



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 Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches. This chapter 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 documents listed in the [“Related Documents”](#) section on page 5-25.

- [Information About DHCP Features](#), page 5-1
- [Information About DHCP Server Port-Based Address Allocation](#), page 5-7
- [Information About IP Source Guard](#), page 5-8
- [Prerequisites](#), page 5-10
- [Guidelines and Limitations](#), page 5-10
- [Default Settings](#), page 5-13
- [Configuring DHCP Features](#), page 5-14
- [Configuring DHCP Server Port-Based Address Allocation](#), page 5-20
- [Configuring IP Source Guard](#), page 5-23
- [Verifying Configuration](#), page 5-24
- [Related Documents](#), page 5-25
- [Feature History](#), page 5-25

Information About 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](#), page 5-2
- [DHCP Relay Agent](#), page 5-2
- [DHCP Snooping](#), page 5-2
- [Option-82 Data Insertion](#), page 5-3

- [Cisco IOS DHCP Server Database, page 5-6](#)
- [DHCP Snooping Binding Database, page 5-6](#)

**Tip**

For information about the DHCP client, see [“Related Documents” section on page 5-25](#).

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 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 [“Configuring DHCP Server Port-Based Address Allocation” section on page 5-20](#).

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 DHCP OFFER, DHCP ACK, DHCP NAK, or DHCP LEASE QUERY 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 DHCP RELEASE or DHCP DECLINE 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 or IP source guard, 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.

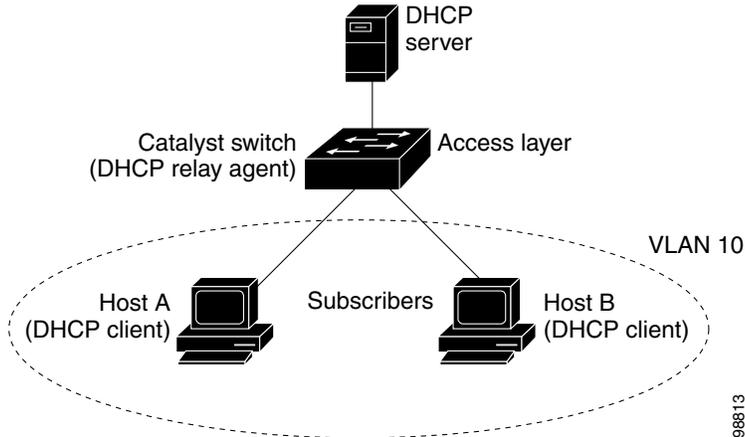


Note

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

Figure 5-1 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 Catalyst switch) is configured with a helper address to enable broadcast forwarding and to transfer DHCP messages between the clients and the server.

Figure 5-1 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, **vlan-mod-port**, 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”](#) section on page 5-16.
- 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 5-2](#) do not change:

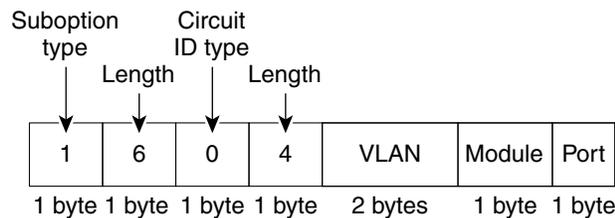
- Circuit ID suboption fields
 - Suboption type
 - Length of the suboption type
 - Circuit ID type
 - Length of the circuit ID type
- Remote ID suboption fields
 - Suboption type
 - Length of the suboption type
 - Remote ID type
 - Length of the circuit ID type

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

Figure 5-2 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 DHCP snooping is globally enabled and when the **ip dhcp snooping information option** global configuration command is entered.

