# IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 2

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# CONTENTS

# DHCP Overview

The Dynamic Host Configuration Protocol (DHCP) is based on the Bootstrap Protocol (BOOTP), which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the capability to automatically allocate reusable network addresses and configuration options to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

This module describes the concepts needed to understand Cisco IOS XE DHCP.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About DHCP

# DHCP Overview

Cisco routers running Cisco IOS XE software include DHCP server and relay agent software. The Cisco IOS XE DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. These address pools can also be configured to supply additional information to the requesting client such as the IP address of the DNS server, the default router, and other configuration parameters. If the Cisco IOS XE DHCP server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

DHCP supports three mechanisms for IP address allocation:

- Automatic allocation--DHCP assigns a permanent IP address to a client.
- Dynamic allocation--DHCP assigns an IP address to a client for a limited period of time, which is called a lease (or until the client explicitly relinquishes the address). DHCP also supports on-demand address pools (ODAPs), which is a feature in which pools of IP addresses can be dynamically increased or reduced in size depending on the address utilization level. ODAPs support address assignment for customers using private addresses.
- Manual allocation--The network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client.

The format of DHCP messages is based on the format of BOOTP messages, which ensures support for BOOTP relay agent functionality and interoperability between BOOTP clients and DHCP servers. BOOTP relay agents eliminate the need for deploying a DHCP server on each physical network segment. BOOTP is explained in RFC 951, *Bootstrap Protocol (BOOTP)* , and RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol* .

The main advantage of DHCP compared to BOOTP is that DHCP does not require that the DHCP server be configured with all MAC addresses of all clients. DHCP defines a process by which the DHCP server knows the IP subnet in which the DHCP client resides, and it can assign an IP address from a pool of valid IP addresses in that subnet. Most of the other information that DHCP might supply, such as the default router IP address, is the same for all hosts in the subnet so DHCP servers can usually configure information per subnet rather than per host. This functionality reduces network administration tasks compared to BOOTP.

# Benefits of Using Cisco IOS XE DHCP

The Cisco IOS XE DHCP implementation offers the following benefits:

- Reduced Internet access costs

Using automatic IP address assignment at each remote site substantially reduces Internet access costs. Static IP addresses are considerably more expensive to purchase than are automatically allocated IP addresses.

- Reduced client configuration tasks and costs

Because DHCP is easy to configure, it minimizes operational overhead and costs associated with device configuration tasks and eases deployment by nontechnical users.

- Centralized management

Because the DHCP server maintains configurations for several subnets, an administrator only needs to update a single, central server when configuration parameters change.

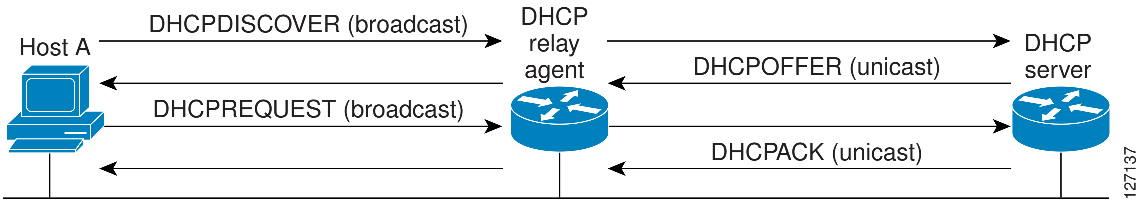
## DHCP Server Relay Agent and Client Operation

DHCP provides a framework for passing configuration information dynamically to hosts on a TCP/IP network. A DHCP client is an Internet host using DHCP to obtain configuration parameters such as an IP address.

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface.

The figure below shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server. The client, Host A, sends a DHCPDISCOVER broadcast message to locate a DHCP server. A relay agent forwards the packets between the DHCP client and server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message.

***Figure 1 DHCP Request for an IP Address from a DHCP Server***



A DHCP client may receive offers from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. Additionally, the offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address.

The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message. The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

The formal request for the offered IP address (the DHCPREQUEST message) that is sent by the client is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DHCP server are invalid (a misconfiguration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server will send to the client a DHCPNAK denial broadcast message, which means the offered configuration parameters have not been assigned, if an error has occurred during the negotiation of the parameters or the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client) of the DHCP server.

## DHCP Database

DHCP address pools are stored in non-volatile RAM (NVRAM). There is no limit on the number of address pools. An address binding is the mapping between the client’s IP and hardware addresses. The client’s IP address can be configured by the administrator (manual address allocation) or assigned from a pool by the DHCP server.

Manual bindings are stored in NVRAM. Manual bindings are just special address pools configured by a network administrator. There is no limit on the number of manual bindings.

Automatic bindings are IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database. Automatic bindings are stored on a remote host called the database agent. A DHCP database agent is any host--for example, an FTP, TFTP, or RCP server--that stores the DHCP bindings database.The bindings are saved as text records for easy maintenance.

You can configure multiple DHCP database agents and you can configure the interval between database updates and transfers for each agent.

## DHCP Attribute Inheritance

The DHCP server database is organized as a tree. The root of the tree is the address pool for natural networks, branches are subnetwork address pools, and leaves are manual bindings to clients. Subnetworks inherit network parameters and clients inherit subnetwork parameters. Therefore, common parameters, for example the domain name, should be configured at the highest (network or subnetwork) level of the tree.

Inherited parameters can be overridden. For example, if a parameter is defined in both the natural network and a subnetwork, the definition of the subnetwork is used.

Address leases are not inherited. If a lease is not specified for an IP address, by default, the DHCP server assigns a one-day lease for the address.

## DHCP Options and Suboptions

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. Options provide a method of appending additional information. Vendors that want to provide additional information to their client not designed into the protocol can use options.

The Cisco IOS XE DHCP implementation also allows most DHCP server options to be customized. For example, the TFTP server, which stores the Cisco IOS XE image, can be customized with option 150 to support intelligent IP phones.

Virtual Private Networks (VPNs) allow the possibility that two pools in separate networks can have the same address space, with private network addresses, served by the same DHCP server. Cisco IOS XE software supports VPN-related options and suboptions such as the relay agent information option and VPN identification suboption. A relay agent can recognize these VPN-related options and suboptions and forward the client-originated DHCP packets to a DHCP server. The DHCP server can use this information to assign IP addresses and other parameters, distinguished by a VPN identifier, to help select the VPN to which the client belongs.

For more information on DHCP options and suboptions, see the “DHCP Options Reference” appendix in the *Network Registrar User’s Guide* , Release 6.3.

During lease negotiation, the DHCP server sends the options shown in the table below to the client.

*Table 1 Default DHCP Server Options*

| DHCP Option Name | DHCP Option Code | Description |
|---|---|---|
| Subnet mask option | 1 | Specifies the client’s subnet mask per RFC 950. |
| Router option | 3 | Specifies a list of IP addresses for routers on the client’s subnet, usually listed in order of preference. |
| Domain name server option | 6 | Specifies a list of DNS name servers available to the client, usually listed in order of preference. |
| Hostname option | 12 | Specifies the name of the client. The name may or may not be qualified with the local domain name. |
| Domain name option | 15 | Specifies the domain name that the client should use when resolving hostnames via the Domain Name System. |
| NetBIOS over TCP/IP name server option | 44 | Specifies a list of RFC 1001/1002 NetBIOS name servers listed in order or preference. |
| NetBIOS over TCP/IP node type option | 46 | Enables NetBIOS over TCP/IP clients that are configurable to be configured as described in RFC 1001/1002. |
| IP address lease time option | 51 | Allows the client to request a lease for the IP address. |
| DHCP message type option | 53 | Conveys the type of the DHCP message. |
| Server identifier option | 54 | Identifies the IP address of the selected DHCP server. |
| Renewal (T1) time option | 58 | Specifies the time interval from address assignment until the client transitions to the renewing state. |
| Rebinding (T2) time option | 59 | Specifies the time interval from address assignment until the client transitions to the rebinding state. |

# DHCP Server On-Demand Address Pool Management Overview

The Cisco IOS XE DHCP server on-demand address pool (ODAP) manager is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses. When a Cisco IOS XE router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level.

ODAPs support address assignment using DHCP for customers using private addresses. Each ODAP is configured and associated with a particular Multiprotocol Label Switching (MPLS) VPN. Cisco IOS XE software also provides ODAP support for non-MPLS VPN address pools by adding pool name support to the **peer default ip address dhcp-pool** *pool name*command.

DHCP server subnet allocation is a way of offering entire subnets (ranges of addresses) to relay agents so that remote access devices can provision IP addresses to DHCP clients. This functionality can occur along with or instead of managing individual client addresses. Subnet allocation can improve IP address provisioning, aggregation, characterization, and distribution by relying on the DHCP infrastructure to dynamically manage subnets.

This capability allows the DHCP server to be configured with a pool of subnets for lease to ODAP clients. Subnet pools can be configured for global ODAP clients or MPLS VPN ODAP clients on a per-client basis. The DHCP subnet allocation server creates bindings for the subnet leases and stores these leases in the DHCP database.

# Additional References

The following sections provide references related to DHCP.

### Related Documents

| Related Topic | Document Title |
|---|---|
| DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |
| DHCP server configuration | “Configuring the Cisco IOS XE DHCP Server” module |
| DHCP relay agent configuration | “Configuring the Cisco IOS XE DHCP Relay Agent” module |
| DHCP client configuration | “Configuring the Cisco IOS XE DHCP Client” module |
| DHCP server on-demand address pools | “Configuring the DHCP Server On-Demand Address Pool Manager” module |
| DHCP advanced features | “Configuring DHCP Services for Accounting and Security” module |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 951 | *Bootstrap Protocol (BOOTP)* |
| RFC 2131 | *Dynamic Host Configuration Protocol* |
| RFC 2132 | *DHCP Options and BOOTP Vendor Extensions* |
| RFC 1542 | *Clarifications and Extensions for the Bootstrap Protocol* |

# Technical Assistance

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

# Glossary

**address binding** --A mapping between the client’s IP and hardware (MAC) addresses. The client’s IP address may be configured by the administrator (manual address allocation) or assigned from a pool by the DHCP server (automatic address allocation). The binding also contains a lease expiration date. The default for the lease expiration date is one day.

**address conflict** --A duplication of use of the same IP address by two hosts. During address assignment, DHCP checks for conflicts using ping and gratuitous (ARP). If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

**address pool** --The range of IP addresses assigned by the DHCP server. Address pools are indexed by subnet number.

**automatic address allocation** --An address assignment method where a network administrator obtains an IP address for a client for a finite period of time or until the client explicitly relinquishes the address. Automatic allocation is particularly useful for assigning an address to a client that will be connected to the network only temporarily or for sharing a limited pool of IP addresses among a group of clients that do not need permanent IP addresses. Automatic allocation may also be a good choice for assigning an IP address to a new client being permanently connected to a network where IP addresses are sufficiently scarce that it is important to reclaim them when old clients are retired.

**BOOTP** --Bootstrap Protocol. A protocol that provides a method for a booting computer to find out its IP address and the location of the boot file with the rest of its parameters.

**client** --Any host requesting configuration parameters.

database--A collection of address pools and bindings.

**database agent** --Any host storing the DHCP bindings database, for example, a Trivial File Transfer Protocol (TFTP) server.

**DHCP** --Dynamic Host Configuration Protocol. A protocol that provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

**DNS** --Domain Name System. A system used in the Internet for translating names of network nodes into addresses.

**manual address allocation** --An address assignment method that allocates an administratively assigned IP address to a host. Manual allocation allows DHCP to be used to eliminate the error-prone process of manually configuring hosts with IP addresses.

**PWLAN** --Public Wireless Local Area Network. A type of wireless LAN, often referred to as a hotspot, that anyone having a properly configured computer device can access.

**relay agent** --A router that forwards DHCP and BOOTP messages between a server and a client on different subnets.

**server** --Any host providing configuration parameters.

**SSG** --Service Selection Gateway. The Cisco IOS XE feature set that provides on-demand service enforcement within the Cisco network.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# Configuring the Cisco IOS XE DHCP Server

Cisco routers running Cisco IOS XE software include Dynamic Host Configuration Protocol (DHCP) server and relay agent software. The Cisco IOS XE DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. The DHCP server can be configured to assign additional parameters such as the IP address of the domain name system (DNS) server and the default router.

This module describes the concepts and the tasks needed to configure the Cisco IOS XE DHCP server.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for Configuring the DHCP Server

Before you configure the Cisco IOS XE DHCP server, you should understand the concepts documented in the “DHCP Overview” module.

The Cisco IOS XE DHCP server and relay agent are enabled by default. You can verify if they have been disabled by checking your configuration file. If they have been disabled, the **no service dhcp** command will appear in the configuration file. Use the **service dhcp** command to reenable the functionality if necessary.

The Cisco IOS XE DHCP relay agent will be enabled on an interface only when the **ip helper-address** is configured. This command enables the DHCP broadcast to be forwarded to the configured DHCP server.

# Information About the Cisco IOS XE DHCP Server

## Overview of the DHCP Server

TheCisco IOS XE DHCP server accepts address assignment requests and renewals and assigns the addresses from predefined groups of addresses contained within DHCP address pools. These address pools can also be configured to supply additional information to the requesting client such as the IP address of the DNS server, the default router, and other configuration parameters. The Cisco IOS XE DHCP server can accept broadcasts from locally attached LAN segments or from DHCP requests that have been forwarded by other DHCP relay agents within the network.

## Database Agents

A DHCP database agent is any host (for example, an FTP, TFTP, or rcp server) or storage media on the DHCP server (for example, disk0) that stores the DHCP bindings database. You can configure multiple DHCP database agents, and you can configure the interval between database updates and transfers for each agent.

Automatic bindings are IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database. Automatic binding information (such as lease expiration date and time, interface index, and VPN routing and forwarding [VRF] name) is stored on a database agent. The bindings are saved as text records for easy maintenance.

### Address Conflicts

An address conflict occurs when two hosts use the same IP address. During address assignment, DHCP checks for conflicts using ping and gratuitous Address Resolution Protocol (ARP). If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

## DHCP Address Pool Conventions

You can configure a DHCP address pool with a name that is a symbolic string (such as “engineering”) or an integer (such as 0). Configuring a DHCP address pool also puts the router into DHCP pool configuration mode--identified by the (dhcp-config)# prompt--from which you can configure pool parameters (for example, the IP subnet number and default router list).

### DHCP Address Pool Selection

DHCP defines a process by which the DHCP server knows the IP subnet in which the DHCP client resides, and it can assign an IP address from a pool of valid IP addresses in that subnet. The process by which the DHCP server identifies which DHCP address pool to use to service a client request is described in this section.

The DHCP server identifies which DHCP address pool to use to service a client request as follows:

- If the client is not directly connected (the giaddr field of the DHCPDISCOVER broadcast message is non-zero), the DHCP server matches the DHCPDISCOVER with a DHCP pool that has the subnet that contains the IP address in the giaddr field.
- If the client is directly connected (the giaddr field is zero), the DHCP server matches the DHCPDISCOVER with DHCP pool(s) that contain the subnet(s) configured on the receiving interface. If the interface has secondary IP addresses, the subnets associated with the secondary IP addresses are examined for possible allocation only after the subnet associated with the primary IP address (on the interface) is exhausted.

Cisco IOS XE DHCP server software supports advanced capabilities for IP address allocation. See the "Configuring DHCP Address Allocation Using Option 82" section for more information.

## Address Bindings

An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server.

Manual bindings are IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database. Manual bindings are stored in NVRAM on the DHCP server. Manual bindings are just special address pools. There is no limit on the number of manual bindings, but you can only configure one manual binding per host pool.

Automatic bindings are IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database. Because the bindings are stored in volatile memory on the DHCP server, binding information is lost in the event of a power failure or upon router reload for any other reason. To prevent the loss of automatic binding information in such an event, a copy of the automatic binding information can be stored on a remote host called a DHCP database agent. The bindings are periodically written to the database agent. If the router reloads, the bindings are read back from the database agent to the DHCP database on the DHCP server.

**Note** We strongly recommend using database agents. However, the Cisco IOS XE DHCP server can function without database agents.

All DHCP clients send a client identifier (DHCP option 61) in the DHCP packet. To configure manual bindings, you must enter the **client-identifier** DHCP pool configuration command with the appropriate hexadecimal values identifying the DHCP client.

## Ping Packet Settings

By default, the DHCP server pings a pool address twice before assigning a particular address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client.

By default, the DHCP server waits 2 seconds before timing out a ping packet.

# DHCP Attribute Inheritance

The DHCP server database is organized as a tree. The root of the tree is the address pool for natural networks, branches are subnetwork address pools, and leaves are manual bindings to clients. Subnetworks inherit network parameters and clients inherit subnetwork parameters. Therefore, common parameters, for example the domain name, should be configured at the highest (network or subnetwork) level of the tree.

Inherited parameters can be overridden. For example, if a parameter is defined in both the natural network and a subnetwork, the definition of the subnetwork is used.

Address leases are not inherited. If a lease is not specified for an IP address, by default, the DHCP server assigns a one-day lease for the address.

# DHCP Server Address Allocation Using Option 82

The Cisco IOS XE DHCP server can allocate dynamic IP addresses based on the relay information option (option 82) information sent by the relay agent.

Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway address (giaddr field of the DHCP packet) or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using option 82, the Cisco IOS XE relay agent has long been able to include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. The Cisco IOS XE DHCP server can also use option 82 as a means to provide additional information to properly allocate IP addresses to DHCP clients.

- DHCP Address Allocation Using Option 82 Feature Design, page 12
- Usage Scenario for DHCP Address Allocation Using Option 82, page 12
- DHCP Class Capability, page 13

## DHCP Address Allocation Using Option 82 Feature Design

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options. Option 82 is organized as a single DHCP option that contains information known by the relay agent.

This feature is designed to allow the Cisco IOS XE DHCP server to use option 82 information to help determine which IP addresses to allocate to clients. The information sent via option 82 will be used to identify which port the DHCP request came in on. This feature does not parse out the individual suboptions contained within option 82. Rather, the address allocation is done by matching a configured pattern byte by byte.

The feature introduces a new DHCP class capability, which is a method to group DHCP clients based on some shared characteristics other than the subnet in which the clients reside.

## Usage Scenario for DHCP Address Allocation Using Option 82

In an example application, DHCP clients are connected to two ports of a single switch. Each port can be configured to be part of two VLANs: VLAN1 and VLAN2. DHCP clients belong to either VLAN1 or VLAN2 and it is assumed that the switch can differentiate the VLAN that a particular DHCP Discover message belongs to (possibly through Layer 2 encapsulation). Each VLAN has its own subnet and all

DHCP messages from the same VLAN (same switch) will have the giaddr field set to the same value indicating the subnet of the VLAN.

The problem is that for a DHCP client connecting to port 1 of VLAN1, it must be allocated an IP address from one range within the VLAN's subnet, whereas a DHCP client connecting to port 2 of VLAN1 must be allocated an IP address from another range. Both these two IP address ranges are part of the same subnet (and have the same subnet mask). In the normal DHCP address allocation, the DHCP server will look only at the giaddr field and thus will not be able to differentiate between the two ranges.

To solve this problem, a relay agent residing at the switch inserts the relay information option (option 82), which carries information specific to the port, and the DHCP server must inspect both the giaddr field and the inserted option 82 during the address selection process.

## DHCP Class Capability

The Cisco IOS XE software will look up a pool based on IP address (giaddr or incoming interface IP address) and then match the request to a class or classes configured in the pool in the order the classes are specified in the DHCP pool configuration.

When a DHCP address pool has been configured with one or more DHCP classes, the pool becomes a restricted access pool, which means that no addresses will be allocated from the pool unless one or more of the classes in the pool is matched. This design allows DHCP classes to be used for either access control (no default class is configured on the pool) or to provide further address range partitions with the subnet of the pool.

Multiple pools can be configured with the same class, eliminating the need to configure the same pattern in multiple pools.

The following capabilities are currently supported for DHCP class-based address allocation:

- Specifying the full relay agent information option value as a raw hexadecimal string by using the **relay-information hex** command in the new relay agent information configuration mode.
- Support for bitmasking the raw relay information hexadecimal value.
- Support for a wildcard at the end of the hexadecimal string specified by the **relay-information hex** command.

# How to Configure the Cisco IOS XE DHCP Server

# Configuring a DHCP Database Agent or Disabling Conflict Logging

Perform this task to configure a DHCP database agent.

**Note** We strongly recommend using database agents. However, the Cisco IOS XE server can run without them. If you choose not to configure a DHCP database agent, disable the recording of DHCP address conflicts on the DHCP server by using the **no ip dhcp conflict logging** command in global configuration mode. If there is conflict logging but no database agent configured, bindings are lost across router reboots. Possible false conflicts can occur causing the address to be removed from the address pool until the network administrator intervenes.

>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*]
   - or
   - **no ip dhcp conflict logging**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | Do one of the following:<br>• **ip dhcp database** *url* [**timeout** *seconds* \| **write-delay** *seconds*]<br>• or<br>• **no ip dhcp conflict logging**<br>**Example:**<br>`Router(config)# ip dhcp database ftp:// user:password@172.16.1.1/router-dhcp timeout 80`<br>**Example:**<br>**Example:**<br>`Router(config)# no ip dhcp conflict logging` | Configures a DHCP server to save automatic bindings on a remote host called a database agent.<br>or<br>Disables DHCP address conflict logging.<br>• Choose this option only if you do not configure a DHCP database agent. See the Configuring a DHCP Database Agent or Disabling Conflict Logging, page 14 section for guidelines. |

# Excluding IP Addresses

Perform this task to specify IP addresses (excluded addresses) that the DHCP server should not assign to clients.

The IP address configured on the router interface is automatically excluded from the DHCP address pool. The DHCP server assumes that all other IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients.

You need to exclude addresses from the pool if the DHCP server should not allocate those IP addresses. An example usage scenario is when two DHCP servers are set up to service the same network segment (subnet) for redundancy. If the two DHCP servers do not coordinate their services with each other using a protocol such as DHCP failover, then each DHCP server must be configured to allocate from a non-overlapping set of addresses in the shared subnet. See the "Configuring Manual Bindings Example" for a configuration example.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp excluded-address** *low-address* [*high-address*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip dhcp excluded-address** *low-address* [*high-address*]<br>**Example:**<br>`Router(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.103` | Specifies the IP addresses that the DHCP server should not assign to DHCP clients. |

# Configuring DHCP Address Pools

## Configuring a DHCP Address Pool

Perform this task to configure a DHCP address pool. On a per-address pool basis, specify DHCP options for the client as necessary.

Before you configure the DHCP address pool, you need to:

- Identify DHCP options for devices where necessary, including the following:
  - Default boot image name
  - Default routers
  - Domain Name System (DNS) servers
  - NetBIOS name server
  - Primary subnet
- Decide on a NetBIOS node type (b, p, m, or h).
- Decide on a DNS domain name.

**Note** You cannot configure manual bindings within the same pool that is configured with the **network** DHCP pool configuration command. To configure manual bindings, see the "Configuring Manual Bindings" section.

