interface-name**	Automatically generate 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 4	**interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.

	Command or Action	Purpose
Step 5	**ip dhcp server use subscriber-id client-id**	Configure the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Pre-assigning IP Addresses

After enabling DHCP port-based address allocation on the router, use the ip dhcp pool global configuration command to preassign IP addresses and to associate them to clients. To restrict assignments from the DHCP pool to preconfigured reservations, you can enter the reserved-only DHCP pool configuration command. Unreserved addresses that are part of the network or on pool ranges are not offered to the client, and other clients are not served by the pool. By entering this command, users can configure a group of switches with DHCP pools that share a common IP subnet and that ignore requests from clients of other switches.

Beginning in privileged EXEC mode follow these steps to preassign an IP address and to associate it to a client identified by the interface name.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp use subscriber-id client-id**	Configure the DHCP server to globally use the subscriber identifier as the client identifier on all incoming DHCP messages.
Step 3	**ip dhcp subscriber-id interface-name**	Automatically generate 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 4	**interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.
Step 5	**ip dhcp server use subscriber-id client-id**	Configure the DHCP server to use the subscriber identifier as the client identifier on all incoming DHCP messages on the interface.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Removing an IP Address Reservation from a DHCP Pool

To remove an IP address reservation from a DHCP pool, use the no address ip-address client-id string DHCP pool configuration command. To change the address pool to nonrestricted, enter the no reserved-only DHCP pool configuration command.

Automatic Generation of Subscriber Identifier

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.

```
Router# show running config
Building configuration...
Current configuration : 4899 bytes
!
hostname router
!
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#
```

Disabling DHCP Port-Based Address Allocation

To disable DHCP port-based address allocation, use the no ip dhcp use subscriber-id client-id global configuration command. To disable the automatic generation of a subscriber identifier, use the no ip dhcp subscriber-id interface-name global configuration command. To disable the subscriber identifier on an interface, use the no ip dhcp server use subscriber-id client-id interface configuration command.

Displaying DHCP Server Port-Based Address Allocation

To display the DHCP server port-based address allocation information, use one or more of the privileged EXEC commands as shown in table below:

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

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