Figure 5-2 Suboption Packet Formats

Circuit ID Suboption Frame Format



Remote ID Suboption Frame Format

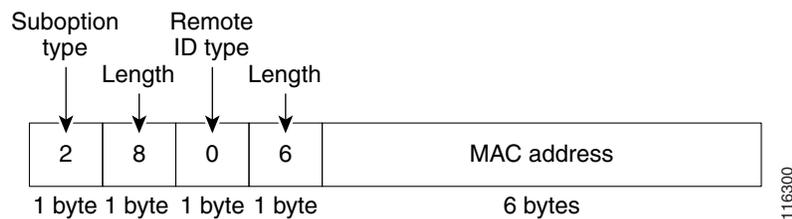
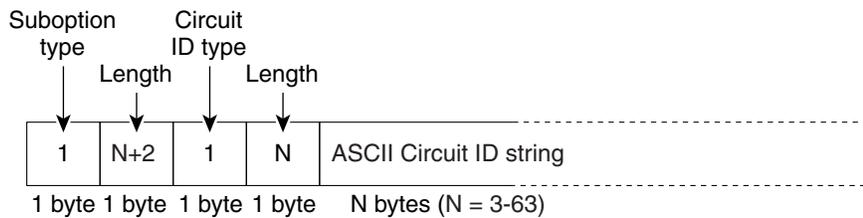
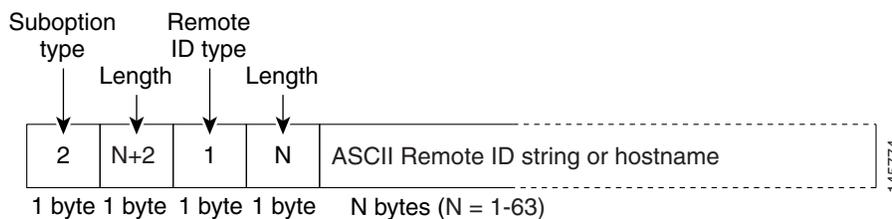


Figure 5-3 shows the packet formats for user-configured remote ID and circuit ID suboptions. The switch uses these packet formats when you globally enable DHCP snooping and enter the **ip dhcp snooping information option format remote-id** global configuration command and the **ip dhcp snooping vlan 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 5-3 User-Configured Suboption Packet Formats**Circuit ID Suboption Frame Format (for user-configured string):****Remote ID Suboption Frame Format (for user-configured string):**

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 [“Related Documents”](#) section on page 5-25.

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.

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* 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 or IP source guard is enabled, 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 switch 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 switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch 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 switch 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 switch starts and the calculated checksum value equals the stored checksum value, the switch reads entries from the binding file and adds the bindings to its DHCP snooping binding database. The switch ignores an entry when one of these situations occurs:

- The switch 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 switch 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.

Information About 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 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.

Information About IP Source Guard

IPSG is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor.

You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.



Note

The port ACL takes precedence over any VLAN maps that affect the same interface.

The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

IP source guard is supported only on Layer 2 ports, including access and trunk ports. You can configure IP source guard with source IP address filtering or with source IP and MAC address filtering.

This section includes the following topics:

- [Source IP Address Filtering, page 5-8](#)
- [Source IP and MAC Address Filtering, page 5-9](#)
- [IP Source Guard for Static Hosts, page 5-9](#)

Source IP Address Filtering

When IP source guard is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table.

When a DHCP snooping binding or static IP source binding is added, changed, or deleted on an interface, the switch modifies the port ACL using the IP source binding changes, and re-applies the port ACL to the interface.

If you enable IP source guard on an interface on which IP source bindings are not configured (dynamically learned by DHCP snooping or manually configured), the switch creates and applies a port ACL that denies all IP traffic on the interface. If you disable IP source guard, the switch removes the port ACL from the interface.

Source IP and MAC Address Filtering

When IP source guard is enabled with this option, IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table.

When IP source guard with source IP and MAC address filtering is enabled, the switch filters IP and non-IP traffic. If the source MAC address of an IP or non-IP packet matches a valid IP source binding, the switch forwards the packet. The switch drops all other types of packets except DHCP packets.

The switch uses port security to filter source MAC addresses. The interface can shut down when a port-security violation occurs.

IP Source Guard for Static Hosts



Note

Do not use IPSG (IP source guard) for static hosts on uplink ports or trunk ports.

IPSG for static hosts extends the IPSG capability to non-DHCP and static environments. The previous IPSG used the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without a valid DHCP binding entry is dropped. This security feature restricts IP traffic on nonrouted Layer 2 interfaces. It filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings. The previous version of IPSG required a DHCP environment for IPSG to work.

IPSG for static hosts allows IPSG to work without DHCP. IPSG for static hosts relies on IP device tracking-table entries to install port ACLs. The switch creates static entries based on ARP requests or other IP packets to maintain the list of valid hosts for a given port. You can also specify the number of hosts allowed to send traffic to a given port. This is equivalent to port security at Layer 3.

IPSG for static hosts also supports dynamic hosts. If a dynamic host receives a DHCP-assigned IP address that is available in the IP DHCP snooping table, the same entry is learned by the IP device tracking table. When you enter the **show ip device tracking all EXEC** command, the IP device tracking table displays the entries as ACTIVE.