>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask* | / *prefix-length*]
5. **domain-name** *domain*
6. **dns-server** *address* [*address2 ... address8]*
7. **bootfile** *filename*
8. **next-server** *address* [*address2 ... address8]*
9. **netbios-name-server** *address* [*address2 ... address8]*
10. **netbios-node-type** *type*
11. **default-router** *address* [*address2 ... address8]*
12. **option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*}
13. **lease** *{days* [*hours*] [*minutes*]| **infinite**}
14. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp pool** *name*<br>**Example:**<br>`Router(config)# ip dhcp pool 1` | Creates a name for the DHCP server address pool and enters DHCP pool configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **network** *network-number* [*mask* \| / *prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# network 172.16.0.0 /16` | Specifies the subnet network number and mask of the DHCP address pool. |
| **Step 5** | **domain-name** *domain*<br>**Example:**<br>`Router(dhcp-config)# domain-name cisco.com` | Specifies the domain name for the client. |
| **Step 6** | **dns-server** *address* [*address2 ... address8]*<br>**Example:**<br>`Router(dhcp-config)# dns server 172.16.1.103 172.16.2.103` | Specifies the IP address of a DNS server that is available to a DHCP client.<br>• One IP address is required; however, you can specify up to eight IP addresses in one command line.<br>• Servers should be listed in order of preference. |
| **Step 7** | **bootfile** *filename*<br>**Example:**<br>`Router(dhcp-config)# bootfile xllboot` | (Optional) Specifies the name of the default boot image for a DHCP client.<br>• The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load. |
| **Step 8** | **next-server** *address* [*address2 ... address8]*<br>**Example:**<br>`Router(dhcp-config)# next-server 172.17.1.103 172.17.2.103` | (Optional) Configures the next server in the boot process of a DHCP client.<br>• If multiple servers are specified, DHCP assigns them to clients in round-robin order. The first client gets address 1, the next client gets address 2, and so on.<br>• If this command is not configured, DHCP uses the server specified by the **ip helper address** command as the boot server. |
| **Step 9** | **netbios-name-server** *address* [*address2 ... address8]*<br>**Example:**<br>`Router(dhcp-config)# netbios-name-server 172.16.1.103 172.16.2.103` | (Optional) Specifies the NetBIOS Windows Internet Naming Service (WINS) server that is available to a Microsoft DHCP client.<br>• One address is required; however, you can specify up to eight addresses in one command line.<br>• Servers should be listed in order of preference. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **netbios-node-type** *type*<br>**Example:**<br>`Router(dhcp-config)# netbios-node-type h-node` | (Optional) Specifies the NetBIOS node type for a Microsoft DHCP client. |
| **Step 11** | **default-router** *address* [*address2 ... address8]*<br>**Example:**<br>`Router(dhcp-config)# default-router 172.16.1.100 172.16.1.101` | (Optional) Specifies the IP address of the default router for a DHCP client.<br>• The IP address should be on the same subnet as the client.<br>• One IP address is required; however, you can specify a up to eight IP addresses in one command line. These default routers are listed in order of preference; that is, *address* is the most preferred router, address2 is the next most preferred router, and so on.<br>• When a DHCP client requests an IP address, the router--acting as a DHCP server--accesses the default router list to select another router that the DHCP client is to use as the first hop for forwarding messages. After a DHCP client has booted, the client begins sending packets to its default router. |
| **Step 12** | **option** *code* [**instance** *number*] {**ascii** *string* \| **hex** *string* \| *ip-address*}<br>**Example:**<br>`Router(dhcp-config)# option 19 hex 01` | (Optional) Configures DHCP server options. |
| **Step 13** | **lease** *{days* [*hours*] [*minutes*]\| **infinite**}<br>**Example:**<br>`Router(dhcp-config)# lease 30` | (Optional) Specifies the duration of the lease.<br>• The default is a one-day lease.<br>• The **infinite** keyword specifies that the duration of the lease is unlimited. |
| **Step 14** | **end**<br>**Example:**<br>`Router(config-dhcp-subnet-secondary)# end` | Returns to global configuration mode. |

## Verifying the DHCP Address Pool Configuration

Perform this task to verify the DHCP address pool configuration.

### SUMMARY STEPS

1. **enable**
2. **show ip dhcp pool** [*name*]
3. **show ip dhcp binding** [*address*]
4. **show ip dhcp conflict** [*address*]
5. **show ip dhcp database** [*url*]
6. **show ip dhcp server statistics** [*type-number*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show ip dhcp pool** [*name*]<br>**Example:**<br>`Router# show ip dhcp pool` | (Optional) Displays information about DHCP address pools. |
| **Step 3** | **show ip dhcp binding** [*address*]<br>**Example:**<br>`Router# show ip dhcp binding` | (Optional) Displays a list of all bindings created on a specific DHCP server.<br>• Use the **show ip dhcp binding** command to display the IP addresses that have already been assigned. Verify that the address pool has not been exhausted. If necessary, re-create the pool to create a larger pool of addresses.<br>• Use the **show ip dhcp binding** command to display the lease expiration date and time of the IP address of the host. |
| **Step 4** | **show ip dhcp conflict** [*address*]<br>**Example:**<br>`Router# show ip dhcp conflict` | (Optional) Displays a list of all address conflicts. |
| **Step 5** | **show ip dhcp database** [*url*]<br>**Example:**<br>`Router# show ip dhcp database` | (Optional) Displays recent activity on the DHCP database. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show ip dhcp server statistics** [*type-number*]<br>**Example:**<br>`Router# show ip dhcp server statistics` | (Optional) Displays count information about server statistics and messages sent and received. |

# Configuring Manual Bindings

**Note** You cannot configure manual bindings within the same pool that is configured with the **network**command in DHCP pool configuration mode. See the "Configuring DHCP Address Pools" section for information about DHCP address pools and the **network** command.

>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **host** *address* [*mask*| / *prefix-length*]
5. **client-identifier** *unique-identifier*
6. **hardware-address** *hardware-address type*
7. **client-name** *name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool pool1` | Creates a name for the DHCP server address pool and places you in DHCP pool configuration mode--identified by the (dhcp-config)# prompt. |
| **Step 4** | **host** *address* [*mask*\| / *prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# host 172.16.2.254` | Specifies the IP address and subnet mask of the client.<br>• There is no limit on the number of manual bindings but you can only configure one manual binding per host pool. |
| **Step 5** | **client-identifier** *unique-identifier*<br>**Example:**<br>`Router(dhcp-config)# client-identifier 01b7.0813.8811.66` | Specifies the unique identifier for DHCP clients. This command is used for DHCP requests.<br>• DHCP clients require client identifiers. The unique identification of the client is specified in dotted hexadecimal notation, for example, 01b7.0813.8811.66, where 01 represents the Ethernet media type.<br>• See "Troubleshooting_Tips" below for information on how to determine the client identifier of the DHCP client. |
| **Step 6** | **hardware-address** *hardware-address type*<br>**Example:**<br>`Router(dhcp-config)# hardware-address b708.1388.f166 ieee802` | (Optional) Specifies a hardware address for the client. This command is used for BOOTP requests. |
| **Step 7** | **client-name** *name*<br>**Example:**<br>`Router(dhcp-config)# client-name client1` | (Optional) Specifies the name of the client using any standard ASCII character.<br>• The client name should not include the domain name. For example, the name mars should not be specified as mars.cisco.com. |

- Troubleshooting Tips, page 22

## Troubleshooting Tips

You can determine the client identifier by using the **debug ip dhcp server packet** command. In the following example, the client is identified by the value 0b07.1134.a029.

```
Router# debug ip dhcp server packet

DHCPD:DHCPDISCOVER received from client 0b07.1134.a029 through relay 10.1.0.253.
DHCPD:assigned IP address 10.1.0.3 to client 0b07.1134.a029.
.
```

```
.
.
```

# Customizing DHCP Server Operation

Perform this task to customize the behavior of the DHCP server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp ping packets** *number*
4. **ip dhcp ping timeout** *milliseconds*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp ping packets** *number*<br>**Example:**<br>`Router(config)# ip dhcp ping packets 5` | (Optional) Specifies the number of ping packets the DHCP server sends to a pool address before assigning the address to a requesting client.<br>• The default is two packets. Setting the *number*argument to a value of 0 disables the DHCP server ping operation completely. |
| **Step 4** | **ip dhcp ping timeout** *milliseconds*<br>**Example:**<br>`Router(config)# ip dhcp ping timeout 850` | (Optional) Specifies the amount of time the DHCP server waits for a ping reply from an address pool. |

# Configuring a Remote Router to Import DHCP Server Options from a Central DHCP Server

The Cisco IOS DHCP server can dynamically configure options such as the DNS and WINS addresses to respond to DHCP requests from local clients behind the customer premises equipment (CPE). Previously, network administrators needed to manually configure the Cisco IOS DHCP server on each device. The Cisco IOS DHCP server was enhanced to allow configuration information to be updated automatically.

Network administrators can configure one or more centralized DHCP servers to update specific DHCP options within the DHCP pools. The remote servers can request or “import” these option parameters from the centralized servers.

This section contains the following tasks:

- Configuring the Central DHCP Server to Update DHCP Options, page 24
- Configuring the Remote Router to Import DHCP Options, page 25

## Configuring the Central DHCP Server to Update DHCP Options

Perform this task to configure the central DHCP server to update DHCP options.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask* | / *prefix-length*]
5. **dns-server** *address* [*address2* ... *address8*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp pool** *name*<br>**Example:**<br>`Router(config)# ip dhcp pool 1` | Creates a name for the DHCP server address pool and enters DHCP pool configuration mode. |
| **Step 4** | **network** *network-number* [*mask* \| / *prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# network 172.16.0.0 /16` | Specifies the subnet network number and mask of the DHCP address pool. |

| | Command or Action | Purpose |
|---|---|---|
| Step 5 | **dns-server** *address* [*address2 ... address8*]<br>**Example:**<br>`Router(dhcp-config)# dns server 172.16.1.103 172.16.2.103` | (Optional) Specifies the IP address of a DNS server that is available to a DHCP client.<br>• One IP address is required; however, you can specify up to eight IP addresses in one command line.<br>• Servers should be listed in order of preference. |

## Configuring the Remote Router to Import DHCP Options

Perform this task to configure the remote router to import DHCP options from a central DHCP server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **network** *network-number* [*mask* | / *prefix-length*]
5. **import all**
6. **exit**
7. **interface** *type number*
8. **ip address dhcp**
9. **end**
10. **show ip dhcp import**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool sanjose1` | Creates a name for the DHCP server address pool and enters DHCP pool configuration mode. |
| **Step 4** | **network** *network-number* [*mask* \| / *prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# network 172.30.0.0 /16` | Specifies the subnet network number and mask of the DHCP address pool. |
| **Step 5** | **import all**<br>**Example:**<br>`Router(dhcp-config)# import all` | Imports DHCP option parameters into the DHCP server database. |
| **Step 6** | **exit**<br>**Example:**<br>`Router(dhcp-config)# exit` | Exits DHCP pool configuration mode. |
| **Step 7** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Configures an interface and enters interface configuration mode. |
| **Step 8** | **ip address dhcp**<br>**Example:**<br>`Router(config-if)# ip address dhcp` | Specifies that the interface acquires an IP address through DHCP. |
| **Step 9** | **end**<br>**Example:**<br>`Router(dhcp-config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **show ip dhcp import**<br>**Example:**<br>`Router# show ip dhcp import` | Displays the options that have been imported from the central DHCP server. |

# Configuring DHCP Address Allocation Using Option 82

## Restrictions for DHCP Address Allocation Using Option 82

If the relay agent inserts option 82 but does not set the giaddr field in the DHCP packet, the DHCP server interface must be configured as a trusted interface by using the **ip dhcp relay information trusted** global configuration command. This configuration prevents the server from dropping the DHCP message.

## Enabling Option 82 for DHCP Address Allocation

By default, the Cisco IOS XE DHCP server can use information provided by option 82 to allocate IP addresses. To reenable this capability if it has been disabled, perform the task described in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp use class**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip dhcp use class**<br>**Example:**<br>`Router(config)# ip dhcp use class` | Controls whether DHCP classes are used for address allocation.<br>• This functionality is enabled by default.<br>• Use the **no** form of this command to disable this functionality without deleting the DHCP class configuration. |

## Troubleshooting Tips

If DHCP classes are configured in the pool, but the DHCP server does not make use of the classes, verify if the **no ip dhcp use class**command was configured.

## Defining the DHCP Class and Relay Agent Information Patterns

Perform this task to define the DHCP class and relay agent information patterns.

You must know the hexadecimal value of each byte location in option 82 to be able to configure the **relay-information hex** command. The option 82 format may vary from product to product. Contact the relay agent vendor for this information.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp class** *class-name*
4. **relay agent information**
5. **relay-information hex** *pattern* [*] [**bitmask** *mask*]
6. Repeat Steps 3 through 5 for each DHCP class you need to configure.

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp class** *class-name*<br>**Example:**<br>`Router(config)# ip dhcp class CLASS1` | Defines a DHCP class and enters DHCP class configuration mode. |
| **Step 4** | **relay agent information**<br>**Example:**<br>`Router(dhcp-class)# relay agent information` | Enters relay agent information option configuration mode.<br>• If this step is omitted, then the DHCP class matches to any relay agent information option, whether it is present or not. |
| **Step 5** | **relay-information hex** *pattern* [*] [**bitmask** *mask*]<br>**Example:**<br>`Router(dhcp-class-relayinfo)# relay-information hex 01030a0b0c02050000000123` | (Optional) Specifies a hexadecimal value for the full relay information option.<br>• The *pattern* argument creates a pattern that is used to match to the DHCP class.<br>• If you omit this step, no pattern is configured and it is considered a match to any relay agent information option value, but the relay information option must be present in the DHCP packet.<br>• You can configure multiple **relay-information hex** commands in a DHCP class. |
| **Step 6** | Repeat Steps 3 through 5 for each DHCP class you need to configure. | -- |

## Troubleshooting Tips

You can enable the **debug ip dhcp server class** command to display the class matching results.

## Defining the DHCP Address Pool

Perform this task to define the DHCP address pool.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask* | / *prefix-length*]
5. **class** *class-name*
6. **address range** *start-ip end-ip*
7. Repeat Steps 5 and 6 for each DHCP class you need to associate to the DHCP pool.

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp pool** *name*<br>**Example:**<br>`Router(config)# ip dhcp pool ABC` | Configures a DHCP address pool on a Cisco IOS XE DHCP server and enters DHCP pool configuration mode.<br>• Multiple pools can be configured with the same class, eliminating the need to configure the same pattern in multiple pools. |
| **Step 4** | **network** *network-number* [*mask* | / *prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# network 10.0.20.0` | Configures the subnet number and mask for a DHCP address pool on a Cisco IOS XE DHCP server. |
| **Step 5** | **class** *class-name*<br>**Example:**<br>`Router(dhcp-config)# class CLASS1` | Associates a class with a pool and enters DHCP pool class configuration mode.<br>• This command will also create a DHCP class if the DHCP class is not yet defined. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **address range** *start-ip end-ip*<br>**Example:**<br>`Router(dhcp-pool-class)# address range 10.0.20.1 10.0.20.100` | (Optional) Sets an address range for a DHCP class in a DHCP server address pool.<br>• If this command is not configured for a class, the default value is the entire subnet of the pool. |
| **Step 7** | Repeat Steps 5 and 6 for each DHCP class you need to associate to the DHCP pool. | Each class in the DHCP pool will be examined for a match in the order configured. |

# Configuring a Static Route with the Next-Hop Dynamically Obtained Through DHCP

Perform this task to configure a static route to use a DHCP default gateway as the next-hop router.

This task enables static routes to be assigned using a DHCP default gateway as the next-hop router. This behavior was not possible before the introduction of this feature because the gateway IP address is not known until after the DHCP address assignment. A static route could not be configured with the command-line interface (CLI) that used that DHCP-supplied address.

The static routes are installed in the routing table when the default gateway is assigned by the DHCP server. The routes remain in the routing table until the DHCP lease expires at which time the routes are removed.

When a DHCP client releases an address, the corresponding static route (the route configured with the **ip route**command) is automatically removed from the routing table. If the DHCP router option (option 3 of the DHCP packet) changes during the client renewal, the DHCP default gateway changes to the new IP address supplied in the renewal.

This feature is particularly useful for VPN deployments such as Dynamic Multipoint VPNs (DMVPNs). This feature is useful when a non-physical interface like a multipoint generic routing encapsulation (mGRE) tunnel is configured on the router and certain traffic needs to be excluded from going to the tunnel interface.

Verify all DHCP client and server configuration steps. Ensure that the DHCP client and server are properly defined to supply a DHCP router option 3.

**Note**

- If the DHCP client is not able to obtain an IP address or default router IP address, the static route is not installed in the routing table.
- If the lease has expired and the DHCP client cannot renew the address, the DHCP IP address assigned to the client is released and any associated static routes are removed from the routing table.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} **dhcp** [*distance*]
4. **end**
5. **show ip route**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip route** *prefix mask* {*ip-address* \| *interface-type interface-number* [*ip-address*]} **dhcp** [*distance*]<br>**Example:**<br>`Router(config)# ip route 209.165.200.225 255.255.255.255 GigabitEthernet 0/0/0 dhcp`<br>**Example:**<br>`Router(config)# ip route 209.165.200.226 255.255.255.255 GigabitEthernet 0/0/1 dhcp 20` | Assigns a static route for the default next-hop router when the DHCP server is accessed for an IP address.<br>• If more than one interface on a router is configured to obtain an IP address from a DHCP server, use the **ip route** *prefix mask interface-type interface-number* **dhcp** command for each interface. If the interface is not specified, the route is added to the routing table as soon as any of the interfaces obtain an IP address and default router. |
| **Step 4** | **end**<br>**Example:**<br>`Router(config)# end` | Returns to global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **show ip route**<br>**Example:**<br>`Router# show ip route` | (Optional) Displays the current state of the routing table.<br>• Use this command to display assigned static routes once the DHCP client obtains an address and a default router address from the DHCP server. |

# Clearing DHCP Server Variables

Perform this task to clear DHCP server variables.

### SUMMARY STEPS

1. **enable**
2. **clear ip dhcp binding** {*address* | *****}
3. **clear ip dhcp conflict** {*address* | *****}
4. **clear ip dhcp server statistics**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **clear ip dhcp binding** {*address* | *****}<br>**Example:**<br>`Router# clear ip dhcp binding *` | Deletes an automatic address binding from the DHCP database.<br>• Specifying the *address* argument clears the automatic binding for a specific (client) IP address, whereas specifying an asterisk (*****) clears all automatic bindings. |
| **Step 3** | **clear ip dhcp conflict** {*address* | *****}<br>**Example:**<br>`Router# clear ip dhcp conflict 172.16.1.103` | Clears an address conflict from the DHCP database.<br>• Specifying the *address* argument clears the conflict for a specific IP address, whereas specifying an asterisk (*****) clears conflicts for all addresses. |
| **Step 4** | **clear ip dhcp server statistics**<br>**Example:**<br>`Router# clear ip dhcp server statistics` | Resets all DHCP server counters to 0. |

# Configuration Examples for the Cisco IOS XE DHCP Server

## Configuring the DHCP Database Agent Example

The following example shows how to store bindings on host 172.16.4.253. The file transfer protocol is FTP. The server should wait 2 minutes (120 seconds) before writing database changes.

```
ip dhcp database ftp://user:password@172.16.4.253/router-dhcp write-delay 120
```

## Excluding IP Addresses Example

In the following example, server A and server B service the subnet 10.0.20.0/24. Splitting the subnet equally between the two servers, server A is configured to allocate IP addresses 10.0.20.1 to 10.0.20.125 and server B is configured to allocate IP addresses 10.0.20.126 to 10.0.20.254.

### Server A

```
ip dhcp excluded-address 10.0.20.126 10.0.20.255
!
ip dhcp pool A
 network 10.0.20.0 255.255.255.0
```

### Server B

```
ip dhcp excluded-address 10.0.20.0 10.0.20.125
!
ip dhcp pool B
 network 10.0.20.0 255.255.255.0
```

## Configuring DHCP Address Pools Example

In the following example, three DHCP address pools are created: one in network 172.16.0.0, one in subnetwork 172.16.1.0, and one in subnetwork 172.16.2.0. Attributes from network 172.16.0.0--such as the domain name, DNS server, NetBIOS name server, and NetBIOS node type--are inherited in subnetworks 172.16.1.0 and 172.16.2.0. In each pool, clients are granted 30-day leases and all addresses in each subnetwork, except the excluded addresses, are available to the DHCP server for assigning to clients. The table below lists the IP addresses for the devices in three DHCP address pools.

*Table 2 DHCP Address Pool Configuration Example*

| Pool 0 (Network 172.16.0.0) | Pool 1 (Subnetwork 172.16.1.0) | Pool 2 (Subnetwork 172.16.2.0) | | | |
|---|---|---|---|---|---|
| Device | IP Address | Device | IP Address | Device | IP Address |
| Default routers | - | Default routers | 172.16.1.100<br>172.16.1.101 | Default routers | 172.16.2.100<br>172.16.2.101 |
| DNS server | 172.16.1.102<br>172.16.2.102 | -- | -- | -- | -- |
| NetBIOS name server | 172.16.1.103<br>172.16.2.103 | -- | -- | -- | -- |
| NetBIOS node type | h-node | -- | -- | -- | -- |

```
ip dhcp database ftp://user:password@172.16.4.253/router-dhcp write-delay 120
ip dhcp excluded-address 172.16.1.100 172.16.1.103
ip dhcp excluded-address 172.16.2.100 172.16.2.103
!
ip dhcp pool 0
 network 172.16.0.0 /16
 domain-name cisco.com
 dns-server 172.16.1.102 172.16.2.102
 netbios-name-server 172.16.1.103 172.16.2.103
 netbios-node-type h-node
!
ip dhcp pool 1
 network 172.16.1.0 /24
 default-router 172.16.1.100 172.16.1.101
 lease 30
!
ip dhcp pool 2
 network 172.16.2.0 /24
 default-router 172.16.2.100 172.16.2.101
 lease 30
```

## Configuring Manual Bindings Example

The following example shows how to create a manual binding for a client named Mars.cisco.com. The MAC address of the client is 02c7.f800.0422 and the IP address of the client is 172.16.2.254.

```
ip dhcp pool Mars
 host 172.16.2.254
 hardware-address 02c7.f800.0422 ieee802
 client-name Mars
```

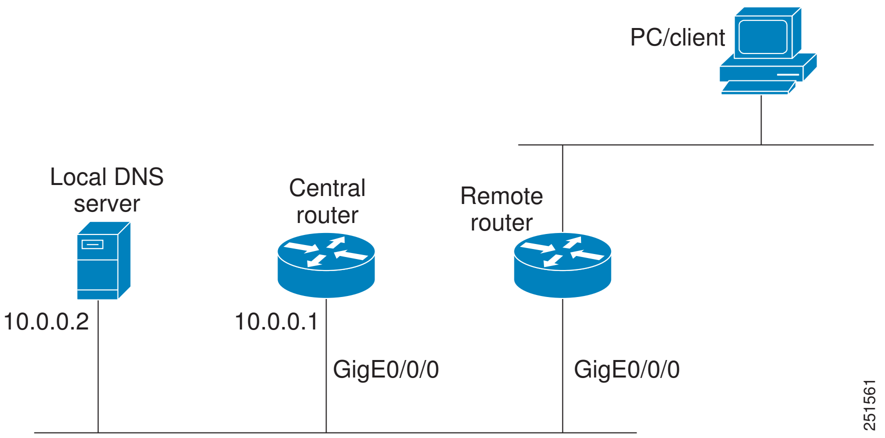
Because attributes are inherited, the previous configuration is equivalent to the following:

```
ip dhcp pool Mars
 host 172.16.2.254 mask 255.255.255.0
 hardware-address 02c7.f800.0422 ieee802
 client-name Mars
 default-router 172.16.2.100 172.16.2.101
 domain-name cisco.com
 dns-server 172.16.1.102 172.16.2.102
 netbios-name-server 172.16.1.103 172.16.2.103
 netbios-node-type h-node
```

# Importing DHCP Options Example

The following example shows a remote and central server configured to support the importing of DHCP options. The central server is configured to automatically update DHCP options, such as DNS and WINs addresses, within the DHCP pools. In response to a DHCP request from a local client behind CPE equipment, the remote server can request or “import” these option parameters from the centralized server. See the figure below for a diagram of the network topology.