Note

Some IP hosts with multiple network interfaces can inject some invalid packets into a network interface. The invalid packets contain the IP or MAC address for another network interface of the host as the source address. The invalid packets can cause IPSG for static hosts to connect to the host, to learn the invalid IP or MAC address bindings, and to reject the valid bindings. Consult the vendor of the corresponding operating system and the network interface to prevent the host from injecting invalid packets.

IPSG for static hosts initially learns IP or MAC bindings dynamically through an ACL-based snooping mechanism. IP or MAC bindings are learned from static hosts by ARP and IP packets. They are stored in the device tracking database. When the number of IP addresses that have been dynamically learned or statically configured on a given port reaches a maximum, the hardware drops any packet with a new IP

address. To resolve hosts that have moved or gone away for any reason, IPSPG for static hosts leverages IP device tracking to age out dynamically learned IP address bindings. This feature can be used with DHCP snooping. Multiple bindings are established on a port that is connected to both DHCP and static hosts. For example, bindings are stored in both the device tracking database as well as in the DHCP snooping binding database.

Prerequisites

DHCP Server

- Before you configure DHCP features and IP source guard, you must understand the concepts documented in the [“Information About DHCP Features”](#) section on page 5-1, [“Information About DHCP Server Port-Based Address Allocation”](#) section on page 5-7, and [“Information About IP Source Guard”](#) section on page 5-8.
- The Cisco DHCP server and the relay agent are enabled by default. Use the **no service dhcp** command to disable the Cisco DHCP server and the relay agent and the **service dhcp** command to reenables the functionality.
- Port 67 (the DHCP server port) is closed in the Cisco DHCP/BOOTP default configuration. There are two logical parts to the **service dhcp** command: service enabled and service running. The DHCP service is enabled by default, but port 67 does not open until the DHCP service is running. If the DHCP service is running, the **show ip sockets details** or the **show sockets detail** command displays port 67 as open.

DHCP Relay Agent

- You must enable the Cisco DHCP relay agent on an interface by using the **ip helper-address** command. This command enables a DHCP broadcast to be forwarded to the configured DHCP server.

Guidelines and Limitations

- [DHCP Snooping, page 5-10](#)
- [Port-Based Address Allocation, page 5-11](#)
- [IP Source Guard, page 5-12](#)

DHCP Snooping

These are the configuration guidelines for DHCP snooping:

- You must globally enable DHCP snooping on the switch.
- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- When you globally enable DHCP snooping on the switch, these Cisco IOS commands are not available until snooping is disabled. If you enter these commands, the switch returns an error message, and the configuration is not applied.
 - **ip dhcp relay information check** global configuration command

- **ip dhcp relay information policy** global configuration command
- **ip dhcp relay information trust-all** global configuration command
- **ip dhcp relay information trusted** interface configuration command
- Before configuring the DHCP snooping information option on your switch, 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 switch, 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 switch, 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 the 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 switch 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 be enabled and configured. For more information, see the “Administering the Switch” chapter in the *System Management Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches*.
 - If NTP is configured, the switch writes binding changes to the binding file only when the switch 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.
- You can display DHCP snooping statistics by entering the **show ip dhcp snooping statistics** user EXEC command, and you can clear the snooping statistics counters by entering the **clear ip dhcp snooping statistics** privileged EXEC command.

**Note**

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.

Port-Based Address Allocation

These are the configuration guidelines for DHCP 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.

IP Source Guard

These are the configuration guidelines for IP source guard:

- You can configure static IP bindings only on nonrouted ports. If you enter the **ip source binding mac-address vlan vlan-id ip-address interface interface-id** global configuration command on a routed interface, this error message appears:

```
Static IP source binding can only be configured on switch port.
```
- When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN to which the interface belongs.
- If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.



Note If IP source guard is enabled and you enable or disable DHCP snooping on a VLAN on the trunk interface, the switch might not properly filter traffic.

- If you enable IP source guard with source IP and MAC address filtering, DHCP snooping and port security must be enabled on the interface. You must also enter the **ip dhcp snooping information option** global configuration command and ensure that the DHCP server supports option 82. When IP source guard is enabled with MAC address filtering, the DHCP host MAC address is not learned until the host is granted a lease. When forwarding packets from the server to the host, DHCP snooping uses option-82 data to identify the host port.
- When configuring IP source guard on interfaces on which a private VLAN is configured, port security is not supported.
- IP source guard is not supported on EtherChannels.
- You can enable this feature when IEEE 802.1x port-based authentication is enabled.
- If the number of ternary content addressable memory (TCAM) entries exceeds the maximum available, the CPU usage increases.