*Figure 2 DHCP Example Network Topology*



## Central Router

```
!do not assign this range to DHCP clients
ip dhcp-excluded address 10.0.0.1 10.0.0.5
!
ip dhcp pool central
! Specifies network number and mask for DHCP clients
 network 10.0.0.0 255.255.255.0
! Specifies the domain name for the client
 domain-name central
! Specifies DNS server that will respond to DHCP clients when they need to correlate
host ! name to ip address
 dns-server 10.0.0.2
!Specifies the NETBIOS WINS server
 netbios-name-server 10.0.0.2
!
interface GigabitEthernet0/0/0
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
```

## Remote Router

```
ip dhcp pool client
! Imports DHCP option parameters into DHCP server database
 import all
 network 20.0.0.0 255.255.255.0
!
interface GigabitEthernet0/0/0
 ip address dhcp
 duplex auto
 speed auto
```

## Configuring DHCP Address Allocation Using Option 82 Example

This example configures two DHCP classes. CLASS1 defines the group of DHCP clients whose address requests contain the relay agent information option with the specified hexadecimal values. CLASS2 defines the group of DHCP clients whose address requests contain the configured relay agent information suboptions. CLASS3 has no pattern configured and is treated as a “match to any” class. This type of class is useful for specifying a “default” class.

In the following example, the subnet of pool ABC has been divided into three ranges without further subnetting of the 10.0.20.0/24 subnet. If there is a DHCP Discover message from the 10.0.20.0/24 subnet with option 82 matching that of class CLASS1, an available address in the range from 10.0.20.1 to 10.0.20.100 will be allocated. If there is no free address in CLASS1's address range, the DHCP Discover message will be matched against CLASS2, and so on.

Thus, each class in the DHCP pool will be examined for a match in the order configured by the user. In pool ABC, the order of matching is CLASS1, CLASS2, and finally CLASS3. In pool DEF, class CLASS2 does not have any address range configured. By default, the address range for a particular class is the pool's entire subnet(s). Therefore, clients matching CLASS2 may be allocated addresses from 11.0.20.1 to 11.0.20.254.

Multiple pools can be configured with the same class, eliminating the need to configure the same patterns in multiple pools. In the future, further classification method may be implemented. For example, there may be a need to specify that one or more pools should only be used to service a particular class of devices (for example, cable modems and IP phones).

```
! Defines the DHCP classes and relay information patterns
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 0000000000000000000000FF
ip dhcp class CLASS2
 relay agent information
  relay-information hex 01040102030402020102
  relay-information hex 01040101030402020102
ip dhcp class CLASS3
 relay agent information
! Associates the DHCP pool with DHCP classes
ip dhcp pool ABC
 network 10.0.20.0 255.255.255.0
 class CLASS1
  address range 10.0.20.1 10.0.20.100
class CLASS2
  address range 10.0.20.101 10.0.20.200
 class CLASS3
  address range 10.0.20.201 10.0.20.254
ip dhcp pool DEF
 network 11.0.20.0 255.255.255.0
 class CLASS1
  address range 11.0.20.1 11.0.20.64
 class CLASS2
```

## Configuring a Static Route with the Next-Hop Dynamically Obtained Through DHCP Example

The following example shows how to configure two GigabitEthernet interfaces to obtain the next-hop router IP address from the DHCP server:

```
ip route 10.10.10.0 255.255.255.0 dhcp 200
ip route 10.10.20.1 255.255.255.255 gigaether 1 dhcp
```

# Additional References

The following sections provide references related to the Cisco IOS XE DHCP server.

## Related Documents

| Related Topic | Document Title |
|---|---|
| DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |
| DHCP conceptual information | "DHCP Overview" module |
| DHCP relay agent configuration | "Configuring the Cisco IOS XE DHCP Relay Agent" module |
| DHCP client configuration | "Configuring the Cisco IOS XE DHCP Client" module |
| DHCP On-Demand Address Pool Manager | "Configuring the DHCP On-Demand Address Pool Manager" module |

## Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this functionality. | -- |

## MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

## RFCs

| RFCs | Title |
|---|---|
| RFC 951 | *Bootstrap Protocol (BOOTP)* |
| RFC 1542 | *Clarifications and Extensions for the Bootstrap Protocol* |
| RFC 2131 | *Dynamic Host Configuration Protocol* |

| RFCs | Title |
|---|---|
| RFC 2132 | *DHCP Options and BOOTP Vendor Extensions* |

### Technical Assistance

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

# Feature Information for the Cisco IOS XE DHCP Server

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 3 Feature Information for the Cisco IOS XE DHCP Server*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Server | Cisco IOS XE Release 2.1 | Cisco routers running Cisco IOS XE software include Dynamic Host Configuration Protocol (DHCP) server and relay agent software. The Cisco IOS XE DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. The DHCP server can be configured to assign additional parameters such as the IP address of the domain name system (DNS) server and the default router. |
| DHCP Address Allocation Using Option 82 | Cisco IOS XE Release 2.1 | The Cisco IOS XE DHCP server can allocate dynamic IP addresses based on the relay information option (option 82) information sent by the relay agent.<br>The following commands were introduced by this feature: **address range**, **class**, **ip dhcp class**, **ip dhcp use class**, **relay agent information**, **relay-information hex**. |
| DHCP Statically Configured Routes Using a DHCP Gateway | Cisco IOS XE Release 2.1 | This feature enables the configuration of static routes that point to an assigned DHCP next hop router.<br>The following commands were modified by this feature: **ip route**, **show ip route**. |
| DHCP Server Options - Import and Autoconfiguration | Cisco IOS XE Release 2.3 | Options imported by multiple subsystems can co-exist in the DHCP address pool. When the session is terminated or the lease is released, the imported options are cleared. |

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# Configuring the DHCP Server On-Demand Address Pool Manager

The Cisco IOS XE DHCP server on-demand address pool (ODAP) manager is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses. When a Cisco IOS XE router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level. A DHCP pool configured in the router can also be used as an IP address pooling mechanism. The IP address pooling mechanism is configured in the router to specify the source of IP addresses for PPP peers.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for Configuring the DHCP Server On-Demand Address Pool Manager

Before you configure the ODAP manager, you should understand the concepts documented in the “DHCP Overview” module.

You must configure standard Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) unless you intend to use non-MPLS VPNs.

In order for the IP address pooling mechanism to work correctly, the VPN routing and forwarding instance (VRF) of the PPP session must match that configured on the pool. Typically this matching is done either by configuring the **ip vrf forwarding** *vrf-name* command on the virtual template interface, or if AAA is used to authorize the PPP user, it can be part of the user's profile configuration.

# Restrictions for Configuring the DHCP Server On-Demand Address Pool Manager

- The **ip dhcp excluded-address** global configuration command cannot be used to exclude addresses from VRF associated pools.
- The **vrf** DHCP pool configuration command is currently not supported for host pools.
- Attribute inheritance is not supported on VRF pools.
- A router can be configured as a subnet allocation server and a DHCP server at the same time with one restriction: separate pools must be created for subnet allocation and IP address assignment. An address pool cannot be used by DHCP for both subnet allocation and IP address assignment.

# Information About the DHCP Server On-Demand Address Pool Manager

## ODAP Manager Operation

ODAPs enable pools of IP addresses to be dynamically increased or reduced in size depending on the address utilization level. Once configured, the ODAP is populated with one or more subnets leased from a source server and is ready to serve address requests from DHCP clients or from PPP sessions. The source server can be a remote DHCP server or a RADIUS server (via AAA). Currently, only the Cisco Access Registrar RADIUS server supports ODAPs. Subnets can be added to the pool when a certain utilization level (high utilization mark) is achieved. When the utilization level falls below a certain level (low utilization mark), a subnet can be returned to the server from which it was originally leased. Summarized routes for each leased subnet must be inserted or removed from the related VRF with each addition or removal of subnets into the ODAP.

ODAPs support address assignment using DHCP for customers using private addresses such as in MPLS VPNs. VPNs allow the possibility that two pools in separate networks can have the same address space, with private network addresses, served by the same DHCP server. These IP addresses can be distinguished by a VPN identifier to help select the VPN to which the client belongs.

Each ODAP is configured and associated with a particular MPLS VPN. Cisco IOS XE software also supports non-MPLS VPN address pools by adding pool name support to the **peer default ip address dhcp-pool** *pool-name*command.

For MPLS VPNs, each VPN is associated with one or more VRFs. The VRF is a key element in the VPN technology because it maintains the routing information that defines a customer VPN site. This customer site is attached to a provider edge (PE) router. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

A PPP session belonging to a specific VPN is only allocated an address from the ODAP associated with that VPN. These PPP sessions are terminated on a Virtual Home Gateway (VHG)/PE router where the ODAP is configured. The VHG/PE router maps the remote user to the corresponding MPLS VPNs.

For PPP sessions, individual address allocation from an ODAP follows a First Leased subnet First (FLF) policy. FLF searches for a free address beginning on the first leased subnet, followed by a search on the second leased subnet if no free address is available in the first subnet, and so on. This policy provides the benefit of grouping the leased addresses over time to a set of subnets, which allows an efficient subnet release and route summarization.

However, the FLF policy differs from the normal DHCP address selection policy. Normal DHCP address selection takes into account the IP address of the receiving interface or the gateway address if it is nonzero. To support both policies, the DHCP server needs to be able to distinguish between a normal DHCP address request and an address request for a PPP client. The ODAP manager uses an IP address pooling mechanism for PPP that allows the DHCP server to distinguish between a normal DHCP address request and a request from a PPP client.

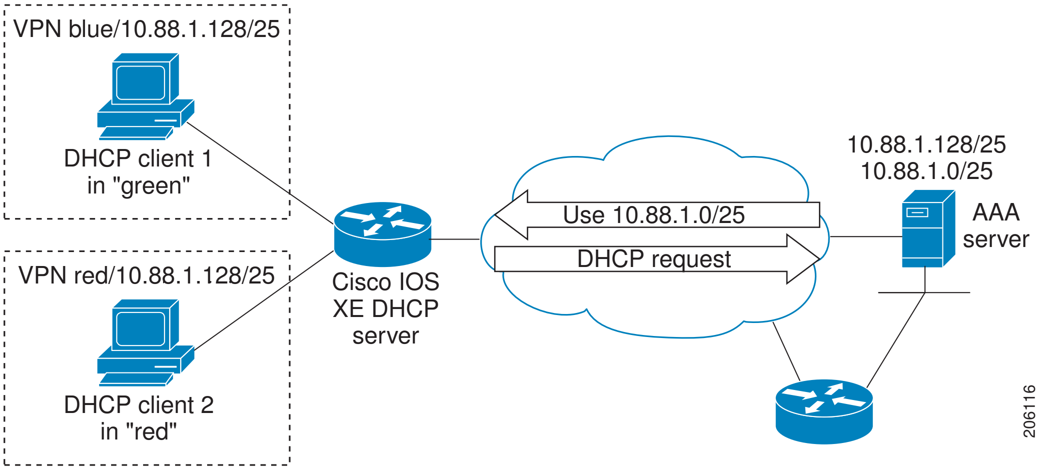
Subnet release from an ODAP follows a Last Leased subnet First (LLF) policy, which prefers the last leased subnet to be released first. This LLF policy searches for a releasable subnet (a subnet with no addresses currently being leased) starting with the last leased subnet. If a releasable subnet is found (candidate subnet), it is released, and the summarized route for that subnet is removed. If more than one releasable subnet exists at that time, only the most recently allocated is released. If there are no releasable subnets, no action is taken. If by releasing the candidate subnet, the high utilization mark is reached, the subnet is not released. The first leased subnet is never released (regardless of the instantaneous utilization level) until the ODAP is disabled.

When a DHCP pool receives multiple subnets from an upstream DHCP server, an address from each subnet is automatically configured on the client connected interface so that the addresses within the subnets can be requested by DHCP clients.

The first address in the first subnet is automatically assigned to the primary address on the interface. The first address of each subsequent subnet is assigned to secondary addresses on the interface. In addition, as client addresses are reclaimed, the count of lease addresses for that subnet is decremented. Once a lease counter for a subnet reaches zero (that is, lease expiry), the subnet is returned to the pool. The previous address on the interface is removed and the first secondary address on the interface is promoted as the primary address of the interface.

The figure below shows an ODAP manager configured on the Cisco IOS XE DHCP server. The ODAP requests an initial pool from the AAA server. Clients make DHCP requests and the DHCP server fulfills requests from the pool. When the utilization rate meets 90 percent, the ODAP manager requests an expansion and the AAA server allocates another subnet from which the ODAP manager can allocate addresses.

*Figure 3 ODAP Address Pool Management for MPLS VPNs*



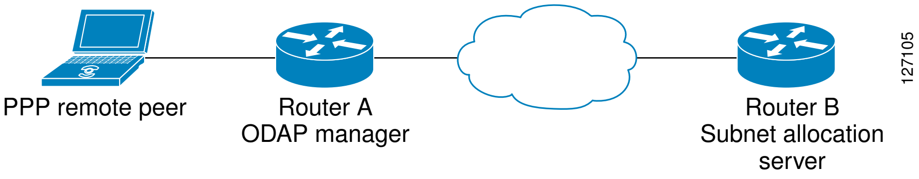
# Subnet Allocation Server Operation

You can also configure the ODAP manager to allocate subnets instead of individual IP addresses.

This capability allows the network operator to configure a Cisco IOS XE router as a subnet allocation server. The operation of a subnet allocation server is similar to the operation of a DHCP server, except that pools of subnets are created and assigned instead of pools of IP addresses. Subnet allocation pools are created and configured by using the **subnet prefix-length** command in DHCP pool configuration mode. The size of each assigned or allocated subnet is set by the *prefix-length* argument, using standard Common InterDomain Routing (CIDR) bit count notation to determine the number of addresses that are configured in each subnet lease.

When a DHCP server is configured as a subnet allocation server, it provides subnet allocation pools for ODAP manager allocation. In the figure below, Router B is the subnet allocation server and allocates subnets to the ODAP manager based on the demand for IP addresses and subnet availability. Router B is configured to allocate an initial amount of address space in the form of subnets to the ODAP manager. The size of the subnet allocated by the ODAP manager is determined by the subnet size that is configured on the subnet allocation server. The ODAP manager will then assign addresses to clients from these subnets and allocate more subnets as the need for address space increases.

*Figure 4 Subnet Allocation Server Topology*



When the ODAP manager allocates a subnet, the subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP manager requires the address space. The binding is removed and the subnet is returned to the subnet pool only when the ODAP manager releases the subnet as address space utilization decreases.

The subnet allocation server can also be associated with a VRF. A VRF consists of an IP routing table, a derived CEF table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

## Benefits of Using ODAPs

### Efficient Address Management

The ODAP manager allows customers to optimize their use of IP addresses, thus conserving address space.

### Efficient Route Summarization and Update

The ODAP manager inserts a summarized route when a subnet is added to the ODAP.

### Multiple VRF and Independent Private Addressing Support

The ODAP manager automatically injects subnet routing information into the appropriate VRF.

# How to Configure the DHCP Server On-Demand Address Pool Manager

## Defining DHCP ODAPs as the Global Default Mechanism

Perform this task to specify that the global default mechanism to use is on-demand address pooling.

IP addressing allows configuration of a global default address pooling mechanism. The DHCP server needs to be able to distinguish between a normal DHCP address request and an address request for a PPP client.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip address-pool dhcp-pool**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip address-pool dhcp-pool**<br>**Example:**<br>`Router(config)# ip address-pool dhcp-pool` | Enables on-demand address pooling as the global default IP address mechanism.<br>- For remote access (PPP) sessions into MPLS VPNs, IP addresses are obtained from locally configured VRF-associated DHCP pools. |

# Defining DHCP ODAPs on an Interface

Perform this task to configure on-demand address pools on an interface.

The interface on-demand address pooling configuration overrides the global default mechanism on that interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **peer default ip address dhcp-pool** [*pool-name*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br>**Example:**<br>`Router(config)# interface Virtual-Template1` | Specifies the interface and enters interface configuration mode. |
| Step 4 | **peer default ip address dhcp-pool** [*pool-name*]<br>**Example:**<br>`Router(config-if)# peer default ip address dhcp-pool mypool` | Specifies an IP address from an on-demand address pool to be returned to a remote peer connecting to this interface.<br>• The *pool-name* argument supports non-MPLS VPNs and is mandatory if the session is not associated with any VRF. Multiple pool names can be accepted but must be separated by white space. |

# Configuring the DHCP Pool as an ODAP

Perform this task to configure a DHCP address pool as an ODAP pool.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **vrf** *name*
5. **origin** {**dhcp** | **aaa**| **ipcp**} [**subnet size initial** *size* [**autogrow** *size*]]
6. **utilization mark low** *percentage-number*
7. **utilization mark high** *percentage-number*
8. **end**
9. **show ip dhcp pool** [*pool-name*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool red-pool` | Configures a DHCP address pool on a Cisco IOS XE DHCP server and enters DHCP pool configuration mode. |
| Step 4 | **vrf** *name*<br>**Example:**<br>`Router(dhcp-config)# vrf red` | (Optional) Associates the address pool with a VRF name.<br>- Only use this command for MPLS VPNs. |
| Step 5 | **origin** {**dhcp** \| **aaa**\| **ipcp**} [**subnet size initial** *size* [**autogrow** *size*]]<br>**Example:**<br>`Router(dhcp-config)# origin dhcp subnet size initial /16 autogrow /16` | Configures an address pool as an on-demand address pool.<br>- If you do not configure the pool as an autogrow pool, the pool will not request additional subnets if one subnet is already in the pool.<br>- You can enter size as either the subnet mask (nnnn.nnnn.nnnn.nnnn) or prefix size (/nn). The valid values are /0 and /4 to /30.<br>- When a DHCP pool receives multiple subnets from an upstream DHCP server, an address from each subnet is automatically configured on the client connected interface so that the addresses within the subnets can be requested by DHCP clients. The first address in the first subnet is automatically assigned to the primary address on the interface. The first address of each subsequent subnet is assigned to secondary addresses on the interface. In addition, as client addresses are reclaimed, the count of lease addresses for that subnet is decremented. Once a lease counter for a subnet reaches zero (that is, lease expiry), the subnet is returned to the pool. The previous address on the interface is removed and the first secondary address on the interface is promoted as the primary address of the interface.<br>- If the **origin aaa** option is configured, AAA must be configured. |
| Step 6 | **utilization mark low** *percentage-number*<br>**Example:**<br>`Router(dhcp-config)# utilization mark low 40` | Sets the low utilization mark of the pool size.<br>- This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured.<br>- The default value is 0 percent. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **utilization mark high** *percentage-number*<br>**Example:**<br>`Router(dhcp-config)# utilization mark high 60` | Sets the high utilization mark of the pool size.<br>• This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured.<br>• The default value is 100 percent. |
| **Step 8** | **end**<br>**Example:**<br>`Router(dhcp-config)# end` | Returns to global configuration mode. |
| **Step 9** | **show ip dhcp pool** [*pool-name*]<br>**Example:**<br>`Router# show ip dhcp pool` | (Optional) Displays information about DHCP address pools.<br>• Information about the primary and secondary interface address assignment is also displayed. |

# Configuring ODAPs to Obtain Subnets Through IPCP Negotiation

Perform this task to configure your router to use subnets obtained through IP Control Protocol (IPCP) negotiation.

You can assign IP address pools to customer premises equipment (CPE) devices, which, in turn, assign IP addresses to the CPE and to a DHCP pool. This functionality has three requirements:

- The Cisco IOS XE CPE device must be able to request and use the subnet.
- The RADIUS server (via AAA) must be able to provide that subnet and insert the framed route into the proper VRF table.
- The PE router must be able to facilitate providing the subnet through (IPCP) negotiation.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **import all**
5. **origin ipcp**
6. **exit**
7. **interface** *type number*
8. **ip address pool** *pool-name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool red-pool` | Configures a DHCP address pool on a Cisco IOS XE DHCP server and enters DHCP pool configuration mode. |
| Step 4 | **import all**<br>**Example:**<br>`Router(dhcp-config)# import all` | Imports option parameters into the Cisco IOS XE DHCP server database. |
| Step 5 | **origin ipcp**<br>**Example:**<br>`Router(dhcp-config)# origin ipcp` | Configures an address pool as an on-demand address pool using IPCP as the subnet allocation protocol. |
| Step 6 | **exit**<br>**Example:**<br>`Router(dhcp-config)# exit` | Exits DHCP pool configuration mode. |
| Step 7 | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/0` | Specifies the interface and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 8 | **ip address pool** *pool-name*<br>**Example:**<br>`Router(config-if)# ip address pool red-pool` | Specifies that the interface IP address will be automatically configured from the named pool, when the pool is populated with a subnet from IPCP. |

# Configuring AAA

Perform this task to configure AAA.

To allow ODAP to obtain subnets from the AAA server, the AAA client must be configured on the VHG/PE router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization configuration default group radius**
5. Do one of the following:
   - **aaa accounting network default start-stop group radius**
   - or
   - **aaa accounting network default stop-only group radius**
6. **aaa session-id common**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **aaa new-model**<br>**Example:**<br>`Router(config)# aaa new-model` | Enables AAA access control. |
| Step 4 | **aaa authorization configuration default group radius**<br>**Example:**<br>`Router(config)# aaa authorization configuration default group radius` | Downloads static route configuration information from the AAA server using RADIUS. |
| Step 5 | Do one of the following:<br>• **aaa accounting network default start-stop group radius**<br>• or<br>• **aaa accounting network default stop-only group radius**<br>**Example:**<br>`Router(config)# aaa accounting network default start-stop group radius`<br>**Example:**<br>**Example:**<br>`Router(config)# aaa accounting network default stop-only group radius` | Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. Sends a “start” accounting notice at the beginning of a process.<br>or<br>Enables AAA accounting of requested services for billing or security purposes when you use RADIUS. Sends a “stop” accounting notice at the end of the requested user process. |
| Step 6 | **aaa session-id common**<br>**Example:**<br>`Router(config)# aaa session-id common` | Ensures that the same session ID will be used for each AAA accounting service type within a call. |

# Configuring RADIUS

- ODAP AAA Profile, page 55

## ODAP AAA Profile

The AAA server sends the RADIUS Cisco AV pair attributes “pool-addr” and “pool-mask” to the Cisco IOS XE DHCP server in the access request and access accept. The pool-addr attribute is the IP address and the pool-mask attribute is the network mask (for example, pool-addr=192.168.1.0 and pool-mask=255.255.0.0). Together, these attributes make up a network address (address/mask) that is allocated by the AAA server to the Cisco IOS XE DHCP server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip radius source-interface** *subinterface-name*
4. **radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number*
5. **radius server attribute 32 include-in-access-req**
6. **radius server attribute 44 include-in-access-req**
7. **radius-server vsa send accounting**
8. **radius-server vsa send authentication**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip radius source-interface** *subinterface-name*<br>**Example:**<br>`Router(config)#`<br>`ip radius source-interface GigabitEthernet0/0/0` | Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number*<br>**Example:**<br>`Router(config)#`<br>`radius-server host 172.16.1.1 auth-port 1645 acct-port 1646` | Specifies a RADIUS server host.<br>• The *ip-address* argument specifies the IP address of the RADIUS server host. |
| **Step 5** | **radius server attribute 32 include-in-access-req**<br>**Example:**<br>`Router(config)#`<br>`radius server attribute 32 include-in-access-req` | Sends RADIUS attribute 32 (NAS-Identifier) in an access request or accounting request. |
| **Step 6** | **radius server attribute 44 include-in-access-req**<br>**Example:**<br>`Router(config)#`<br>`radius server attribute 44 include-in-access-req` | Sends RADIUS attribute 44 (Accounting Session ID) in an access request or accounting request. |
| **Step 7** | **radius-server vsa send accounting**<br>**Example:**<br>`Router(config)#`<br>`radius-server vsa send accounting` | Configures the network access server (NAS) to recognize and use vendor-specific accounting attributes. |
| **Step 8** | **radius-server vsa send authentication**<br>**Example:**<br>`Router(config)#`<br>`radius-server vsa send authentication` | Configures the NAS to recognize and use vendor-specific authentication attributes. |

# Disabling ODAPs

This task shows how to disable an ODAP from a DHCP pool.