Default Settings

Feature	Default Setting
DHCP server	Enabled in Cisco IOS software; requires configuration. Note The switch responds to DHCP requests only if it is configured as a DHCP server.
DHCP relay agent	Enabled. Note The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
DHCP packet forwarding address	None configured.
Checking the relay agent information	Enabled (invalid messages are dropped). Note The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
DHCP relay agent forwarding policy	Replace the existing relay agent information. Note The switch relays DHCP packets only if the IP address of the DHCP server is configured on the SVI of the DHCP client.
DHCP snooping enabled globally	Disabled.
DHCP snooping information option	Enabled.
DHCP snooping option to accept packets on untrusted ingress interfaces	Disabled. Note Use this feature when the switch is an aggregation switch that receives packets with option-82 information from an edge switch.
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.
DHCP snooping binding database agent	Enabled in Cisco IOS software; requires configuration. This feature is operational only when a destination is configured.
DHCP server port-based address allocation	Disabled.
IP source guard	Disabled.

Configuring DHCP Features

- [Configuring the DHCP Server, page 5-14](#)
- [Configuring the DHCP Relay Agent, page 5-14](#)
- [Specifying the Packet Forwarding Address, page 5-15](#)
- [Enabling DHCP Snooping and Option 82, page 5-16](#)
- [Enabling DHCP Snooping on Private VLANs, page 5-18](#)
- [Enabling the Cisco IOS DHCP Server Database, page 5-18](#)
- [Enabling the DHCP Snooping Binding Database Agent, page 5-18](#)

Configuring the DHCP Server

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

For procedures to configure the switch as a DHCP server, see the [“Related Documents” section on page 5-25](#).

Configuring the DHCP Relay Agent

BEFORE YOU BEGIN

Review the [Guidelines and Limitations](#) for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	service dhcp	Enable the DHCP relay agent on your switch. 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.

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

EXAMPLE

The following example shows to enable DHCP services on the DHCP server:

```
Switch(config)# service dhcp
```

Specifying the Packet Forwarding Address

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

BEFORE YOU BEGIN

Review the [Guidelines and Limitations](#) for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface vlan <i>vlan-id</i>	Create a switch virtual interface by entering a VLAN ID, and enter interface configuration mode.
Step 3	ip address <i>ip-address subnet-mask</i>	Configure the interface with an IP address and an IP subnet.
Step 4	ip helper-address <i>address</i>	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	exit	Return to global configuration mode.
Step 6	interface range <i>port-range</i> or interface <i>interface-id</i>	Configure multiple physical ports that are connected to the DHCP clients, and enter interface range configuration mode. or Configure a single physical port that is connected to the DHCP client, and enter interface configuration mode.
Step 7	no shutdown	Enable the interface(s), if necessary. By default, user network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled and network node interfaces (NNIs) are enabled.
Step 8	switchport mode access	Define the VLAN membership mode for the port.
Step 9	switchport access vlan <i>vlan-id</i>	Assign the ports to the same VLAN as configured in Step 2.
Step 10	end	Return to privileged EXEC mode.
Step 11	show running-config	Verify your entries.
Step 12	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

EXAMPLE

```
Switch(config)# interface vlan 10
Switch(config-if)# ip address 10.108.1.27 255.255.255.0
Switch(config-if)# ip helper-address 10.24.43.2
Switch(config-if)# exit
Switch(config)# interface range gigabitethernet 1/1 - 6
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# end
```

Enabling DHCP Snooping and Option 82

BEFORE YOU BEGIN

Review the [Guidelines and Limitations](#) for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp snooping	Enable DHCP snooping globally.
Step 3	ip dhcp snooping vlan <i>vlan-range</i>	Enable DHCP snooping on a VLAN or range of VLANs. The range is 1 to 4094. 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 4	ip dhcp snooping information option	Enable the switch 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 [<i>string ASCII-string</i> <i>hostname</i>]	(Optional) Configure the remote-ID suboption. You can configure the remote ID to be: <ul style="list-style-type: none"> String of up to 63 ASCII characters (no spaces) Configured hostname for the switch <p>Note If the hostname is longer than 63 characters, it is truncated to 63 characters in the remote-ID configuration.</p> <p>The default remote ID is the switch MAC address.</p>