When an ODAP is disabled, all leased subnets are released. If active PPP sessions are using addresses from the released subnets, those sessions will be reset. DHCP clients leasing addresses from the released subnets will not be able to renew their leases.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **no origin** {**dhcp**| **aaa**| **ipcp**}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool red-pool` | Configures a DHCP address pool on a Cisco IOS XE DHCP server and enters DHCP pool configuration mode. |
| **Step 4** | **no origin** {**dhcp**\| **aaa**\| **ipcp**}<br>**Example:**<br>`Router(dhcp-config)# no origin dhcp` | Disables the ODAP. |

# Verifying ODAP Operation

Perform this task to verify ODAP operation.

### SUMMARY STEPS

1. **enable**
2. **show ip dhcp pool** [*pool-name*] The following output is for two DHCP pools: Green and Global. Pool Green is configured with a high utilization mark of 50 and a low utilization mark of 30. The pool is also configured to obtain more subnets when the high utilization mark is reached (autogrow). The Subnet size field indicates the values configured in the **origin** command as the initial and incremental subnet sizes that would be requested by the pool named Green. The Total addresses field is a count of all the usable addresses in the pool. The Leased addresses field is a total count of how many bindings were created from the pool. The Pending event field shows subnet request, which means that a subnet request is pending for the pool. The subnet request was scheduled because the Leased addresses count has exceeded the high utilization level of the pool. Subnets currently added to pool Green are shown in sequence. The Current index column shows the address that would be allocated next from this subnet. The IP address range column shows the range of usable addresses from the subnet. The Leased addresses column shows individual count of bindings created from each subnet. Three subnets are currently added to pool Green. The first two subnets have used all their addresses and thus the Current index is showing 0.0.0.0. Notice that pool Green and pool Global can have the same subnet (172.16.0.1-172.16.0.6) because pool Green is configured to be in VRF Green, while pool Global is configured to be in the global address space.
3. **show ip dhcp binding** The following output shows the bindings from pool Green. The Type field shows On-demand, which indicates that the address binding was created for a PPP session. The Lease expiration field shows Infinite, which means that the binding is valid as long as the session is up. If a subnet must be released back to the leasing server while the session is still up, the session is reset so that it will be forced to obtain a new IP address. The Hardware address column for an On-demand entry shows the identifier for the session as detected by PPP. There are no bindings shown under the Bindings from all pools not associated with VRF field because the Global pool has not allocated any addresses.

### DETAILED STEPS

**Step 1** **enable**

Enables privileged EXEC mode. Enter your password if prompted.

**Example:**

```
Router> enable
```

**Step 2** **show ip dhcp pool** [*pool-name*] The following output is for two DHCP pools: Green and Global. Pool Green is configured with a high utilization mark of 50 and a low utilization mark of 30. The pool is also configured to obtain more subnets when the high utilization mark is reached (autogrow). The Subnet size field indicates the values configured in the **origin** command as the initial and incremental subnet sizes that would be requested by the pool named Green. The Total addresses field is a count of all the usable addresses in the pool. The Leased addresses field is a total count of how many bindings were created from the pool. The Pending event field shows subnet request, which means that a subnet request is pending for the pool. The subnet request was scheduled because the Leased addresses count has exceeded the high utilization level of the pool. Subnets currently added to pool Green are shown in sequence. The Current index column shows the address that would be allocated next from this subnet. The IP address range column shows the range of usable addresses from the subnet. The Leased addresses column shows individual count of bindings created from each subnet. Three subnets are currently added to pool Green. The first two subnets have used all their addresses and thus the Current index is showing 0.0.0.0. Notice that pool Green and pool Global can have the same subnet (172.16.0.1-172.16.0.6) because pool Green is configured to be in VRF Green, while pool Global is configured to be in the global address space.

**Example:**

```
Router# show ip dhcp pool
Pool Green :
 Utilization mark (high/low)    : 50 / 30
 Subnet size (first/next)       : 24 / 24 (autogrow)
 VRF name                       : Green
 Total addresses                : 18
 Leased addresses               : 13
 Pending event                  : subnet request
 3 subnets are currently in the pool :
 Current index        IP address range                    Leased addresses
 0.0.0.0              172.16.0.1       - 172.16.0.6        6
 0.0.0.0              172.16.0.9       - 172.16.0.14       6
 172.16.0.18          172.16.0.17      - 172.16.0.22       1
Pool Global :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 24 / 24 (autogrow)
 Total addresses                : 6
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 172.16.0.1           172.16.0.1       - 172.16.0.6        0
```

**Step 3** **show ip dhcp binding** The following output shows the bindings from pool Green. The Type field shows On-demand, which indicates that the address binding was created for a PPP session. The Lease expiration field shows Infinite, which means that the binding is valid as long as the session is up. If a subnet must be released back to the leasing server while the session is still up, the session is reset so that it will be forced to obtain a new IP address. The Hardware address column for an On-demand entry shows the identifier for the session as detected by PPP. There are no bindings shown under the Bindings from all pools not associated with VRF field because the Global pool has not allocated any addresses.

**Example:**

```
Router# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address       Hardware address        Lease expiration        Type
Bindings from VRF pool Green:
IP address       Hardware address        Lease expiration        Type
172.16.0.1       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3930.39
172.16.0.2       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3839.31
172.16.0.3       5674.312d.7465.7374.    Infinite                On-demand
                 2d36.3432.34
172.16.0.4       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3236.34
172.16.0.5       5674.312d.7465.7374.    Infinite                On-demand
                 2d34.3331.37
172.16.0.6       5674.312d.7465.7374.    Infinite                On-demand
                 2d37.3237.39
172.16.0.9       5674.312d.7465.7374.    Infinite                On-demand
                 2d39.3732.36
172.16.0.10      5674.312d.7465.7374.    Infinite                On-demand
                 2d31.3637
172.16.0.11      5674.312d.7465.7374.    Infinite                On-demand
                 2d39.3137.36
172.16.0.12      5674.312d.7465.7374.    Infinite                On-demand
                 2d37.3838.30
172.16.0.13      5674.312d.7465.7374.    Infinite                On-demand
                 2d32.3339.37
172.16.0.14      5674.312d.7465.7374.    Infinite                On-demand
                 2d31.3038.31
172.16.0.17      5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3832.38
```

```
172.16.0.18      5674.312d.7465.7374.    Infinite               On-demand
                 2d32.3735.31
```

- Troubleshooting Tips, page 60

## Troubleshooting Tips

By default, the Cisco IOS XE DHCP server on which the ODAP manager is based attempts to verify an address availability by performing a ping operation to the address before allocation. The default DHCP ping configuration will wait for 2 seconds for an ICMP echo reply. This default configuration results in the DHCP server servicing one address request every 2 seconds. The number of ping packets being sent and the ping timeout are configurable. Thus, to reduce the address allocation time, you can reduce either the timeout or the number of ping packets sent. Reducing the timeout or the ping packets being sent will improve the address allocation time, at the cost of less ability to detect duplicate addresses.

Each ODAP will make a finite number of attempts (up to four retries) to obtain a subnet from DHCP or AAA. If these attempts are not successful, the subnet request from the pool automatically starts when there is another individual address request to the pool (for example, from a newly brought up PPP session). If a pool has not been allocated any subnets, you can force restarting the subnet request process by using the **clear ip dhcp pool** *pool-name* **subnet *** EXEC command.

# Monitoring and Maintaining the ODAP

This task shows how to monitor and maintain the ODAP.

Note the following behavior for the **clear ip dhcp binding**, **clear ip dhcp conflict**, and **clear ip dhcp subnet** commands:

- If you do not specify the **pool** *pool-name* option and an IP address is specified, it is assumed that the IP address is an address in the global address space and will look among all the non-VRF DHCP pools for the specified binding/conflict/subnet.
- If you do not specify the **pool** *pool-name* option and the * option is specified, it is assumed that all automatic/ or on-demand bindings/conflicts/subnets in all VRF and non-VRF pools are to be deleted.
- If you specify both the **pool** *pool-name* option and the * option, all automatic or on-demand bindings/ conflicts/subnets in the specified pool only will be cleared.
- If you specify the **pool** *pool-name* option and an IP address, the specified binding/conflict or the subnet containing the specified IP address will be deleted from the specified pool.

### SUMMARY STEPS

1. **enable**
2. **clear ip dhcp** [**pool** *pool-name*] **binding** {***** | *address*}
3. **clear ip dhcp** [**pool** *pool-name*] **conflict** {***** | *address*}
4. **clear ip dhcp** [**pool** *pool-name*] **subnet**{*****| *address*}
5. **debug dhcp details**
6. **debug ip dhcp server events**
7. **show ip dhcp import**
8. **show ip interface** [*type number*]
9. **show ip dhcp pool** *pool-name*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **clear ip dhcp** [**pool** *pool-name*] **binding** {***** \| *address*}<br>**Example:**<br>`Router# clear ip dhcp binding *` | Deletes an automatic address binding or objects from a specific pool from the DHCP server database. |
| **Step 3** | **clear ip dhcp** [**pool** *pool-name*] **conflict** {***** \| *address*}<br>**Example:**<br>`Router# clear ip dhcp conflict *` | Clears an address conflict or conflicts from a specific pool from the DHCP server database. |
| **Step 4** | **clear ip dhcp** [**pool** *pool-name*] **subnet**{*****\| *address*}<br>**Example:**<br>`Router# clear ip dhcp subnet *` | Clears all currently leased subnets in the named DHCP pool or all DHCP pools if *name* is not specified. |
| **Step 5** | **debug dhcp details**<br>**Example:**<br>`Router# debug dhcp details` | Monitors the subnet allocation/releasing in the on-demand address pools. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **debug ip dhcp server events**<br>**Example:**<br>`Router# debug ip dhcp server events` | Reports DHCP server events, like address assignments and database updates. |
| **Step 7** | **show ip dhcp import**<br>**Example:**<br>`Router# show ip dhcp import` | Displays the option parameters that were imported into the DHCP server database. |
| **Step 8** | **show ip interface** [*type number*]<br>**Example:**<br>`Router# show ip interface` | Displays the usability status of interfaces configured for IP. |
| **Step 9** | **show ip dhcp pool** *pool-name*<br>**Example:**<br>`Router# show ip dhcp pool green` | Displays DHCP address pool information. |

# How to Configure DHCP ODAP Subnet Allocation Server Support

## Configuring a Global Pool on a Subnet Allocation Server

Perform this task to configure a global subnet pool on a subnet allocation server.

### Global Subnet Pools

Global subnet pools are created in a centralized network. The ODAP manager allocates subnets from the subnet allocation server based on subnet availability. When the ODAP manager allocates a subnet, the subnet allocation server creates a subnet binding. This binding is stored in the DHCP database for as long as the ODAP manager requires the address space. The binding is destroyed and the subnet is returned to the subnet pool only when the ODAP manager releases the subnet as address space utilization decreases.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **network** *network-number* [*mask*| / *prefix-length*]
5. **subnet prefix-length** *prefix-length*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool GLOBAL-POOL` | Enters DHCP pool configuration mode and specifies the subnet pool name. |
| **Step 4** | **network** *network-number* [*mask*| / *prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# network 10.0.0.0 255.255.255.0` | Configures the subnet number and mask for a DHCP address pool on a Cisco IOS XE DHCP server.<br>• The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length* argument. |
| **Step 5** | **subnet prefix-length** *prefix-length*<br>**Example:**<br>`Router(dhcp-config)# subnet prefix-length 8` | Configures the subnet prefix length. The range of the *prefix-length* argument is from 1 to 31.<br>• This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation format. |

# Configuring a VRF Subnet Pool on a Subnet Allocation Server

## VRF Subnet Pools

A subnet allocation server can be configured to assign subnets from VRF subnet allocation pools for MPLS VPN clients. VPN routes between the ODAP manager and the subnet allocation server are configured based on VRF name or VPN ID configuration. The VRF and VPN ID are configured to maintain routing information that defines customer VPN sites. The VPN customer site (or Customer Equipment [CE]) is attached to a provider edge (PE) router. The VRF is used to specify the VPN and consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

The VRF name and VPN ID can be configured on the ODAP manager and subnet allocation server prior to the configuration of the subnet allocation pool.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **vrf** vrf-name
5. **network** *network-number* [*mask* |*/prefix-length*]
6. **subnet prefix-length** *prefix-length*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool VRF-POOL` | Enters DHCP pool configuration mode and specifies the subnet pool name. |
| **Step 4** | **vrf** vrf-name<br>**Example:**<br>`Router(dhcp-config)# vrf RED` | Associates the on-demand address pool with a VPN routing and forwarding (VRF) instance name (or tag).<br>• The **vrf**keyword and *vrf-name* argument are used to specify the VPN for the VRF pool. The *vrf-name* argument must match the VRF name (or tag) that is configured for the client. |
| **Step 5** | **network** *network-number* [*mask* \|/*prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# network 10.1.1.0 /24` | Configures the subnet number and mask for a DHCP address pool on a Cisco IOS XE DHCP server.<br>• The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length* argument. |
| **Step 6** | **subnet prefix-length** *prefix-length*<br>**Example:**<br>`Router(dhcp-config)# subnet prefix-length 16` | Configures the subnet prefix length. The range of the *prefix-length* argument is from 1 to 31.<br>• This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation format. |

# Using a VPN ID to Configure a VRF Subnet Pool on a Subnet Allocation Server

Perform this task to configure a VRF subnet pool, using a VPN ID, on a subnet allocation server.

- VRF Pools and VPN IDs, page 65

## VRF Pools and VPN IDs

A subnet allocation server can also be configured to assign subnets from VPN subnet allocation pools based on the VPN ID of a client. The VPN ID (or Organizational Unique Identifier [OUI]) is a unique identifier assigned by the IEEE.

The VRF name and VPN ID can be configured on the ODAP manager and subnet allocation server prior to the configuration of the subnet allocation pool.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf vrf-name**
4. **rd** *route-distinguisher*
5. **route-target both** route-target-number
6. **vpn id** vpn-id
7. **exit**
8. **ip dhcp pool** pool-name
9. **vrf** vrf-name
10. **network** *network-number* [*mask* |*/prefix-length*]
11. **subnet prefix-length** *prefix-length*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip vrf vrf-name**<br>**Example:**<br>`Router(config)#ip vrf RED` | Creates a VRF routing table and specifies the VRF name (or tag).<br>• The *vrf-name* argument must match the VRF name that is configured for the client and VRF pool in Step 9. |
| **Step 4** | **rd** *route-distinguisher*<br>**Example:**<br>`Router(config-vrf)# rd 100:1` | Creates routing and forwarding tables for a VRF instance created in Step 3.<br>• There are two formats for configuring the route distinguisher argument. It can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn). |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **route-target both** route-target-number<br>**Example:**<br>`Router(config-vrf)# route-target both 100:1` | Creates a route-target extended community for the VRF instance that was created in Step 3.<br>• The **both** keyword is used to specify which routes should be imported and exported to the target VPN extended community (or the ODAP manager in this configuration).<br>• The *route-target-number*argument follows the same format as the *route-distinguisher* argument in Step 4. These two arguments must match. |
| **Step 6** | **vpn id** vpn-id<br>**Example:**<br>`Router(config-vrf)# vpn id 1234:123456` | Configures the VPN ID.<br>• This command is only used if the client (ODAP manager) is also configured with or assigned a VPN ID. |
| **Step 7** | **exit**<br>**Example:**<br>`Router(config-vrf)# exit` | Exits VRF configuration mode and enters global configuration mode. |
| **Step 8** | **ip dhcp pool** pool-name<br>**Example:**<br>`Router(config)# ip dhcp pool VPN-POOL` | Enters DHCP pool configuration mode and specifies the subnet pool name.<br>• The **VRF**keyword and *vrf-name* argument are used to specify the VPN for the VRF pool. The *vrf-name* argument must match the VRF name (or tag) that is configured for the client. |
| **Step 9** | **vrf** vrf-name<br>**Example:**<br>`Router(dhcp-config)#vrf RED` | Associates the on-demand address pool with a VRF instance name.<br>• The *vrf-name* argument must match the *vrf-name* argument that was configured in Step 3. |
| **Step 10** | **network** *network-number* [*mask* \|/ *prefix-length*]<br>**Example:**<br>`Router(dhcp-config)# network 192.168.0.0 /24` | Configures the subnet number and mask for a DHCP address pool on a Cisco IOS XE DHCP server.<br>• The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length* argument. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **subnet prefix-length** *prefix-length*<br>**Example:**<br>`Router(dhcp-config)# subnet prefix-length 16` | Configures the subnet prefix length.<br>• The range of the *prefix-length* argument is from 1 to 31.<br>• This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation format. |

# Verifying the Subnet Allocation and DHCP Bindings

Perform this task to verify subnet allocation and DHCP bindings.

The **show ip dhcp pool** and **show ip dhcp binding**commands do not need to be issued together or even in the same session as there are differences in the information that is provided. These commands, however, can be used to display and verify subnet allocation and DHCP bindings. The **show running-config | begin dhcp** command is used to display the local configuration of DHCP and the configuration of the **subnet prefix-length** command.

### SUMMARY STEPS

1. **enable**
2. **show running-config** | begin dhcp
3. **show ip dhcp pool [pool-name]**
4. **show ip dhcp binding [ip-address]**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show running-config** \| begin dhcp<br>**Example:**<br>`Router# show running-config \| begin dhcp` | Used to display the local configuration of the router.<br>• The configuration of the **subnet prefix-length** command will be displayed under the DHCP pools, for which subnet lease allocation has been configured. The subnet allocation size will be shown, following this command, in CIDR bit count notation.<br>• The sample output is filtered with the **begin** keyword to start displaying output at the DHCP section of the running configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **show ip dhcp pool [pool-name]**<br>**Example:**<br>`Router# show ip dhcp pool` | Displays information about DHCP pools.<br>• This command can be used to verify subnet allocation pool configuration on both the subnet allocation server and the ODAP manager.<br>• The output of this command displays specific address pool information, including the name of the pool, utilization of address space, subnet size, number of total addresses, number of leased address, and pending events. |
| **Step 4** | **show ip dhcp binding [ip-address]**<br>**Example:**<br>`Router# show ip dhcp binding` | Displays information about DHCP bindings.<br>• This command can be used to display subnet allocation to DHCP binding mapping information.<br>• The output from this command displays binding information for individual IP address assignment and allocated subnets. The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet). Bindings for individual IP address only display an IP address and are not followed by a subnet mask. |

# Troubleshooting the DHCP ODAP Subnet Allocation Server

Perform this task to troubleshoot the DHCP ODAP subnet allocation server.

### SUMMARY STEPS

1. **enable**
2. **debug dhcp** [**detail**]
3. **debug ip dhcp server** {**events** | **packets** | **linkage**}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **debug dhcp** [**detail**]<br>**Example:**<br>`Router# debug dhcp detail` | Displays debugging information about DHCP client activities and monitors the status of DHCP packets.<br>• This example is issued with the **detail**keyword on the ODAP manager. The **detail**keyword is used to display and monitor the lease entry structure of the client and the state transitions of lease entries. This command also displays the values of the op, htype, hlen, hops, server identifier option, xid, secs, flags, ciaddr, yiaddr, siaddr, and giaddr fields of the DHCP packet that are shown in addition to the length of the options field. |
| **Step 3** | **debug ip dhcp server** {**events** \| **packets** \| **linkage**}<br>**Example:**<br>`Router# debug ip dhcp server packets`<br>**Example:**<br>`Router# debug ip dhcp server events` | Enables DHCP server debugging.<br>• This example is issued with the **packets** and events keywords on the subnet allocation server. The output displays lease transition and reception, as well as database information. |

# Configuration Examples for DHCP Server On-Demand Address Pool Manager

## Defining DHCP ODAPs as the Global Default Mechanism Example

The following example shows how to configure the on-demand address pooling mechanism to be used to serve an address request from a PPP client.

```
ip address-pool dhcp-pool
```

```
!
ip dhcp pool Green-pool
```

## Defining DHCP ODAPs on an Interface Example

The following example shows how to configure an interface to retrieve an IP address from an on-demand address pool:

```
interface Virtual-Template1
 ip vrf forwarding green
 ip unnumbered loopback1
 ppp authentication chap
 peer default ip address dhcp-pool
!
```

## Configuring the DHCP Pool as an ODAP Example

The following example shows two ODAPs configured to obtain their subnets from an external DHCP server:

```
Router# show run
Building configuration...
Current configuration : 3943 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
no logging console
enable password lab
!
username vpn_green_net1 password 0 lab
username vpn_red_net1 password 0 lab
ip subnet-zero
!
ip dhcp pool green_pool
   vrf Green
   utilization mark high 60
   utilization mark low 40
   origin dhcp subnet size initial /24 autogrow /24
!
ip dhcp pool red_pool
   vrf Red
   origin dhcp
!
ip vrf Green
 rd 200:1
 route-target export 200:1
 route-target import 200:1
!
ip vrf Red
 rd 300:1
 route-target export 300:1
 route-target import 300:1
ip cef
ip address-pool dhcp-pool
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Loopback1
```

```
 ip vrf forwarding Green
 ip address 100.10.10.1 255.255.255.255
!
interface Loopback2
 ip vrf forwarding Red
 ip address 110.10.10.1 255.255.255.255
!
interface ATM2/0/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface ATM3/0/0
 no ip address
 no atm ilmi-keepalive
!
interface GigabitEthernet0/0/0
 ip address 10.0.105.12 255.255.255.224
 duplex half
!
interface GigabitEthernet0/0/1
 ip address 150.10.10.1 255.255.255.0
 duplex half
!
interface GigabitEthernet0/0/2
 ip address 120.10.10.1 255.255.255.0
 duplex half
 tag-switching ip
!
interface Virtual-Template1
 ip vrf forwarding Green
 ip unnumbered Loopback1
 ppp authentication chap
!
interface Virtual-Template2
 ip vrf forwarding Green
 ip unnumbered Loopback1
 ppp authentication chap
!
interface Virtual-Template3
 ip vrf forwarding Green
 ip unnumbered Loopback1
 ppp authentication chap
!
interface Virtual-Template4
 ip vrf forwarding Red
 ip unnumbered Loopback2
 ppp authentication chap
!
interface Virtual-Template5
 ip vrf forwarding Red
 ip unnumbered Loopback2
 ppp authentication chap
!
interface Virtual-Template6
 ip vrf forwarding Red
 ip unnumbered Loopback2
 ppp authentication chap
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 1.1.1.1 0.0.0.0 area 0
 network 120.10.10.0 0.0.0.255 area 0
 network 150.10.10.0 0.0.0.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family ipv4 vrf Red
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 110.0.0.0
 exit-address-family
 !
 address-family ipv4 vrf Green
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 100.0.0.0
 exit-address-family
 !
 address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
 exit-address-family
!
ip classless
ip route 172.19.0.0 255.255.0.0 10.0.105.1
no ip http server
ip pim bidir-enable
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
 login
!
end
```

# Configuring the DHCP Pool as an ODAP for Non-MPLS VPNs Example

The following example shows how to configure an interface to retrieve an IP address from an on-demand address pool. In this example, two non-VRF ODAPs are configured. There are two virtual-templates and two DHCP address pools, usergroup1 and usergroup2. Each virtual-template interface is configured to obtain IP addresses for the peer from the associated address pool.

```
!
ip dhcp pool usergroup1
 origin dhcp subnet size initial /24 autogrow /24
 lease 0 1
!
ip dhcp pool usergroup2
 origin dhcp subnet size initial /24 autogrow /24
 lease 0 1
!
interface virtual-template1
 ip unnumbered loopback1
 peer default ip address dhcp-pool usergroup1
!
interface virtual-template2
 ip unnumbered loopback1
 peer default ip address dhcp-pool usergroup2
```

# Configuring AAA and RADIUS Example

The following example shows one pool “Green” configured to obtain its subnets from the AAA (RADIUS) server located at IP address 172.16.1.1:

```
!
aaa new-model
!
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa session-id common
!
ip subnet-zero
!
ip dhcp ping packets 0
!
ip dhcp pool Green
 vrf Green
 utilization mark high 50
 utilization mark low 30
 origin aaa subnet size initial /28 autogrow /28
!
ip vrf Green
 rd 300:1
 route-target export 300:1
 route-target import 300:1
!
interface GigabitEthernet0/1/1
 ip address 172.16.1.12 255.255.255.0
 duplex half
!
interface Virtual-Template1
 ip vrf forwarding Green
 no ip address
!
ip radius source-interface GigabitEthernet0/1/1
!
!IP address of the RADIUS server host
radius-server host 172.16.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 32 include-in-access-req
radius-server attribute 44 include-in-access-req
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

# Configuring a Global Pool for a Subnet Allocation Server Example

The following example shows how to configure a router to be a subnet allocation server and create a global subnet allocation pool named “GLOBAL-POOL” that allocates subnets from the 10.0.0.0/24 network. The configuration of the **subnet prefix-length** command in this example configures the size of each subnet that is allocated from the subnet pool to support 254 host IP addresses.