	Command	Purpose
Step 6	ip dhcp snooping information option allowed-untrusted	(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 is disabled. Note You must enter this command only on aggregation switches that are connected to trusted devices.
Step 7	interface <i>interface-id</i>	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 vlan <i>vlan</i> information option format-type circuit-id string [override] <i>ASCII-string</i>	(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 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 10	ip dhcp snooping trust	(Optional) Configure the interface as trusted or untrusted. You can use the no keyword to configure an interface to receive messages from an untrusted client. The default is untrusted.
Step 11	ip dhcp snooping limit rate <i>rate</i>	(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 VLAN on which DHCP snooping is enabled.
Step 12	exit	Return to global configuration mode.
Step 13	ip dhcp snooping verify mac-address	(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.
Step 14	end	Return to privileged EXEC mode.
Step 15	show running-config	Verify your entries.
Step 16	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable DHCP snooping, use the **no ip dhcp snooping** global configuration command. To disable DHCP snooping on a VLAN or range of VLANs, use the **no ip dhcp snooping vlan *vlan-range*** 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.

EXAMPLE

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

Enabling DHCP Snooping on Private VLANs

You can enable DHCP snooping on private VLANs. If DHCP snooping is enabled, the configuration is propagated to both a primary VLAN and its associated secondary VLANs. If DHCP snooping is enabled on the primary VLAN, it is also configured on the secondary VLANs.

If DHCP snooping is already configured on the primary VLAN and you configure DHCP snooping with different settings on a secondary VLAN, the configuration for the secondary VLAN does not take effect. You must configure DHCP snooping on the primary VLAN. If DHCP snooping is not configured on the primary VLAN, this message appears when you are configuring DHCP snooping on the secondary VLAN, such as VLAN 200:

```
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.
```

The **show ip dhcp snooping** privileged EXEC command output shows all VLANs, including primary and secondary private VLANs, on which DHCP snooping is enabled.

Enabling the Cisco IOS DHCP Server Database

For procedures, refer to the [“Related Documents” section on page 5-25](#).

Enabling the DHCP Snooping Binding Database Agent

BEFORE YOU BEGIN

You must enable DHCP snooping on the interface before entering this command as described in the [“Enabling DHCP Snooping and Option 82” procedure on page 5-16](#).

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp snooping database { flash://filename ftp://user:password@host/filename http://[[username:password]@]{hostname me \ 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: <ul style="list-style-type: none"> • 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 <i>seconds</i>	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 <i>seconds</i>	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 <i>mac-address</i> vlan <i>vlan-id</i> ip-address interface <i>interface-id</i> expiry <i>seconds</i>	(Optional) Add binding entries to the DHCP snooping binding database. The <i>vlan-id</i> range is from 1 to 4904. The <i>seconds</i> 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 switch.
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.

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.

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.

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

EXAMPLE

This example shows how to specify the database URL using TFTP:

```
Switch(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Switch(config)# ip dhcp snooping database write-delay 15
```

Configuring DHCP Server Port-Based Address Allocation

- [Enabling Port-Based Address Allocation, page 5-20](#)
- [Preassigning an IP Address and Associating it to a Client, page 5-21](#)

Enabling Port-Based Address Allocation

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

BEFORE YOU BEGIN

Review the [Guidelines and Limitations](#) for this feature.

DETAILED STEPS

	Command	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.

EXAMPLE

In the following example, the DHCP server will ignore any client identifier fields in the DHCP messages and use the subscriber ID as the client identifier. The DHCP server uses the subscriber identifier as the client identifier for all incoming messages received on Ethernet interface 0/0.

```
Switch(config)# ip dhcp use subscriber-id client-id
Switch(config)# ip dhcp subscriber-id interface-name
Switch(config)# interface Ethernet 0/0
Switch(config-if)# ip dhcp server use subscriber-id client-id
Switch(config)# end
```

Preassigning an IP Address and Associating it to a Client

After enabling DHCP port-based address allocation on the switch, 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.

BEFORE YOU BEGIN

Review the “[Guidelines and Limitations](#)” section on page 5-10 for port-based address allocation configuration guidelines.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	ip dhcp pool <i>poolname</i>	Enter DHCP pool configuration mode, and define the name for the DHCP pool. The pool name can be a symbolic string (such as Engineering) or an integer (such as 0).
Step 3	network <i>network-number</i> [<i>mask</i> <i>/prefix-length</i>]	Specify the subnet network number and mask of the DHCP address pool.
Step 4	address <i>ip-address</i> client-id <i>string</i> [<i>ascii</i>]	Reserve an IP address for a DHCP client identified by the interface name. <i>string</i> —can be an ASCII value or a hexadecimal value.
Step 5	reserved-only	(Optional) Use only reserved addresses in the DHCP address pool. The default is to not restrict pool addresses.
Step 6	end	Return to privileged EXEC mode.
Step 7	show ip dhcp pool	Verify DHCP pool configuration.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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. 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.