```
ip dhcp pool GLOBAL-POOL
 network 10.0.0.0 255.255.255.0
 subnet prefix-length 24
!
```

# Configuring a VRF Pool for a Subnet Allocation Server Example

The following example shows how to configure a router to be a subnet allocation server and create a VRF subnet allocation pool named “VRF-POOL” that allocates subnets from the 172.16.0.0/16 network and configures the VPN to match the VRF named “RED.” The configuration of the **subnet prefix-length** command in this example configures the size of each subnet that is allocated from the subnet pool to support 62 host IP addresses.

```
 ip dhcp pool VRF-POOL
 vrf RED
 network 172.16.0.0 /16
 subnet prefix-length 26
!
```

# Using a VPN ID to Configure a VRF Pool on a Subnet Allocation Server Example

The following example shows how to configure a router to be a subnet allocation server and create a VRF subnet allocation pool named “VRF-POOL” that allocates subnets from the 192.168.0.0/24 network and configures the VRF named “RED.” The VPN ID must match the unique identifier that is assigned to the client site. The route target and route distinguisher are configured in the as-number:network-number format. The route target and route distinguisher must match. The configuration of the **subnet prefix-length** command in this example configures the size of each subnet that is allocated from the subnet pool to support 30 host IP addresses.

```
ip vrf RED
 rd 100:1
 route-target both 100:1
 vpn id 1234:123456
 exit
 ip dhcp pool VPN-POOL
  vrf RED
  network 192.168.0.0 /24
  subnet prefix-length /27
  exit
```

# Verifying Local Configuration on a Subnet Allocation Server Example

The following example is output from the **show running-config**command. This command can be used to verify the local configuration on a subnet allocation server. The output from this command displays the configuration of the subnet prefix-length command under the DHCP pool named “GLOBAL-POOL.” The total size of the subnet allocation pool is set to 254 addresses with the **network** command. The configuration of the **subnet prefix-length** command configures this pool to allocate a subnet that will support 254 host IP addresses. Because the total pool size supports only 254 addresses, only one subnet can be allocated from this pool.

```
Router# show running-config | begin dhcp
ip dhcp pool GLOBAL-POOL
   network 10.0.0.0 255.255.255.0
   subnet prefix-length 24
!
```

# Verifying Address Pool Allocation Information Example

The following examples are output from the **show ip dhcp pool**command. This command can be used to verify subnet allocation pool configuration on the subnet allocation server and the ODAP manager. The output from this command displays information about the address pool name, utilization level, configured subnet size, total number of addresses (from subnet), pending events, and specific subnet lease information.

The following sample output shows that the configured subnet allocation size is /24 (254 IP addresses), that there is a pending subnet allocation request, and there are no subnets in the pool:

```
Router> show ip dhcp pool ISP-1
Pool ISP-1 :
 Utilization mark (high/low)    :100 / 0
 Subnet size (first/next)       :24 / 24 (autogrow)
 Total addresses                :0
 Leased addresses               :0
 Pending event                  :subnet request
 0 subnet is currently in the pool
```

The next example shows that the configured subnet allocation size is /24 (254 IP address), the configured VRF name is “RED”, and a subnet containing 254 IP addresses has been allocated but no IP addresses have been leased from the subnet:

```
Router> show ip dhcp pool SUBNET-ALLOC
Pool SUBNET-ALLOC :
 Utilization mark (high/low)    :100 / 0
 Subnet size (first/next)       :24 / 24 (autogrow)
 VRF name                       :RED
 Total addresses                :254
 Leased addresses               :0
 Pending event                  :none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.0.0.1              10.0.0.1          - 10.0.0.254         0
```

## Verifying Subnet Allocation and DHCP Bindings Example

The following example is from the **show ip dhcp binding** command. This command can be used to display subnet allocation to DHCP binding mapping information. The output of this command shows the subnet lease to MAC address mapping, the lease expiration, and the lease type (subnet lease bindings are configured to be automatically created and released by default). The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet) in CIDR bit count notation. Bindings for individual IP address only display an IP address and are not followed by a subnet mask.

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.0/26         0063.6973.636f.2d64.    Mar 29 2009 04:36 AM    Automatic
                    656d.6574.6572.2d47.
                    4c4f.4241.4c
```

# Additional References

The following sections provide references related to configuring the DHCP ODAP manager.

### Related Documents

| Related Topic | Document Title |
|---|---|
| DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |

| Related Topic | Document Title |
|---|---|
| DHCP conceptual information | “DHCP Overview” module |
| DHCP server configuration | “Configuring the Cisco IOS XE DHCP Server” module |
| DHCP client configuration | “Configuring the Cisco IOS XE DHCP Client” module |
| DHCP relay agent configuration | “Configuring the Cisco IOS XE DHCP Relay Agent” module |
| DHCP advanced features | “Configuring DHCP Services for Accounting and Security” module |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this functionality. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 951 | *Bootstrap Protocol (BOOTP)* |
| RFC 1542 | *Clarifications and Extensions for the Bootstrap Protocol* |
| RFC 2131 | *Dynamic Host Configuration Protocol* |
| RFC 2685 | *Virtual Private Networks Identifier* |
| RFC 3046 | *DHCP Relay Information Option* |

### Technical Assistance

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

# Feature Information for the DHCP Server On-Demand Address Pool Manager

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 4 Feature Information for the DHCP On-Demand Address Pool Manager*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Server On-Demand Address Pool Manager for Non-MPLS VPNs | Cisco IOS XE Release 2.3 | This feature was enhanced to provide ODAP support for non-MPLS VPNs.<br>The following command was modified by this feature: **peer default ip address** |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP ODAP Server Support | Cisco IOS XE Release 2.3 | This feature introduces the capability to configure a DHCP server (or router) as a subnet allocation server. This capability allows the Cisco IOS DHCP server to be configured with a pool of subnets for lease to ODAP clients.<br>The following commands were introduced or modified by this feature: **subnet prefix-length** and **show ip dhcp binding** |
| DHCP Server On-Demand Address Pool Manager | Cisco IOS XE Release 2.3 | The ODAP manager is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses. When a Cisco IOS router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level.<br>The following commands were introduced by this feature: **aaa session-id**, **clear ip dhcp subnet**, **ip address pool**, **ip dhcp aaa default username**, **origin**, **show ip dhcp pool**, **utilization mark high**, **utilization mark low**, **vrf**.<br>The following commands were modified by this feature: **clear ip dhcp binding**, **clear ip dhcp conflict**, **ip address-pool**, **peer default ip address**. |

# Glossary

**AAA** --authentication, authorization, and accounting. Suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server.

**Cisco Access Registrar** --A RADIUS server that supports service provider deployment of access services by centralizing AAA information and simplifying provisioning and management.

**client** --A host trying to configure its interface (obtain an IP address) using DHCP or BOOTP protocols.

**DHCP** --Dynamic Host Configuration Protocol.

**incremental subnet size** --The desired size of the second and subsequent subnets requested for an on-demand pool.

**initial subnet size** --The desired size of the first subnet requested for an on-demand pool.

**IPCP** --IP Control Protocol. Protocol that establishes and configures IP over PPP.

**MPLS** --Multiprotocol Label Switching. Emerging industry standard upon which tag switching is based.

**ODAP** --on-demand address pool.

**PE router** --provider edge router.

**PPP** --Point-to-Point Protocol.

**RADIUS** -- Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

**relay agent** --A router that forwards DHCP and BOOTP messages between a server and a client on different subnets.

**releasable subnet** --A leased subnet that has no address leased from it.

**server** --DHCP or BOOTP server.

**VHG** --Virtual Home Gateway. A Cisco IOS software component that terminates PPP sessions. It is owned and managed by the service provider on behalf of its customer to provide access to remote users of that customers network. A single service provider device (router) can host multiple VHGs of different customers. A VHG can be dynamically brought up and down based on the access pattern of the remote users. Note that there is no single IOS feature called the VHG; it is a collection of function and features.

**VHG/PE** router--A device that terminates PPP sessions and maps the remote users to the corresponding MPLS VPNs.

**VPN** --Virtual Private Network. Enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VPN information** --In this document, VPN information refers to VRF name or VPN ID.

**VRF** --VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router. Each VPN instantiated on the PE router has its own VRF.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# Configuring the Cisco IOS XE DHCP Relay Agent

Cisco routers running Cisco IOS XE software include Dynamic Host Configuration Protocol (DHCP) server and relay agent software. A DHCP relay agent is any host that forwards DHCP packets between clients and servers. This module describes the concepts and tasks needed to configure the Cisco IOS XE DHCP relay agent.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for Configuring the DHCP Relay Agent

Before you configure the DHCP relay agent, you should understand the concepts documented in the “DHCP Overview” module.

The Cisco IOS XE DHCP server and relay agent are enabled by default. You can verify if they have been disabled by checking your configuration file. If they have been disabled, the **no service dhcp** command will appear in the configuration file. Use the **service dhcp** command to reenable the functionality if necessary.

The Cisco IOS XE DHCP relay agent will be enabled on an interface only when the **ip helper-address** is configured. This command enables the DHCP broadcast to be forwarded to the configured DHCP server.

# Information About the DHCP Relay Agent

## DHCP Relay Agent Overview

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway IP address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

The Cisco IOS XE DHCP relay agent supports the use of unnumbered interfaces. An unnumbered interface can “borrow” the IP address of another interface already configured on the router, which conserves network and address space. For DHCP clients connected though the unnumbered interfaces, the DHCP relay agent automatically adds a static host route once the DHCP client obtains an address, specifying the unnumbered interface as the outbound interface. The route is automatically removed once the lease time expires or when the client releases the address.

## Packet Forwarding Address

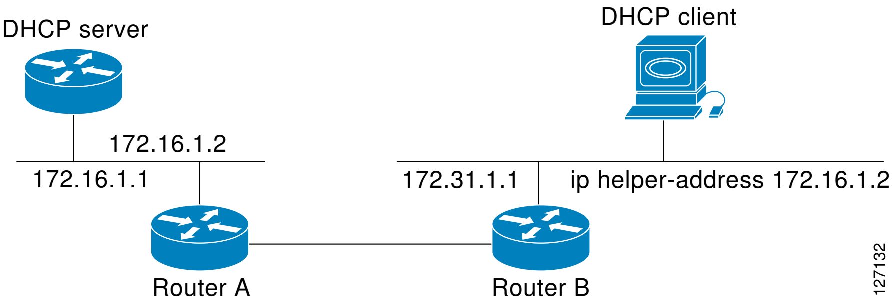
DHCP clients need to use User Datagram Protocol (UDP) broadcasts to send their initial DHCPDISCOVER messages because they don’t have information about the network to which they are attached. If the client is on a network segment that does not include a server, UDP broadcasts normally are not forwarded because most routers are configured to not forward broadcast traffic.

You can remedy this situation by configuring the interface of your router that is receiving the broadcasts to forward certain classes of broadcasts to a helper address. You can use more than one helper address per interface.

When a router forwards these address assignment/parameter requests, it is acting as a DHCP relay agent. The Cisco router implementation of the DHCP relay agent is provided via the **ip helper-address** interface configuration command.

In the figure below, the DHCP client broadcasts a request for an IP address and additional configuration parameters on its local LAN. Router B, acting as a DHCP relay agent, picks up the broadcast and generates a new DHCP message to send out on another interface. As part of this DHCP message, the relay agent inserts the IP address of the interface containing the **ip helper-address** command into the gateway IP address (giaddr) field of the DHCP packet. This IP address enables the DHCP server to determine which subnet should receive the offer and identify the appropriate IP address range to offer. The DHCP relay agent sends the local broadcast, via IP unicast, to the DHCP server address 172.16.1.2 specified by the **ip helper-address** interface configuration command.

*Figure 5 Forwarding UDP Broadcasts to a DHCP Server Using a Helper Address*



# Relay Agent Information Option

Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway IP address (giaddr field of the DHCP packet) or the incoming interface IP address. In some networks, it is necessary to use additional information to further determine which IP addresses to allocate. By using the relay agent information option (option 82), the Cisco IOS XE relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

Cisco IOS XE supports this functionality by using the **ip dhcp relay information option** command. The relay agent will automatically add the circuit identifier suboption and the remote ID suboption to the relay agent information option and forward them to the DHCP server.

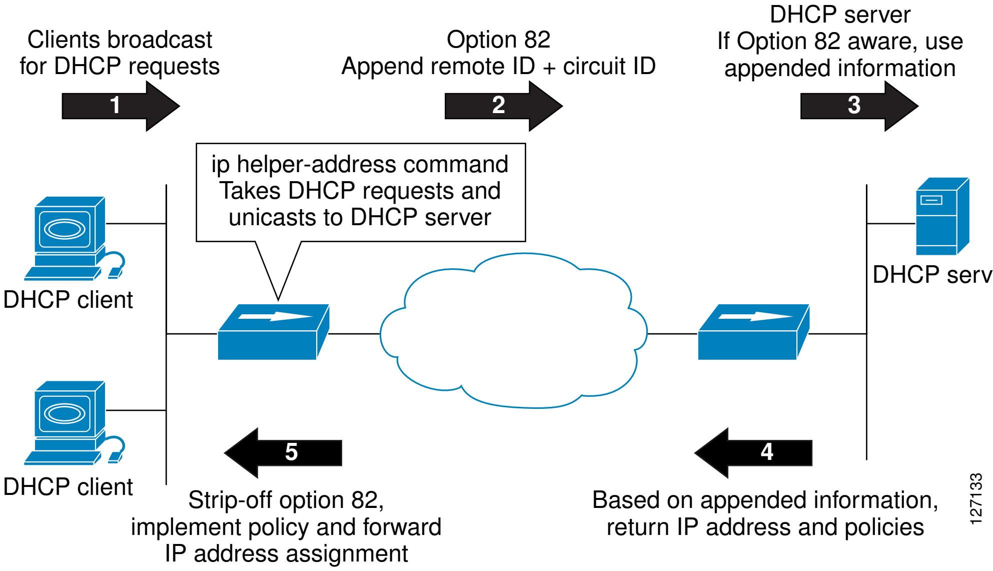
The DHCP server can use this information to assign IP addresses, perform access control, and set quality of service (QoS) and security policies (or other parameter-assignment policies) for each subscriber of a service provider network.

The figure below shows how the relay agent information option is inserted into the DHCP packet as follows:

1. The DHCP client generates a DHCP request and broadcasts it on the network.
2. The DHCP relay agent intercepts the broadcast DHCP request packet and inserts the relay agent information option (option 82) in the packet. The relay agent information option contains the related suboptions.
3. The DHCP relay agent unicasts the DHCP packet to the DHCP server.
4. The DHCP server receives the packet and uses the suboptions to assign IP addresses and other configuration parameters and forwards them back to the client.

5 The relay agent strips off the suboption fields of the packet while forwarding to the client.

*Figure 6 Relay Agent Information Option Operation*



- Relay Agent Information Reforwarding Policy, page 84

## Relay Agent Information Reforwarding Policy

A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, the relay information from the previous relay agent is replaced. If this behavior is not suitable for your network, you can use the **ip dhcp relay information policy** {**drop** | **keep** | **replace**} global configuration command to change it.

To ensure the correct operation of the reforwarding policy, make sure to disable the relay agent information check by using the **no ip dhcp relay information check** global configuration command.

# DHCP Relay Agent Support for MPLS VPNs

DHCP relay support for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) enables a network administrator to conserve address space by allowing overlapping addresses. The relay agent can support multiple clients on different VPNs, and many of these clients from different VPNs can share the same IP address.

Configuring VPNs involves an adjustment to the usual DHCP host IP address designation. VPNs use private address spaces that might not be unique across the Internet.

In some environments, a relay agent resides in a network element that also has access to one or more MPLS VPNs. A DHCP server that provides service to DHCP clients on those different VPNs must locate the VPN in which each client resides. The network element that contains the relay agent typically captures the VPN association of the DHCP client and includes this information in the relay agent information option of the DHCP packet.

DHCP relay support for MPLS VPNs allows the relay agent to forward this necessary VPN-related information to the DHCP server using the following three suboptions of the DHCP relay agent information option:

- VPN identifier
- Subnet selection
- Server identifier override

The VPN identifier suboption is used by the relay agent to tell the DHCP server the VPN for every DHCP request it passes on to the DHCP server, and it is also used to properly forward any DHCP reply that the DHCP server sends back to the relay agent. The VPN identifier suboption contains the VPN ID configured on the incoming interface to which the client is connected. If you configure the VRF name but not the VPN ID, the VRF name is used as the VPN identifier suboption. If the interface is in global routing space, the VPN suboptions are not added.

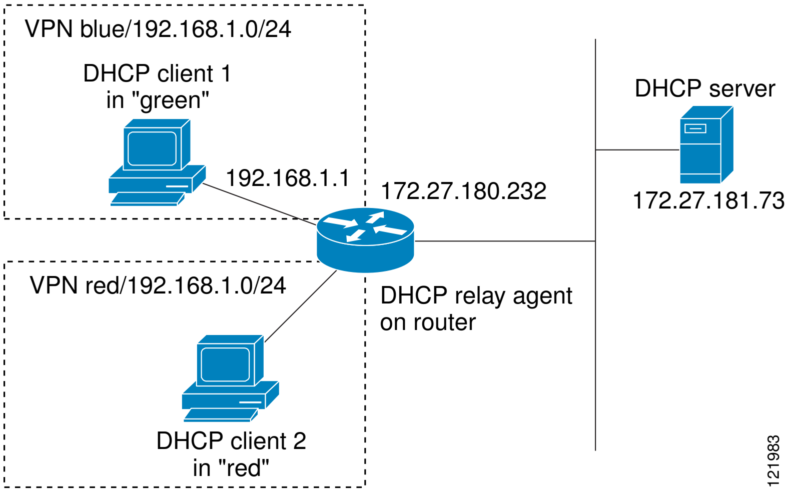
The subnet selection suboption allows the separation of the subnet where the client resides from the IP address used to communicate with the relay agent. In typical DHCP processing, the gateway address specifies both the subnet on which a DHCP client resides and the IP address that the server can use to communicate with the relay agent. Situations exist where the relay agent needs to specify the subnet on which a DHCP client resides that is different from the IP address the server can use to communicate with the relay agent. The subnet selection suboption is included in the relay agent information option and passed on to the DHCP server. The gateway address is changed to the outgoing interface of the relay agent toward the DHCP server. The DHCP server uses this gateway address to send reply packets back to the relay agent.

The server identifier override suboption value is copied in the reply packet from the DHCP server instead of the normal server ID address. The server identifier override suboption contains the incoming interface IP address, which is the IP address on the relay agent that is accessible from the client. Using this information, the DHCP client sends all renew and release packets to the relay agent. The relay agent adds all of the VPN suboptions and then forwards the renew and release packets to the original DHCP server.

After adding these suboptions to the DHCP relay agent information option, the gateway address is changed to the outgoing interface of the relay agent toward the DHCP server. When the packets are returned from the DHCP server, the relay agent removes the relay agent information options and forwards the packets to the DHCP client on the correct VPN.

The figure below shows a VPN scenario where the DHCP relay agent and DHCP server can recognize the VPN that each client resides within. DHCP client 1 is part of VPN green and DHCP client 2 is part of VPN red and both have the same private IP address 192.168.1.0/24. Because the clients have the same IP address, the DHCP relay agent and DHCP server use the VPN identifier, subnet selection, and server identifier override suboptions of the relay agent information option to distinguish the correct VPN of the client.

***Figure 7 Virtual Private Network DHCP Configuration***



# DHCP Relay Support for Option 82 Encapsulation

When two relay agents are relaying messages between the DHCP client and DHCP server, the second relay agent (closer to the server), by default, replaces the first option 82 information with its own option 82. The remote ID and circuit ID information from the first relay agent is lost. In some deployment scenarios, it is necessary to maintain the initial option 82 from the first relay agent, in addition to the option 82 from the second relay agent. For example, an Intelligent Service Gateway (ISG) acting as a second relay agent is connected to a Layer 2 device. The Layer 2 device connects to the household and identifies the household with its own option 82.