EXAMPLE

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.

```
IE-2000U-4T# show running config

Building configuration...

Current configuration : 3018 bytes
!
! Last configuration change at 02:55:14 UTC Mon Sept 1 2013
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IE-2000U-4T
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1998
ip routing
no ip domain-lookup
ip name-server 69.78.134.231
!
ip dhcp relay information policy keep
ip dhcp relay information trust-all
!
ip dhcp pool test1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 69.78.134.231

<output truncated>
```

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

```
IE-2000U-4T# show ip dhcp pool dhcppool

Pool test1 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                 : 1
Excluded addresses               : 0
```

```

Pending event                : none
1 subnet is currently in the pool :
Current index      IP address range      Leased/Excluded/Total
192.168.10.4      192.168.10.1 - 192.168.10.254    1 / 0 / 254

```

Configuring IP Source Guard

Default IP Source Guard Configuration

By default, IP source guard is disabled.

BEFORE YOU BEGIN

Review the [Guidelines and Limitations](#) for this feature.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Specify the interface to be configured, and enter interface configuration mode.
Step 3	no shutdown	Enable the port, if necessary. By default, UNIs and ENIs are disabled and NNIs are enabled.
Step 4	ip verify source or ip verify source port-security	<p>Enable IP source guard with source IP address filtering.</p> <p>Enable IP source guard with source IP and MAC address filtering.</p> <p>Note When you enable both IP Source Guard and Port Security by using the ip verify source port-security interface configuration command, there are two caveats:</p> <ul style="list-style-type: none"> • The DHCP server must support option 82, or the client is not assigned an IP address. • The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.
Step 5	exit	Return to global configuration mode.
Step 6	ip source binding <i>mac-address</i> vlan <i>vlan-id</i> <i>ip-address</i> interface <i>interface-id</i>	<p>Add a static IP source binding.</p> <p>Enter this command for each static binding.</p>
Step 7	end	Return to privileged EXEC mode.

	Command	Purpose
Step 8	show ip verify source [<i>interface interface-id</i>]	Display the IP source guard configuration for all interfaces or for a specific interface.
Step 9	show ip source binding [<i>ip-address</i>] [<i>mac-address</i>] [dhcp-snooping static] [<i>interface interface-id</i>] [vlan <i>vlan-id</i>]	Display the IP source bindings on the switch, on a specific VLAN, or on a specific interface.
Step 10	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable IP source guard with source IP address filtering, use the **no ip verify source** interface configuration command.

To delete a static IP source binding entry, use the **no ip source** global configuration command.

EXAMPLE

This example shows how to enable IP source guard with source IP and MAC filtering on VLANs 10 and 11:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source port-security
Switch(config-if)# exit
Switch(config)# ip source binding 0100.0022.0010 vlan 10 10.0.0.2 interface
gigabitethernet0/1
Switch(config)# ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet0/1
Switch(config)# end
```

Verifying Configuration

Command	Purpose
DHCP Snooping	
show ip dhcp snooping	Displays the DHCP snooping configuration for a switch
show ip dhcp snooping binding	Displays only the dynamically configured bindings in the DHCP snooping binding database, also referred to as a binding table. Note If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the manually configured bindings.
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.
DHCP Server Port-Based Address Allocation	
show interface <i>interface id</i>	Display the status and configuration of a specific interface.
show ip dhcp pool	Display the DHCP address pools.

Command	Purpose
show ip dhcp binding	Display address bindings on the Cisco IOS DHCP server.
IP Source Guard	
show ip source binding	Display the IP source bindings on a switch.
show ip verify source	Display the IP source guard configuration on the switch.

Related Documents

- [Cisco IOS Master Command List, All Releases](#)
- [Cisco IOS IP Addressing Services Command Reference](#)
- [IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15M&T](#)

You can find the following information in the above referenced guide:

- DHCP clients
- Manual and automatic address bindings
- Configuring the switch as a DHCP server
- Enabling and configuring the DHCP server database
- Validating the DHCP relay agent information and configuring the relay agent forwarding policy

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