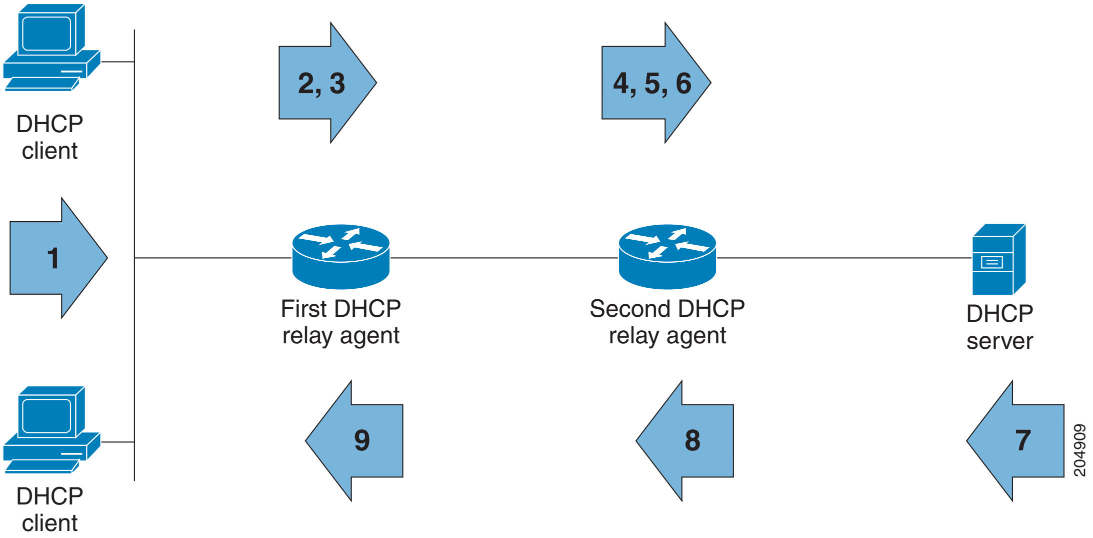
The DHCP Relay Option 82 Encapsulation feature allows the second relay agent to encapsulate option 82 information in a received message from the first relay agent if it is also configured to add its own option 82 information. This configuration allows the DHCP server to use option 82 information from both relay agents. The DHCP server can use the VPN information from the second relay agent along with the option 82 information from the first relay agent to send correct address assignments and other configuration parameters for the client devices based on the VRF, option 60, and encapsulated option 82. The reply message from the DHCP server to the DHCP client traverses the same path as the request messages through the two relay agents to the DHCP client.

Figure 4 shows the processing that occurs on the two relay agents and the DHCP server when this feature is configured:

1. The DHCP client generates a DHCP message (including option 60) and broadcasts it on the network.
2. The first DHCP relay agent intercepts the broadcast DHCP request packet and inserts its own option 82 in the packet.
3. The relay agent automatically adds the circuit ID suboption and the remote ID suboption to option 82 and forwards them to the second relay agent.
4. The second relay agent encapsulates the first relay agent’s option 82 and inserts its own option 82.
5. The gateway IP address (giaddr) is set to the incoming interface on the second relay agent and the original giaddr from the first relay agent is encapsulated.
6. The second DHCP relay agent unicasts the DHCP packet to the DHCP server.
7. The DHCP server receives the packet and uses the VPN suboption information from the second relay, along with the option 82 information from the first relay agent, to assign IP addresses and other configuration parameters and forwards the packet back to the second relay agent.
8. When the second relay agent receives the reply message from the server, it restores the encapsulated option 82 and prior giaddr from the first relay agent. The reply message is then sent to the prior giaddr.

**9** The option 82 is stripped off of the packet by the first relay agent before forwarding to the client.

***Figure 8 DHCP Relay Agent Information Option Encapsulation Support Processing***



# How to Configure the DHCP Relay Agent

- Specifying the Packet Forwarding Address, page 87
- Configuring Relay Agent Information Option Support, page 88
- Configuring Relay Agent Information Option Support per Interface, page 91
- Configuring the Subscriber Identifier Suboption of the Relay Agent Information Option, page 93
- Configuring DHCP Relay Agent Support for MPLS VPNs, page 94
- Setting the Gateway Address of the DHCP Broadcast to a Secondary Address Using Smart Relay Agent Forwarding, page 96
- Configuring Relay Agent Information Option Encapsulation Support, page 97
- Troubleshooting the DHCP Relay Agent, page 98

## Specifying the Packet Forwarding Address

Perform this task to configure the DHCP relay agent to forward packets to a DHCP server.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip helper-address** *address*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet0/0/0` | Configures an interface and enters interface configuration mode. |
| Step 4 | **ip helper-address** *address*<br>**Example:**<br>`Router(config-if)# ip helper-address 172.16.1.2` | Forwards UPD broadcasts, including BOOTP and DHCP.<br>- The *address*argument 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.<br>- If you have multiple servers, you can configure one helper address for each server. |

## Configuring Relay Agent Information Option Support

Perform this task to enable support for the DHCP relay agent information option.

Note

- If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.
- If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.
- If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

See the "Configuring Relay Agent Information Option Support per Interface" section for more information on per-interface support for the relay agent information option.

>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp relay information option**
4. **ip dhcp relay information check**
5. **ip dhcp relay information policy** {**drop** | **keep** | **replace**}
6. **ip dhcp relay information trust-all**
7. **end**
8. **show ip dhcp relay information trusted-sources**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **ip dhcp relay information option**<br>**Example:**<br>`Router(config)# ip dhcp relay information option` | Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server.<br>• This function is disabled by default. |
| Step 4 | **ip dhcp relay information check**<br>**Example:**<br>`Router(config)# ip dhcp relay information check` | (Optional) Configures DHCP to check that the relay agent information option in forwarded BOOTREPLY messages is valid.<br>• By default, DHCP checks that the option-82 field in DHCP reply packets it receives from the DHCP server is valid. If an invalid message is received, the relay agent drops it. If a valid message is received, the relay agent removes the option-82 field and forwards the packet. Use the **ip dhcp relay information check** command to reenable this functionality if it has been disabled. |
| Step 5 | **ip dhcp relay information policy** {**drop** \| **keep** \| **replace**}<br>**Example:**<br>`Router(config)# ip dhcp relay information policy replace` | (Optional) Configures the reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information).<br>• See the "Relay Agent Information Reforwarding Policy" section for more information. |
| Step 6 | **ip dhcp relay information trust-all**<br>**Example:**<br>`Router(config)# ip dhcp relay information trust-all` | (Optional) Configures all interfaces on a router as trusted sources of the DHCP relay information option.<br>• By default, if the gateway address is set to all zeros in the DHCP packet and the relay agent information option is already present in the packet, the DHCP relay agent will discard the packet. Use the **ip dhcp relay information trust-all**command to override this behavior and accept the packets.<br>• This command is useful if there is a switch in between the client and the relay agent that may insert option 82. Use this command to ensure that these packets do not get dropped.<br>• You can configure an individual interface as a trusted source of the DHCP relay information option by using the **ip dhcp relay information trusted** interface configuration mode command. |
| Step 7 | **end**<br>**Example:**<br>`Router(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 8 | **show ip dhcp relay information trusted-sources**<br>**Example:**<br>`Router# show ip dhcp relay information trusted-sources` | (Optional) Displays all interfaces configured to be a trusted source for the DHCP relay information option. |

# Configuring Relay Agent Information Option Support per Interface

Perform this task to enable support for the DHCP relay agent information option (option 82) on a per interface basis.

The interface configuration allows the subscribers with different DHCP option 82 requirements on different interfaces to be reached from one Cisco router.

Read the “Restrictions” and "Relay Agent Information Reforwarding Policy" sections to understand how DHCP processes the relay agent information option for global configurations.

Note

- If an **ip dhcp relay information** command is configured in global configuration mode but not configured in interface configuration mode, the global configuration is applied to all interfaces.
- If an **ip dhcp relay information** command is configured in both global configuration mode and interface configuration mode, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.
- If an **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip dhcp relay information option-insert** [**none**]
5. **ip dhcp relay information check-reply** [**none**]
6. **ip dhcp relay information policy-action** {**drop**| **keep**| **replace**}
7. **exit**
8. Repeat Steps 3 through 7 to configure relay agent information settings on different interfaces.

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet0/0/0` | Configures an interface and enters interface configuration mode. |
| Step 4 | **ip dhcp relay information option-insert** [**none**]<br>**Example:**<br>`Router(config-if)# ip dhcp relay information option-insert` | Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server.<br>- This function is disabled by default. However, if support for the relay agent information option is configured in global configuration mode, but not in interface configuration mode, the interface inherits the global configuration.<br>- The **ip dhcp relay information option-insert none** interface configuration command is saved in the running configuration. This command takes precedence over any global relay agent information configuration. |
| Step 5 | **ip dhcp relay information check-reply** [**none**]<br>**Example:**<br>`Router(config-if)# ip dhcp relay information check-reply` | Configures a DHCP server to validate the relay information option in forwarded BOOTREPLY messages.<br>- By default, DHCP checks that the option-82 field in DHCP reply packets it receives from the DHCP server is valid. If an invalid message is received, the relay agent drops it. If a valid message is received, the relay agent removes the option-82 field and forwards the packet. Use the **ip dhcp relay information check-reply** command to reenable this functionality if it has been disabled.<br>- The **ip dhcp relay information check-reply none** interface configuration command option is saved in the running configuration. This command takes precedence over any global relay agent information configuration. |

| | Command or Action | Purpose |
|---|---|---|
| Step 6 | **ip dhcp relay information policy-action** {**drop**\| **keep**\| **replace**}<br>**Example:**<br>`Router(config-if)# ip dhcp relay information policy-action replace` | Configures the information reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information). |
| Step 7 | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode. |
| Step 8 | Repeat Steps 3 through 7 to configure relay agent information settings on different interfaces. | (Optional) |

## Configuring the Subscriber Identifier Suboption of the Relay Agent Information Option

Perform this task to enable an Internet service provider (ISP) to add a unique identifier to the subscriber-identifier suboption of the relay agent information option.

The unique identifier enables an ISP to identify a subscriber, to assign specific actions to that subscriber (for example, assignment of host IP address, subnet mask, and domain name system DNS), and to trigger accounting.

Before the introduction of this feature, if a subscriber moved, each ISP had to be informed of the change and all ISPs had to reconfigure the DHCP settings for the affected customers at the same time. Even if the service was not changed, every move involved administrative changes in the ISP environment. With the introduction of this feature, if a subscriber moves from one Network Access Server to another, there is no need for a change in the configuration on the part of the DHCP server or ISP.

You should configure the unique identifier for each subscriber.

The new configurable subscriber-identifier option should be configured on the interface connected to the client. When a subscriber moves from one interface to the other, the interface configuration should also be changed.

The server should be able to recognize the new suboption.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp relay information option**
4. **interface** *type number*
5. **ip dhcp relay information option subscriber-id** *string*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip dhcp relay information option**<br>**Example:**<br>`Router(config)# ip dhcp relay information option` | Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server.<br>• This function is disabled by default. |
| Step 4 | **interface** *type number*<br>**Example:**<br>`Router(config)# interface atm4/0/0` | Configures an interface and enters interface configuration mode. |
| Step 5 | **ip dhcp relay information option subscriber-id** *string*<br>**Example:**<br>`Router(config-if)# ip dhcp relay information option subscriber-id newsubscriber123` | Specifies that a DHCP relay agent add a subscriber identifier suboption to the relay information option.<br>• The *string* argument can be up to a maximum of 50 characters and can be alphanumeric.<br>**Note** If more than 50 characters are configured, the string is truncated.<br>**Note** The **ip dhcp relay information option subscriber-id**command is disabled by default to ensure backward capability. |

# Configuring DHCP Relay Agent Support for MPLS VPNs

Perform this task to configure DHCP relay agent support for MPLS VPNs.

Before configuring DHCP relay support for MPLS VPNs, you must configure standard MPLS VPNs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp relay information option vpn**
4. **interface** *type number*
5. **ip helper-address vrf** *name* [**global**] *address*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip dhcp relay information option vpn**<br>**Example:**<br>`Router(config)# ip dhcp relay information option vpn` | Enables the system to insert VPN suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server and sets the gateway address to the outgoing interface toward the DHCP server.<br>• The VPN suboptions are also added to the BOOTP broadcast packets when the command is configured. |
| Step 4 | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet0/0/0` | Configures an interface and enters interface configuration mode. |
| Step 5 | **ip helper-address vrf** *name* [**global**] *address*<br>**Example:**<br>`Router(config-if)# ip helper-address vrf blue 172.27.180.232` | Forwards UDP broadcasts, including BOOTP, received on an interface.<br>• If the DHCP server resides in a different VPN or global space that is different from the VPN, then the **vrf** *name* or **global** options allow you to specify the name of the VRF or global space in which the DHCP server resides. |

# Setting the Gateway Address of the DHCP Broadcast to a Secondary Address Using Smart Relay Agent Forwarding

Perform this task to configure smart relay agent forwarding.

You only need to configure helper addresses on the interface where the UDP broadcasts that you want to forward to the DHCP server are being received, and you only need the **ip dhcp smart-relay** command configured if you have secondary addresses on that interface and you want the router to step through each IP network when forwarding DHCP requests. Without the smart relay agent configured, all requests are forwarded using the primary IP address on the interface.

If the **ip dhcp smart-relay** command is configured, the relay agent counts the number of times the client retries sending a request to the DHCP server when there is no DHCPOFFER message from the DHCP server. After three retries, the relay agent sets the gateway address to the secondary address. If the DHCP server still does not respond after three more retries, then the next secondary address is used as the gateway address.

This functionality is useful when the DHCP server cannot be configured to use secondary pools.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp smart-relay**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp smart-relay**<br>**Example:**<br>`Router(config)# ip dhcp smart-relay` | Allows the DHCP relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server. |

# Configuring Relay Agent Information Option Encapsulation Support

Perform this task to enable support for the encapsulation of the DHCP relay agent information option (option 82).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp relay information option**
4. **ip dhcp relay information option vpn**
5. **ip dhcp relay information policy encapsulate**
6. **interface** *type number*
7. **ip dhcp relay information policy-action encapsulate**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp relay information option**<br>**Example:**<br>`Router(config)# ip dhcp relay information option` | Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server.<br>• This function is disabled by default. |
| **Step 4** | **ip dhcp relay information option vpn**<br>**Example:**<br>`Router(config)# ip dhcp relay information option vpn` | (Optional) Enables the system to insert VPN suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server and sets the gateway address to the outgoing interface toward the DHCP server.<br>• The VPN suboptions are also added to the BOOTP broadcast packets when the command is configured. |

| | Command or Action | Purpose |
|---|---|---|
| Step 5 | **ip dhcp relay information policy encapsulate**<br>**Example:**<br>`Router(config)# ip dhcp relay information policy encapsulate` | Enables the system to encapsulate the DHCP relay agent information option (option-82 field) received from a prior relay agent in forwarded BOOTREQUEST messages to a DHCP server.<br>• Option 82 information from both relay agents will be forwarded to the DHCP server. |
| Step 6 | **interface** *type number*<br>**Example:**<br>`Router(config)# interface FastEthernet0/0` | (Optional) Configures an interface and enters interface configuration mode.<br>• If you configure the **ip dhcp relay information** command in global configuration mode, there is no need to configure the command in interface configuration mode unless you want a different configuration to apply on specific interfaces. |
| Step 7 | **ip dhcp relay information policy-action encapsulate**<br>**Example:**<br>`Router(config-if)# ip dhcp relay information policy-action encapsulate` | (Optional) Enables the system to encapsulate the DHCP relay agent information option (option-82 field) received on an interface from a prior relay agent in forwarded BOOTREQUEST messages to a DHCP server on an interface.<br>• This function is disabled by default. This command has precedence over any global configuration. However, if support for the relay agent information option encapsulation support is configured in global configuration mode, but not in interface configuration mode, the interface inherits the global configuration. |

# Troubleshooting the DHCP Relay Agent

Perform this task to troubleshoot the DHCP relay agent.

The **show ip route dhcp** command is useful to help you understand any problems with the DHCP relay agent adding routes to clients from unnumbered interfaces. All routes added to the routing table by the DHCP server and relay agent are displayed.

### SUMMARY STEPS

1. **enable**
2. **show ip route dhcp**
3. **show ip route dhcp** *ip-address*
4. **show ip route vrf** *vrf-name* **dhcp**
5. **clear ip route** [**vrf** *vrf-name*] **dhcp** [*ip-address*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>- Enter your password if prompted. |
| Step 2 | **show ip route dhcp**<br>**Example:**<br>`Router# show ip route dhcp` | Displays all routes added by the Cisco IOS XE DHCP server and relay agent. |
| Step 3 | **show ip route dhcp** *ip-address*<br>**Example:**<br>`Router# show ip route dhcp 172.16.1.3` | Displays all routes added by the Cisco IOS XE DHCP server and relay agent associated with an IP address. |
| Step 4 | **show ip route vrf** *vrf-name* **dhcp**<br>**Example:**<br>`Router# show ip route vrf red dhcp` | Displays all routes added by the Cisco IOS XE DHCP server and relay agent associated with the named VRF. |
| Step 5 | **clear ip route** [**vrf** *vrf-name*] **dhcp** [*ip-address*]<br>**Example:**<br>`Router# clear ip route dhcp` | Removes routes from the routing table added by the DHCP server and relay agent for the DHCP clients on unnumbered interfaces. |

# Configuration Examples for the DHCP Relay Agent

## Example Configuring the DHCP Relay Agent and Relay Agent Information Option Support

The following example shows how to enable the DHCP server, the relay agent, and the insertion and removal of the DHCP relay information option (option 82). Note that the Cisco IOS XE DHCP server is enabled by default. In this example, the DHCP server was disabled:

```
!reenables the DHCP server
service dhcp
ip dhcp relay information option
!
interface GigabitEthernet 0/0/0
 ip address 192.168.100.1 255.255.255.0
 ip helper-address 10.55.11.3
```

## Example Configuring the DHCP Relay Agent and Relay Agent Information Option Support per Interface

The following example shows that for subscribers being serviced by the same aggregation router, the relay agent information option needs to be processed differently for Asynchronous Transfer Mode (ATM) subscribers than for Gigabit Ethernet digital subscribers. For ATM subscribers, the relay agent information option is configured to be removed from the packet by the relay agent before forwarding to the client. For Gigabit Ethernet subscribers, the connected device provides the relay agent information option, and it is configured to remain in the packet and be forwarded to the client.

```
ip dhcp relay information trust-all
interface Loopback0
 ip address 10.16.0.1 255.255.255.0
!
interface ATM 3/0/0
 no ip address
!
interface ATM 3/0/0
 ip helper-address 10.16.1.2
 ip unnumbered loopback0
 ip dhcp relay information option-insert
!
interface Loopback1
 ip address 10.18.0.1 255.255.255.0
!
interface GigabitEthernet0/0/0
 no ip address
!
interface GigabitEthernet 0/0/1
 encap dot1q 123
 ip unnumbered loopback1
 ip helper-address 10.18.1.2
 ip dhcp relay information policy-action keep
```

## Example Configuring the Subscriber Identifier Suboption

The following example shows how to add a unique identifier to the subscriber-identifier suboption of the relay agent information option.

```
ip dhcp relay information option
!
interface Loopback0
 ip address 10.1.1.129 255.255.255.192
!
```

```
interface ATM 4/0/0
 no ip address
!
interface ATM 4/0/1 point-to-point
 ip helper-address 10.16.1.2
 ip unnumbered Loopback0
 ip dhcp relay information option subscriber-id newperson123
 atm route-bridged ip
 pvc 88/800
 encapsulation aal5snap
```

## Example Configuring DHCP Relay Agent Support for MPLS VPNs

In the following example, the DHCP relay agent receives a DHCP request on Gigabit Ethernet interface 0/0/0 and sends the request to the DHCP server located at IP helper address 10.44.23.7, which is associated with the VRF named red:

```
ip dhcp relay information option vpn
!
interface GigabitEthernet 0/0/0
 ip helper-address vrf red 10.44.23.7
!
```

## Example Configuring DHCP Smart Relay Agent Forwarding

In the following example, the router will forward the DHCP broadcast received on Gigabit Ethernet interface 0/0 to the DHCP server (10.55.11.3), inserting 192.168.100.1 in the giaddr field of the DHCP packet. If the DHCP server has a scope or pool configured for the 192.168.100.0/24 network, it will respond; otherwise it will not respond.

Because the **ip dhcp smart-relay** global configuration command is configured, if the router sends three requests using 192.168.100.1 in the giaddr field, and doesn't get a response, it will move on and start using 172.16.31.254 in the giaddr field instead. Without the smart relay functionality, the route only uses 192.168.100.1 in the giaddr field.

```
ip dhcp smart-relay
!
interface GigabitEthernet0/0/0
 ip address 192.168.100.1 255.255.255.0
 ip address 172.16.31.254 255.255.255.0
 ip helper-address 10.55.11.3
!
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |

| Related Topic | Document Title |
|---|---|
| DHCP conceptual information | “DHCP Overview” module |
| DHCP server configuration | “Configuring the Cisco IOS XE DHCP Server” module |
| DHCP client configuration | “Configuring the Cisco IOS XE DHCP Client” module |
| DHCP server on-demand address pool manager configuration | “Configuring the DHCP Server On-Demand Address Pool Manager” module |
| DHCP advanced features | “Configuring DHCP Services for Accounting and Security” module |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this functionality. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported, and support for existing MIBs has not been modified. | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 951 | *Bootstrap Protocol (BOOTP)* |
| RFC 1542 | *Clarifications and Extensions for the Bootstrap Protocol* |
| RFC 2131 | *Dynamic Host Configuration Protocol* |
| RFC 2685 | *Virtual Private Networks Identifier* |
| RFC 3046 | *DHCP Relay Information Option* |

# Technical Assistance

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

# Feature Information for the Cisco IOS XE DHCP Relay Agent

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 5 Feature Information for the Cisco IOS XE DHCP Relay Agent*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Relay Option 82 per Interface Support | Cisco IOS XE Release 2.1 | This feature enables support for the DHCP relay agent information option (option 82) on a per interface basis. The interface configuration allows different DHCP servers, with different DHCP option 82 requirements to be reached from one Cisco router.<br>The following commands were introduced by this feature: **ip dhcp relay information check-reply**, **ip dhcp relay information option-insert**, **ip dhcp relay information policy-action**. |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Subscriber Identifier Suboption of Option 82 | Cisco IOS XE Release 2.1 | This feature enables an ISP to add a unique identifier to the subscriber-identifier suboption of the relay agent information option.<br>The following command was introduced by this feature: **ip dhcp relay information option subscriber-id**. |
| DHCP Relay MPLS VPN Support | Cisco IOS XE Release 2.1 | DHCP relay support for MPLS VPNs enables a network administrator to conserve address space by allowing overlapping addresses. The relay agent can support multiple clients on different VPNs, and many of these clients from different VPNs can share the same IP address.<br>The following commands were modified by this feature: **ip dhcp relay information option**, **ip helper address**. |
| DHCP Relay Agent Support for Unnumbered Interfaces | Cisco IOS XE Release 2.1 | The Cisco IOS XE DHCP relay agent supports the use of unnumbered interfaces. |

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Relay Option 82 Encapsulation | Cisco IOS XE Release 3.1S | This feature allows a second DHCP relay agent to encapsulate the relay agent information option (option 82) from a prior relay agent, add its own option 82, and forward the packet to the DHCP server. The DHCP server can use the VPN information from the second relay agent along with the option 82 information from the first relay agent to send correct address assignments and other configuration parameters for the client devices based on the VRF, option 60, and encapsulated option 82.<br>The following commands were added or modified by this feature: **ip dhcp relay information policy**, **ip dhcp relay information policy-action**. |

# Glossary

**client** --A host trying to configure its interface (obtain an IP address) using DHCP or BOOTP protocols.

**DHCP** --Dynamic Host Configuration Protocol.

**giaddr** --Gateway IP address. The giaddr field of the DHCP message provides the DHCP server with information about the IP address subnet on which the client is to reside. It also provides the DHCP server with an IP address where the response messages are to be sent.

**MPLS** --Multiprotocol Label Switching. Emerging industry standard upon which tag switching is based.

**relay agent** --A router that forwards DHCP and BOOTP messages between a server and a client on different subnets.

**server** --DHCP or BOOTP server.

**VPN** --Virtual Private Network. Enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router. Each VPN instantiated on the PE router has its own VRF.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# DHCP Relay Server ID Override and Link Selection Option 82 Suboptions

The DHCP Relay Server ID Override and Link Selection Option 82 Suboptions feature enables the relay agent to be part of all DHCP message exchanges by supporting the use of two suboptions of the relay agent information option (option 82). This design allows DHCPv4 to operate in networks where direct communication between the client and server is not possible or desired. When used together, these two suboptions enable the deployment of an architecture where it is desirable to have all DHCP traffic flow through the relay agent, allowing for greater control of DHCP communications.

This feature also introduces the capability to manually configure the interface for the relay agent to use as the source IP address for messages relayed to the DHCP server. This configuration allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface).

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Restrictions for DHCP Relay Server ID Override and Link Selection Option 82 Suboptions

If this feature and the DHCP Relay MPLS VPN Support feature are both configured, DHCP Relay MPLS VPN Support takes precedence.

# Information About DHCP Relay Server ID Override and Link Selection Option 82 Suboptions

## Server ID Override Suboption

The server identifier (ID) override suboption allows the DHCP relay agent to specify a new value for the server ID option, which is inserted by the DHCP server in the reply packet. This suboption allows the DHCP relay agent to act as the actual DHCP server such that the renew requests will come to the relay agent rather than the DHCP server directly. The server ID override suboption contains the incoming interface IP address, which is the IP address on the relay agent that is accessible from the client. Using this information, the DHCP client sends all renew and release request packets to the relay agent. The relay agent adds all of the appropriate suboptions and then forwards the renew and release request packets to the original DHCP server.

## Link Selection Suboption

The link selection suboption provides a mechanism to separate the subnet/link on which the DHCP client resides from the the gateway address (giaddr), which can be used to communicate with the relay agent by the DHCP server. The relay agent will set the suboption to the correct subscriber subnet and the DHCP server will use that value to assign an IP address rather than the giaddr value. The relay agent will set the giaddr to its own IP address so that DHCP messages are routable over the network.

## DHCP Relay Server ID Override and Link Selection Option 82 Suboptions Feature Design

The current DHCP IPv4 deployment model assumes a single routing domain between the DHCP client and DHCP server. In some network designs, the DHCP server can not directly communicate with DHCP clients. Customers may choose this design to make critical infrastructure servers inaccessible and to protect the DHCP server from client attacks.

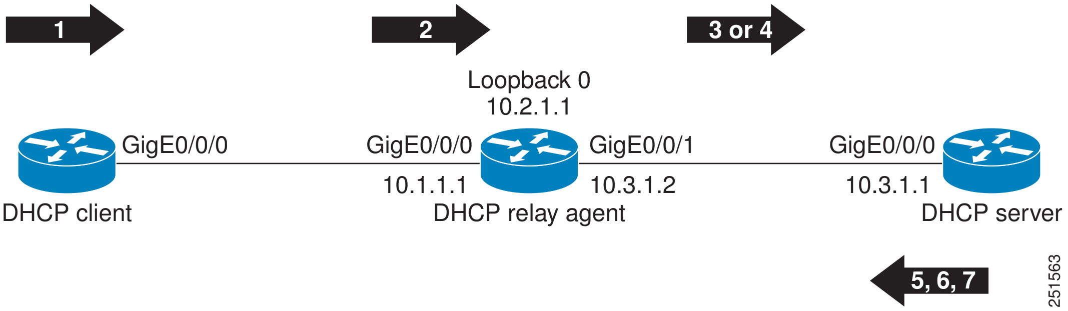
Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. In all cases, the DHCP relay agent must be able to communicate directly with both the DHCP server and DHCP client. By using the relay agent information option (option 82), the DHCP relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

The DHCP Relay Server ID Override and Link Selection Option 82 Suboptions feature enables the relay agent to be part of all DHCP message exchanges by supporting the use of two suboptions of option 82: server ID override and link selection suboptions. This design results in all DHCP messages flowing through the relay agent, allowing for greater control of DHCP communications.

Communication from the DHCP server through the relay agent can also be an issue. If the server needs to reach the client, it must do so through the relay agent. The IP address of the relay agent might not be ideal. For example, if the network is renumbered or if the interface at the relay agent is down for some reason, the server may not be able to reach the client. This feature introduces the capability to manually configure the interface for the relay agent to use as the source IP address for messages relayed to the DHCP server. This configuration allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface).

The figure below shows the processing that occurs on the DHCP relay agent and DHCP server when this feature is configured.

***Figure 9 DHCP Relay Agent and DHCP Server Processing of Option 82 Suboptions***



1 The DHCP client generates a DHCP request and broadcasts it on the network.
2 The DHCP relay agent intercepts the broadcast DHCP request packet and inserts a server ID override suboption and link selection suboption to its relay agent information option in the DHCP packet. The server ID override and link selection suboptions contain the incoming interface IP address, which is the IP address on the relay agent that is accessible from the client (10.1.1.1 in this case).
3 The relay agent sets the giaddr to the IP address of an interface that is reachable by the DHCP server (typically the server-facing interface that will be used to transmit the message, 10.3.1.2 in this case).
4 If the source interface is explicitly configured on a loopback interface (**ip dhcp-relay source-interface** command), the relay agent will use that address as the source IP address (*giaddr*) for messages relayed to the DHCP server (10.2.1.1 in this case).

The following processing occurs on the DHCP server after receiving the forwarded packets from the relay agent:

1 The DHCP server uses the link selection suboption to locate the correct address pools for the DHCP client.
2 The DHCP server sets the server ID option to the value specified by the server ID override suboption of the DHCP packet.
3 The DHCP server sends the reply message to the IP address specified in the giaddr.

The DHCP client will see the relay agent address as the server ID and use that address when unicasting RENEW messages.

# How to Configure Support for the DHCP Relay Server ID Override and Link Selection Suboptions

## Configuring the DHCP Relay Agent to Insert the DHCP Server ID Override and Link Selection Suboptions into Option 82

To configure this feature, perform the steps below:

**Note** If this feature and the DHCP Relay MPLS VPN Support feature are both configured, the DHCP Relay MPLS VPN Support feature takes precedence.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp-relay information option server-override**
4. **ip dhcp-relay source-interface** *type number*
5. **interface** *type number*
6. **ip dhcp relay information option server-id-override**
7. **ip dhcp relay source-interface** *type number*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ip dhcp-relay information option server-override**<br>**Example:**<br>`Router(config)# ip dhcp-relay information option server-override` | Enables the system to globally insert the server ID override and link selection suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server.<br>• If the **ip dhcp relay information option server-id-override**interfaceconfigurationcommand is configured on an interface, it overrides the global configuration on that interface only. |
| **Step 4** | **ip dhcp-relay source-interface** *type number*<br>**Example:**<br>`Router(config)# ip dhcp-relay source-interface loopback 0` | (Optional) Globally configures the source interface for the relay agent to use as the source IP address for relayed messages.<br>• This command allows the network administrator to specify a stable, hardware-independent IP address (such as a loopback interface).<br>• If the **ip dhcp relay source-interface**interfaceconfigurationcommand is configured on an interface, it overrides the global configuration on that interface only. |
| **Step 5** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet0/0/0` | (Optional) Configures an interface and enters interface configuration mode. |
| **Step 6** | **ip dhcp relay information option server-id-override**<br>**Example:**<br>`Router(config-if)# ip dhcp relay information option server-id-override` | (Optional) Enables the system to insert the server ID override and link selection suboptions on a specific interface into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server. |
| **Step 7** | **ip dhcp relay source-interface** *type number*<br>**Example:**<br>`Router(config-if)# ip dhcp relay source-interface loopback 2` | (Optional) Configures the source interface for the relay agent to use as the source IP address for relayed messages. |

# Configuration Examples for DHCP Relay Server ID Override and Link Selection Option 82 Suboptions

## DHCP Relay Server ID Override and Link Selection Option 82 Suboptions Example

In the following example, the IP address of the loopback interface is used as the source IP address for relayed messages. The client initiates IP address negotiation from GigabitEthernet interface 0/0/0. The DHCP relay agent is configured globally to insert the server ID override suboption and link selection suboption into the relay agent information option of the DHCP packet. The relay agent uses the server ID override suboption to force the DHCP server to use that value as the server ID in the DHCP message. The DHCP server uses the link selection suboption to determine from which subnet to assign an IP address.

### DHCP Client

```
interface GigabitEthernet0/0/0
 ip address dhcp
```

### DHCP Relay Agent

```
ip dhcp-relay information option server-override
ip dhcp-relay source-interface loopback0
!
interface Loopback0
 ip address 10.2.1.1 255.255.255.0
!
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.0
 ip helper-address 10.3.1.1
!
interface GigabitEthernet1/0/0
 ip address 10.3.1.2 255.255.255.0
```

### DHCP Server

```
ip dhcp excluded-address 10.3.0.1
ip dhcp pool pool1
 network 10.1.1.0 255.255.255.0
 lease 0 0 1
!
interface GigabitEthernet0/0/0
 ip address 10.3.1.1 255.255.255.0
```

# Additional References

The following sections provide references related to the DHCP Relay Server ID Override and Link Selection Option 82 Suboptions feature.

### Related Documents

| Related Topic | Document Title |
|---|---|
| DHCP conceptual information | "DHCP Overview" module |
| DHCP server configuration tasks, examples, and conceptual information | "Configuring the Cisco IOS XE DHCP Server" module |

| Related Topic | Document Title |
|---|---|
| DHCP relay agent configuration tasks, examples, and conceptual information | "Configuring the Cisco IOS XE DHCP Relay Agent" module |
| DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| RFC 3527 | Link Selection Suboption |
| RFC 5107 | DHCP Server Identifier Override Suboption |

### Technical Assistance

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

# Feature Information for DHCP Relay Server ID Override and Link Selection Option 82 Suboptions

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 6 Feature Information for DHCP Relay Server ID Override and Link Selection Option 82 Suboptions*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Relay Server ID Override and Link Selection Option 82 Suboptions | Cisco IOS XE Release 2.1 | This feature enables the relay agent to be part of all DHCP message exchanges by supporting the use of two suboptions of the relay agent information option (option 82). This design allows DHCPv4 to operate in networks where direct communication between the client and server is not possible or desired. When used together, these two suboptions enable the deployment of an architecture where it is desirable to have all DHCP traffic flow through the relay agent, allowing for greater control of DHCP communications.<br>• The following commands were introduced by this feature: **ip dhcp-relay information option server-override**, **ip dhcp relay information option server-id-override**, **ip dhcp-relay source-interface**, and **ip dhcp relay source-interface**. |

# Glossary

**client** --A host trying to configure its interface (obtain an IP address) using DHCP or BOOTP protocols.

**DHCP** --Dynamic Host Configuration Protocol.

**DHCP options and suboptions** --Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. Options provide a method of appending additional information. Vendors that want to provide additional information to their client not designed into the protocol can use options.

**giaddr** --gateway address field of the DHCP packet. The giaddr provides the DHCP server with information about the IP address subnet in which the client resides. The giaddr also provides the DHCP server with an IP address where the DHCP response messages can be sent.

**relay agent** --A router that forwards DHCP and BOOTP messages between a server and a client on different subnets.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# DHCP Server RADIUS Proxy

The Dynamic Host Configuration Protocol (DHCP) Server RADIUS Proxy is a RADIUS-based address assignment mechanism in which a DHCP server authorizes remote clients and allocates addresses based on replies from a RADIUS server.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for DHCP Server RADIUS Proxy

Before you can configure the DHCP Server RADIUS Proxy, you must be running DHCPv4 or a later version. For information about release and platform support, see "Feature Information for DHCP Server RADIUS Proxy".

## Restrictions for DHCP Server RADIUS Proxy

The DHCP Server RADIUS Proxy supports only one address authorization pool on the router.

# Information About DHCP Server RADIUS Proxy

## DHCP Server RADIUS Proxy Overview

The DHCP Server RADIUS Proxy feature is an address allocation mechanism for RADIUS-based authorization of DHCP leases. This feature supports DHCP options 60 and 121.

1. The DHCP server passes client information to a RADIUS server.
2. The RADIUS server returns all required information to the DHCP server as RADIUS attributes.
3. The DHCP server translates the RADIUS attributes into DHCP options, and sends this information back to RADIUS in a DHCP OFFER message.
4. DHCP binding is synchronized after the RADIUS server authorizes the client session.

If a local pool and an authorization pool are configured on the router, the DHCP server can assign addresses from both pools for different client interfaces.

## DHCP Server RADIUS Proxy Architecture

The allocation of addresses in a DHCP and RADIUS solution occurs as follows:

1. The client accesses the network from a residential gateway and sends a DHCP DISCOVER broadcast message to the relay agent. The DHCP DISCOVER message contains the client IP address, hostname, vendor class identifier, and client identifier.
2. The relay agent sends a DHCP DISCOVER unicast message containing the following information to the router:
    - Relay agent information (option 82) with the remote ID suboption containing the inner and outer VLAN IDs
    - Client information in the DHCP DISCOVER packet

The router determines the address of the DHCP server from the IP helper address on the interface that receives the DHCP packet.

1. RADIUS receives an access-request message to translate the DHCP options to RADIUS attributes.
2. RADIUS responds with an access-accept message, and delivers the following attributes to the DHCP server:
    - Framed-IP-Address
    - Framed-IP-Netmask
    - Session-Timeout
    - Session-Duration
3. The DHCP server sends an OFFER unicast message containing the following translations from the RADIUS server access-accept message to the client:
    - Framed-IP-Address inserted into the DHCP header.
    - Framed-IP-Netmask inserted into DHCP option 1 (subnet mask).

- Session-Timeout inserted into DHCP option 51 (IP address lease time).
- Framed-Route that is translated from the standard Cisco Framed-Route format into DHCP option 121 or the DHCP default gateway option (if the network and netmask are appropriate for a default route).
- A copy of relay agent information (option 82). Before the DHCP client receives the packet, the relay removes option 82.
- T1 time set to the Session-Timeout and T2 time set to the Session-Duration.

4. The client returns a formal request for the offered IP address to the DHCP server in a DHCP REQUEST broadcast message.
5. The DHCP confirms that the IP address is allocated to the client by returning a DHCP ACK unicast message containing lease information and the DHCP options to the client.
6. A RADIUS server accounting request starts, followed by a RADIUS server accounting response that is used by the AAA subsystem.

When a RADIUS server attribute is not present in an access-accept message, the corresponding DHCP option is not sent to the DHCP client. If the required information to produce a particular RADIUS server attribute is not available to the DHCP server, the DHCP server does not include information in the RADIUS packet. Non-inclusion can be in the form of not sending an attribute (if there is no information at all), or omitting information from the attribute (in the case of CLI-based format strings).

If a DHCP option is provided to the DHCP server but is invalid, the DHCP server may not transmit the corresponding RADIUS attribute in the access-request, or may transmit an invalid RADIUS server attribute.

# DHCP Server and RADIUS Translations

The table below lists the translations of DHCP options in a DHCP DISCOVER message to attributes in a RADIUS server access-request message.

***Table 7 DCHP DISCOVER to RADIUS Access-Request Translations***

| DHCP DISCOVER | RADIUS Access-Request |
|---|---|
| Virtual MAC address of the residential gateway | User-Name |
| Not Applicable | User-Password as configured on the DHCP server |
| Gateway address of the relay agent (giaddr field of a DHCP packet) | NAS-identifier |
| Hostname | Cisco AV pair client-hostname that equals the value of DHCP option 12 |
| Vendor class | Cisco AV pair dhcp-vendor-class that equals a hexadecimal-encoded value of DHCP option 60 |
| Client identifier | Cisco AV pair dhcp-client-id that equals the hexadecimal-encoded value of DHCP option 61 |
| DHCP relay information option that can contain VLAN parameter on the D-router | Cisco AV pair dhcp-relay-info that equals the hexadecimal-encoded value of DHCP option 82 |

The table below lists the translations of attributes in a RADIUS server access-accept message to DHCP options in a DHCP OFFER message.

*Table 8 RADIUS Access-Accept to DHCP OFFER Translations*

| RADIUS Access-Accept | DHCP OFFER |
|---|---|
| Framed-IP-Address | IP address of the residential gateway |
| Framed-IP-Netmask | Subnet mask (option 1) |
| Session-Timeout | IP address lease time (option 51) |
| Cisco AV pair session-duration in seconds, where seconds is greater than or equal to the number of seconds in the Session-Timeout attribute. | Provides session control on the DHCP server. This attribute is not transmitted to the DHCP client. |
| Framed-Route (RADIUS attribute 22). One route for each DHCP option is allowed with a maximum of 16 Framed-Route options for a RADIUS packet. | Contains up to 16 classless routes in one option (option 121) |

## RADIUS Profiles for DHCP Server RADIUS Proxy

When you configure RADIUS server user profiles for DHCP server RADIUS proxy, use the following guidelines:

- The Session-Timeout attribute must contain a value, in seconds. If this attribute is not present, the DHCP OFFER is not sent to the client.
- A RADIUS user profile must contain the following attributes:
    - Framed-IP-Address
    - Framed-IP-Netmask
    - Framed-Route
    - Session-Timeout
    - Session-Duration--Session-Duration is the Cisco AV pair session-duration = seconds, where seconds is the maximum time for the duration of a lease including all renewals. The value for Session-Duration must be greater than or equal to the Session-Timeout attribute value, and it cannot be zero.
- Additional RADIUS server attributes are allowed but are not required. The DHCP server ignores additional attributes that it does not understand. If a RADIUS server user profile contains a required attribute that is empty, the DHCP server does not generate the DHCP options.

# How to Configure DHCP Server RADIUS Proxy

## Configuring the DHCP Server for RADIUS-based Authorization

Perform this task on the DHCP server to configure address allocation for RADIUS-based authorization of DHCP leases.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service dhcp**
4. aaa new-model
5. **aaa group server radius** *group-name*
6. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
7. **exit**
8. **aaa authorization network** *method-list-name* **group** *group-name*
9. **aaa accounting network** *method-list-name* **start-stop group** *group-name*
10. **ip dhcp pool** name
11. **accounting** *method-list-name*
12. **authorization method** *method-list-name*
13. **authorization shared-password** password
14. **authorization username** string
15. exit
16. **interface** *type slot* **/** *subslot* **/** *port* [**.** *subinterface*]
17. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id*[**,** *vlan-id*[**-** *vlan-id*]]}
18. **ip address** *address mask*
19. no shutdown
20. **radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
21. **radius-server key** {*0 string* | *7 string* | *string*}
22. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **service dhcp**<br>**Example:**<br>`Router(config)#` **service dhcp** | Enables DHCP server and relay agent features on the router. By default, these features are enabled on the router. |
| **Step 4** | aaa new-model<br>**Example:**<br>`Router(config)#` **aaa new-model** | Enables the authentication, authorization, and accounting (AAA) access control system. |
| **Step 5** | **aaa group server radius** *group-name*<br>**Example:**<br>`Router(config)#` **aaa group server radius group1** | Specifies the name of the server host list to group RADIUS server hosts. Enters server-group configuration mode.<br>*group-name* --Character string to name the server group. The following words cannot be used as group name:<br>• auth-guest<br>• enable<br>• guest<br>• if-authenticated<br>• if-needed<br>• krb5<br>• krb-instance<br>• krb-telnet<br>• line<br>• local<br>• none<br>• radius<br>• rcmd<br>• tacacs<br>• tacacsplus |
| **Step 6** | **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]<br>**Example:**<br>`Router(config-sg)#` **server 10.1.1.1 auth-port 1700 acct-port 1701** | *Specifies the IP address of the RADIUS server host for the defined server group. Repeat this command for each RADIUS server host to associate with the server group.*<br>• *ip-address*-- IP address of the RADIUS server host.<br>• **auth-port** *port-number*-- (Optional) Specifies the UDP destination port for authentication requests. Default value is 1645.<br>• **acct-port** *port-number*-- (Optional) Specifies the UDP destination port for accounting requests. Default value is 1646. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **exit**<br>**Example:**<br>`Router(config-sg)#` **exit** | Exits server-group configuration mode. |
| **Step 8** | **aaa authorization network** *method-list-name* **group** *group-name*<br>**Example:**<br>`Router(config)#` **aaa authorization network auth1 group group1** | Specifies the methods list and server group for DHCP authorization.<br>• *method-list-name* --Character string to name the authorization methods list.<br>• **group** --Specifies a server group.<br>• *group-name* --Name of the server group to apply to DHCP authorization. |
| **Step 9** | **aaa accounting network** *method-list-name* **start-stop group** *group-name*<br>**Example:**<br>`Router(config)#` **aaa accounting network acct1 start-stop group group1** | Specifies that AAA accounting runs for all network service requests.<br>• *method-list-name* --Character string to name the accounting methods list.<br>• **start-stop** --Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice is received by the accounting server.<br>• **group** --Specifies a server group.<br>• *group-name* --Name of the server group to apply to DHCP accounting. |
| **Step 10** | **ip dhcp pool** name<br>**Example:**<br>`Router(config)#` **ip dhcp pool pool1** | Specifies a name for the DHCP server address pool. Enters DHCP pool configuration mode.<br>• *name* --Name of the pool. |
| **Step 11** | **accounting** *method-list-name*<br>**Example:**<br>`Router(config-dhcp)#` **accounting acct1** | Enables DHCP accounting.<br>• *method-list-name* --Name of the accounting methods list. |
| **Step 12** | **authorization method** *method-list-name*<br>**Example:**<br>`Router(config-dhcp)#` **authorization method auth1** | Enables DHCP authorization.<br>• *method-list-name* --Name of the authorization methods list. |

| | Command or Action | Purpose |
|---|---|---|
| Step 13 | **authorization shared-password** password<br>**Example:**<br>`Router(config-dhcp)#` **authorization shared-password cisco** | Specifies the password that is configured in the RADIUS user profile. |
| Step 14 | **authorization username** string<br>**Example:**<br>`Router(config-dhcp)#` **authorization username %%c-user1** | Specifies the parameters that RADIUS sends to a DHCP server when downloading configuration information for a DHCP client.<br>The *string* command argument contains the following formatting characters to insert DHCP client information:<br>• **%c-** --Ethernet address of the DHCP client (chaddr field)<br>• **%i-** --Inner VLAN ID from the DHCP relay information (option 82)<br>• %o---Outer VLAN ID from the DHCP relay information (option 82)<br>• **%p** --Port number from the DHCP relay information (option 82)<br>• **%g** --Gateway address of the DHCP relay agent (giaddr field)<br>• **%%** --Transmits the percent sign (%) character in the string sent to the RADIUS server<br>**Note** The percent (%) is a marker to insert the DHCP client information associated with the specified character. The % is not sent to the RADIUS server unless you specify the %% character. |
| Step 15 | exit<br>**Example:**<br>`Router(config-dhcp)#` **exit** | Exits DHCP pool configuration mode. |
| Step 16 | **interface** *type slot* / *subslot* / *port* [**.** *subinterface*]<br>**Example:**<br>`Router(config)#` **interface ethernet 1/10.0** | Configures an interface or subinterface that allows the DHCP client to obtain an IP address from the DHCP server. Enters interface or subinterface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 17** | **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** \| *vlan-id*[**,** *vlan-id*[**-** *vlan-id*]]}<br>**Example:**<br>`Router(config-subif)#` **encapsulation dot1q 100 second-dot1q 200** | (Optional) Enables IEEE 802.1Q encapsulation of traffic on a subinterface in a virtual LAN (VLAN).<br>• *vlan-id* --VLAN ID, integer in the range 1 to 4094. To separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs, enter a hyphen. (Optional) To separate each VLAN ID range from the next range, enter a comma.<br>• second-dot1q--Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature to configure an inner VLAN ID.<br>• **any** --Any second tag in the range 1 to 4094. |
| **Step 18** | **ip address** *address mask*<br>**Example:**<br>`Router(config-if)#` **ip address 192.168.1.1 255.255.255.0** | Specifies an IP address for an interface or subinterface.<br>• *address* is the IP address of the interface or subinterface.<br>• *mask* is the subnet address for the IP address. |
| **Step 19** | no shutdown<br>**Example:**<br>`Router(config-if)#` **no shutdown** | Enables the interface or subinterface. |
| **Step 20** | **radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]<br>**Example:**<br>`Router(config)#` **radius-server host 10.1.1.1** | Specifies a RADIUS server host.<br>• *ip-address* is the IP address of the RADIUS server host.<br>• **auth-port** *port-number*-- (Optional) Specifies the UDP destination port for authentication requests. Default value is 1645.<br>• **acct-port** *port-number*-- (Optional) Specifies the UDP destination port for accounting requests. Default value is 1646. |
| **Step 21** | **radius-server key** {*0 string* \| *7 string* \| *string*}<br>**Example:**<br>`Router(config)#` **radius-server key cisco** | Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.<br>• **0** *string*-- Specifies an unencrypted (cleartext) shared key<br>• **7** *string* **--** Specifies a hidden shared key.<br>**Note** Any key you enter must match the key on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. |
| **Step 22** | **exit** | Exits global configuration mode. |

# Monitoring and Maintaining the DHCP Server

Perform this task to verify and monitor DHCP server information:

### SUMMARY STEPS

1. **enable**
2. **debug ip dhcp server packet**
3. **debug ip dhcp server events**
4. **show ip dhcp binding** [*address*]
5. **show ip dhcp server statistics**
6. **show ip dhcp pool** [*name*]
7. **show ip route dhcp** [*address*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **debug ip dhcp server packet**<br>**Example:**<br>`Router# debug ip dhcp server packet` | (Optional) Enables DHCP server debugging. |
| Step 3 | **debug ip dhcp server events**<br>**Example:**<br>`Router#` **debug ip dhcp server events** | (Optional) Reports DHCP server events, such as address assignments and database updates. |
| Step 4 | **show ip dhcp binding** [*address*]<br>**Example:**<br>`Router#` **show ip dhcp binding** | (Optional) Displays a list of all bindings created on a specific DHCP server.<br>• Use the **show ip dhcp binding** command to display the IP addresses that have already been assigned. Verify that the address pool has not been exhausted. If necessary, re-create the pool to create a larger pool of addresses.<br>• Use the **show ip dhcp binding** command to display the lease expiration date and time of the IP address of the host. |
| Step 5 | **show ip dhcp server statistics**<br>**Example:**<br>`Router# show ip dhcp server statistics` | (Optional) Displays count information about server statistics and messages sent and received. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show ip dhcp pool** [*name*]<br>**Example:**<br>`Router# show ip dhcp pool` | (Optional) Displays the routes added to the routing table by the DHCP server and relay agent. |
| **Step 7** | **show ip route dhcp** [*address*]<br>**Example:**<br>`Router# show ip route dhcp [address]` | (Optional) Displays information about DHCP address pools. |

# Configuration Examples for DHCP Server Radius Proxy

## Configuring the DHCP Server Example

The following example shows how to configure a DHCP server for RADIUS-based authorization of DHCP leases. In this example, DHCP clients can attach to Ethernet interface 4/0/1 and Ethernet subinterface 4/0/3.10. The username string (%c-user1) specifies that the RADIUS server sends the Ethernet address of DHCP client named user1 to the DHCP server.

```
Router> enable
Router# configure terminal
Router(config)# service dhcp
Router(config)# aaa new-model
Router(config)# aaa group server radius rad1
Router(config-sg)# server 10.1.1.1
Router(config-sg)# server 10.1.5.10
Router(config-sg)# exit
Router(config)# aaa authorization network auth1 group group1
Router(config)# aaa accounting network acct1 start-stop group group1
Router(config)# aaa session-id common
Router(config)# ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100 timeout 5
!
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# accounting acct1
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
Router(config-dhcp)# authorization username %c-user1
Router(config-dhcp)# exit
!
Router(config)# interface ethernet4/0/1
Router(config-if)# ip address 15.0.0.1 255.255.255.0
Router(config-if)# exit
Router(config-if)# interface ethernet4/0/3.10

Router(config-if)# encapsulation dot1q 100 second-dot1q 200
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# radius-server host 10.1.3.2
Router(config)# radius-server key cisco
Router(config)# exit
```

## Configuring RADIUS Profiles Example

The following example shows how to configure a typical RADIUS user profile to send attributes in an access-accept message to the DHCP server:

```
DHCP-00059A3C7800 Password = “metta”
Service-Type = Framed,
Framed-Ip-Address = 10.3.4.5,
Framed-Netmask = 255.255.255.0,
Framed-Route = "0.0.0.0 0.0.0.0 10.3.4.1",
Session-Timeout = 3600,
Cisco:Cisco-Avpair = "session-duration=7200”
```

# Additional References

The following sections provide references related to the DHCP Server RADIUS Proxy feature.

### Related Documents

| Related Topic | Document Title |
|---|---|
| DHCP relay configuration | *Configuring the Cisco IOS XE DHCP Relay Agent* |
| DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this functionality. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs was not modified by this feature. | -- |

# Technical Assistance

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

# Feature Information for DHCP Server RADIUS Proxy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 9 Feature Information for the Cisco IOS XE DHCP Relay Agent*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Server RADIUS Proxy | Cisco IOS XE Release 2.4 | DHCP Server RADIUS Proxy enables a server to authorize remote clients and allocate addresses based on replies from the server.<br>In Cisco IOS XE 2.4, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br>The following commands were modified by this feature: **authorization method (dhcp)**, **authorization shared-password, authorization username (dhcp)**. |

# Glossary

**client** --A host trying to configure its interface (obtain an IP address) using DHCP or BOOTP protocols.

**DHCP** --Dynamic Host Configuration Protocol.

**giaddr** --Gateway IP address. The giaddr field of the DHCP message provides the DHCP server with information about the IP address subnet on which the client is to reside. It also provides the DHCP server with an IP address where the response messages are to be sent.

**MPLS** --Multiprotocol Label Switching. Emerging industry standard upon which tag switching is based.

**relay agent** --A router that forwards DHCP and BOOTP messages between a server and a client on different subnets.

**server** --DHCP or BOOTP server.

**VPN** --Virtual Private Network. Enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF** --VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router. Each VPN instantiated on the PE router has its own VRF.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# Configuring the Cisco IOS XE DHCP Client

Cisco IOS XE Dynamic Host Configuration Protocol (DHCP) client software provides the flexibility to include various configuration options for the DHCP client. A DHCP client is defined as an Internet host using DHCP to obtain configuration parameters such as an IP address. This module describes the concepts and tasks needed to configure the Cisco IOS XE DHCP client.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

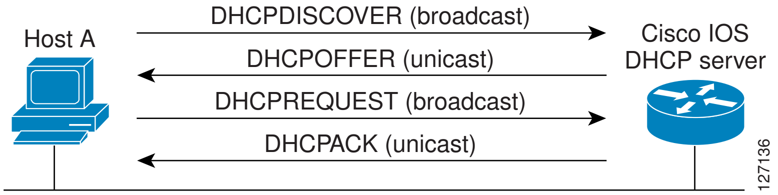
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Information About the DHCP Client

### DHCP Client Operation

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. A DHCP client is an Internet host using DHCP to obtain configuration parameters such as an IP address. The figure below shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server. The client, Host A, sends a DHCPDISCOVER broadcast message to locate a DHCP server. A DHCP server offers configuration parameters (such as an IP address, a MAC address, a domain name, and a lease for the IP address) to the client in a DHCPOFFER unicast message.

***Figure 10 DHCP Request for an IP Address from a DHCP Server***



A DHCP client may receive offers from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. Additionally, the offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address.

The client returns a formal request for the offered IP address to the DHCP server in a DHCPREQUEST broadcast message. The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client.

## DHCP Client Overview

The configurable DHCP client functionality allows a DHCP client to use a user-specified client identifier, class identifier, or suggested lease time when requesting an address from a DHCP server.

Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The DHCP client provides flexibility by allowing the following options to be configured for a DHCP client:

- Option 12--This option specifies the name of the client. The name may or may not be qualified with the local domain.
- Option 51--This option is used in a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for the IP address.
- Option 55--This option allows the DHCP client to request certain options from the DHCP server. The **ip dhcp client request** command allows the system administrator to turn off some of the requested options, thus removing them from the request list.
- Option 60--This option allows the user to configure the vendor class identifier string to use in the DHCP interaction.
- Option 61--This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain.

# How to Configure the DHCP Client

- Configuring the DHCP Client, page 134

## Configuring the DHCP Client

Perform this task to configure the DHCP client.

Cisco routers running Cisco IOS XE software include DHCP server and relay agent software, which are enabled by default. Your router can act as both the DHCP client and DHCP server. Use the **ip address dhcp** interface command to obtain IP address information for the configured interface.

You must configure the **ip dhcp client** commands before entering the **ip address dhcp** command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values. The **ip dhcp client** commands are checked only when an IP address is acquired from DHCP. If any of the **ip dhcp client** commands are entered after an IP address has been acquired from DHCP, it will not take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after the **ip address dhcp** command commandhas been configured.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip dhcp client client-id** {*interface-name*| **ascii** *string*| **hex** *string*}
5. **ip dhcp client class-id** {*string*| **hex** *string*}
6. **ip dhcp client lease** *days* [*hours*][*minutes*]
7. **ip dhcp client hostname** *host-name*
8. [**no**] **ip dhcp client request** *option-name*
9. **ip address dhcp**
10. **exit**
11. **ip dhcp compatibility lease-query client** {**cisco** | **standard**}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface GigabitEthernet 0/0/1` | Configures an interface type and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ip dhcp client client-id** {*interface-name*\| **ascii** *string*\| **hex** *string*}<br>**Example:**<br>`Router(config-if)# ip dhcp client client-id ascii mytest1` | (Optional) Specifies the client identifier.<br>• When you specify the **no** form of this command, the configuration is removed and the system returns to using the default form. It is not possible to configure the system to not include a client identifier. |
| **Step 5** | **ip dhcp client class-id** {*string*\| **hex** *string*}<br>**Example:**<br>`Router(config-if)# ip dhcp client class-id my-class-id` | (Optional) Specifies the class identifier. |
| **Step 6** | **ip dhcp client lease** *days* [*hours*][*minutes*]<br>**Example:**<br>`Router(config-if)# ip dhcp client lease 2` | (Optional) Configures the duration of the lease for an IP address that is requested from a DHCP client to a DHCP server. |
| **Step 7** | **ip dhcp client hostname** *host-name*<br>**Example:**<br>`Router(config-if)# ip dhcp client hostname router1` | (Optional) Specifies or modifies the host name sent in the DHCP message. |
| **Step 8** | [**no**] **ip dhcp client request** *option-name*<br>**Example:**<br>`Router(config-if)# no ip dhcp client request tftp-server-address` | (Optional) Configures a DHCP client to request an option from a DHCP server.<br>• The option name can be **tftp-server-address**, **netbios-nameserver**, **vendor-specific**, **static-route**, **domain-name**, **dns-nameserver**, or **router**. By default, all these options are requested. The **no** form of the command instructs the system to not request certain options. |
| **Step 9** | **ip address dhcp**<br>**Example:**<br>`Router(config-if)# ip address dhcp` | Acquires an IP address on an interface from DHCP. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | (Optional) Exits interface configuration mode. |
| **Step 11** | **ip dhcp compatibility lease-query client** {**cisco** \| **standard**}<br>**Example:**<br>`Router(config)# ip dhcp compatibility lease-query client standard` | (Optional) Configures a DHCP client to send a lease query according to RFC 4388 standard. |

- Troubleshooting Tips, page 137

## Troubleshooting Tips

To verify the configuration, you can use the **debug dhcp detail** EXEC command to display the DHCP packets that were sent and received. To display the server side of the DHCP interaction, use the **debug ip dhcp server packets** command.

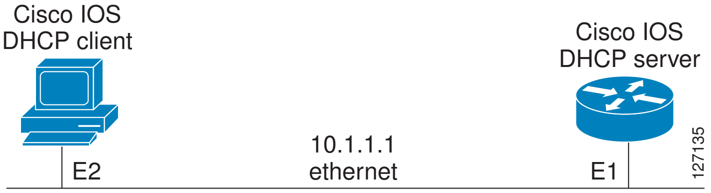
# Configuration Examples for the DHCP Client

- Configuring the DHCP Client Example, page 137
- Customizing the DHCP Client Configuration Example, page 138

## Configuring the DHCP Client Example

The figure below shows a simple network diagram of a DHCP client on an Ethernet LAN.

*Figure 11 Topology Showing DHCP Client with GigabitEthernet Interface*



On the DHCP server, the configuration is as follows:

```
ip dhcp pool 1
 network 10.1.1.0 255.255.255.0
 lease 1 6
```

On the DHCP client, the configuration is as follows on interface GigabitEthernet 0/0/0:

```
interface GigabitEthernet 0/0/0
 ip address dhcp
```

This configuration allows the DHCP client to acquire an IP address from the DHCP server through GigabitEthernet interface 0/0/0.

## Customizing the DHCP Client Configuration Example

The following example shows how to customize the DHCP client configuration with various options on GigabitEthernet interface 0/0/1:

```
interface GigabitEthernet 0/0/1
 ip dhcp client client-id ascii my-test1
 ip dhcp client class-id my-class-id
 ip dhcp client lease 0 1 0
 ip dhcp client hostname sanfran
 no ip dhcp client request tftp-server-address
 ip address dhcp
```

# Additional References

The following sections provide references related to the DHCP client.

### Related Documents

| Related Topic | Document Title |
|---|---|
| DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples. | *Cisco IOS IP Addressing Services Command Reference* |
| DHCP conceptual information | “DHCP Overview” module |
| DHCP server configuration | “Configuring the Cisco IOS XE DHCP Server” module |
| DHCP server on-demand address pools | “Configuring the DHCP Server On-Demand Address Pool Manager” module |
| DHCP relay agent configuration | “Configuring the Cisco IOS XE DHCP Relay Agent” module |
| DHCP advanced features | “Configuring DHCP Services for Accounting and Security” module |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| RFC 2131 | Dynamic Host Configuration Protocol |
| RFC 2132 | DHCP Options and BOOTP Vendor Extensions |

# Technical Assistance

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

# Feature Information for the Cisco IOS XE DHCP Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 10 Feature Information for the Cisco IOS XE DHCP Client*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Client | Cisco IOS XE Release 2.3 | A DHCP client is defined as an Internet host using DHCP to obtain configuration parameters such as an IP address.<br>The following command was introduced by this feature: **ip address dhcp** |
| Configurable DHCP Client | Cisco IOS XE Release 2.3 | The configurable DHCP client functionality allows a DHCP client to use a user-specified client identifier, class identifier, or suggested lease time when requesting an address from a DHCP server.<br>The following commands were introduced by this feature: **ip dhcp client class-id**, **ip dhcp client client-id**, **ip dhcp client hostname**, **ip dhcp client lease**, **ip dhcp client request** |

# Configuring DHCP Services for Accounting and Security

Cisco IOS XE software supports several capabilities that enhance DHCP security, reliability, and accounting in Public Wireless LANs (PWLANs). This functionality can also be used in other network implementations. This module describes the concepts and tasks needed to configure DHCP services for accounting and security.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Prerequisites for Configuring DHCP Services for Accounting and Security

Before you configure DHCP services for accounting and security, you should understand the concepts documented in the “DHCP Overview” module.

# Information About DHCP Services for Accounting and Security

## DHCP Operation in Public Wireless LANs

The configuration of DHCP in a public wireless LAN (PWLAN) simplifies the configuration of wireless clients and reduces the overhead necessary to maintain the network. DHCP clients are leased IP addresses by the DHCP server and then authenticated by the Service Selection Gateway (SSG), which allows the clients to access network services. The DHCP server and client exchange DHCP messages for IP address assignments. When a DHCP server assigns an IP address to a client, a DHCP binding is created. The IP address is leased to the client until the client explicitly releases the IP address and disconnects from the network. If the client disconnects without releasing the address, the server terminates the lease after the lease time is over. In either case, the DHCP server removes the binding and the IP address is returned to the pool.

## Security Vulnerabilities in Public Wireless LANs

As more people start using PWLANs, security becomes an important concern. Most implementations of PWLANs rely on DHCP for users to obtain an IP address while in a hot spot (such as a coffee shop, airport terminal, hotel, and so on) and use this IP address provided by the DHCP server throughout their session.

IP spoofing is a common technique used by hackers to spoof IP addresses. For example, customer A obtains an IP address from DHCP and has already been authenticated to use the PWLAN, but a hacker spoofs the IP address of customer A and uses this IP address to send and receive traffic. Customer A will still be billed for the service even though he or she is not using the service.

Address Resolution Protocol (ARP) table entries are dynamic by design. Request and reply ARP packets are sent and received by all the networking devices in a network. In a DHCP network, the DHCP server stores the leased IP address to the MAC address or the client-identifier of the client in the DHCP binding. But as ARP entries are learned dynamically, an unauthorized client can spoof the IP address given by the DHCP server and start using that IP address. The MAC address of this unauthorized client will replace the MAC address of the authorized client in the ARP table allowing the unauthorized client to freely use the spoofed IP address.

## DHCP Services for Security and Accounting Overview

DHCP security and accounting features have been designed and implemented to address the security concerns in PWLANs but also can be used in other network implementations.

DHCP accounting provides authentication, authorization, and accounting (AAA) and Remote Authentication Dial-In User Service (RADIUS) support for DHCP. The AAA and RADIUS support improves security by sending secure START and STOP accounting messages. The configuration of DHCP accounting adds a layer of security that allows DHCP lease assignment and termination to be triggered for the appropriate RADIUS START and STOP accounting records so that the session state is properly maintained by upstream devices, such as an SSG. This additional security can help to prevent unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases.

The DHCP Secured IP Address Assignment feature prevents IP spoofing by synchronizing the database of the DHCP server with the ARP table to avoid address hijacking. This secure ARP functionality adds an entry to the ARP table for a client when an address is allocated that can be deleted by the DHCP server only when a binding expires.

## DHCP Lease Limits

You can control the number of subscribers globally or on a per-interface basis by configuring a DHCP lease limit. This functionality allows an Internet service provider (ISP) to limit the number of leases available to clients per household or connection.

# How to Configure DHCP Services for Accounting and Security

## Configuring AAA and RADIUS for DHCP Accounting

Perform this task to configure AAA and RADIUS for DHCP accounting.

RADIUS provides the accounting capability for the transmission of secure START and STOP messages. AAA and RADIUS are enabled prior to the configuration of DHCP accounting but can also be enabled to secure an insecure DHCP network. The configuration steps in this section are required for configuring DHCP accounting in a new or existing network.

DHCP accounting introduces the attributes shown in the table below. These attributes are processed directly by the RADIUS server when DHCP accounting is enabled. These attributes can be monitored in the output of the debug radius command. The output will show the status of the DHCP leases and specific configuration details about the client. The accounting keyword can be used with the debug radius command to filter the output and display only DHCP accounting messages.

***Table 11 RADIUS Accounting Attributes***

| Attribute | Description |
|---|---|
| Calling-Station-ID | The output from this attribute displays the MAC address of the client. |
| Framed-IP-Address | The output from this attribute displays the IP address that is leased to the client. |
| Acct-Terminate-Cause | The output from this attribute displays the message “session-timeout” if a client does not explicitly disconnect. |

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
5. **server** *ip-address* **auth-port** *port-number* **acct-port** *port-number*
6. **exit**
7. **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** group-name
8. aaa session-id {common | unique}
9. ip radius source-interface type-number [vrf vrf-name]
10. radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]
11. radius-server retransmit number-of-retries

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br>**Example:**<br>`Router(config)# aaa new-model` | Enables the AAA access control model.<br>• DHCP accounting functions only in the access control model.<br>**Note** TACACS and extended TACACS commands are not available after this command is configured and are not supported by DHCP accounting. |
| **Step 4** | **aaa group server radius** *group-name*<br>**Example:**<br>`Router(config)# aaa group server radius RGROUP-1` | Creates a server group for AAA or TACACS+ services and enters server group configuration mode.<br>• The server group is created in this step so that accounting services can be applied. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **server** *ip-address* **auth-port** *port-number* **acct-port** *port-number*<br>**Example:**<br>`Router(config-sg-radius)# server 10.0.0.1 auth-port 1645 acct-port 1646` | Specifies the servers that are members of the server group that was created in Step 4.<br>• You must open port numbers for authorization and accounting. 1645 is the default port number for authorization, and 1646 is the default port number for accounting. The range of port numbers that can be specified is from 0 to 65535.<br>• The values entered for the auth-port port-number and acct-port port-number keywords and arguments must match the port numbers that will be configured in Step 10. |
| **Step 6** | **exit**<br>**Example:**<br>`Router(config-sg-radius)# exit` | Exits server group configuration mode and enters global configuration mode. |
| **Step 7** | **aaa accounting** {**system** \| **network** \| **exec** \| **connection** \| **commands** *level*} {**default** \| *list-name*} {**start-stop** \| **stop-only** \| **none**} [**broadcast**] **group** group-name<br>**Example:**<br>`Router(config)# aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1` | Configures RADIUS accounting for the specified server group.<br>• The RADIUS accounting server is specified in the first list-name argument (RADIUS-GROUP1), and the target server group is specified in the second group-name argument (RGROUP-1).<br>• This command enables start and stop accounting for DHCP accounting. The start-stop keyword enables the transmission of both START and STOP accounting messages. The stop-only keyword will enable the generation and verification of STOP accounting messages only. |
| **Step 8** | aaa session-id {common \| unique}<br>**Example:**<br>`Router(config)# aaa session-id common` | Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type. |
| **Step 9** | ip radius source-interface type-number [vrf vrf-name]<br>**Example:**<br>`Router(config)# ip radius source-interface GigabitEthernet 0/0/0` | Forces RADIUS to use the IP address of the specified interface for all outgoing RADIUS packets. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | radius-server host {hostname \| ip-address} [auth-port port-number] [acct-port port-number]<br>**Example:**<br>`Router(config)# radius-server host 10.1.1.1 auth-port 1645 acct-port 1646` | Specifies the radius server host.<br>• The values entered for the auth-port port-number and acct-port port-number keywords and arguments must match the port numbers that were configured in Step 5. |
| **Step 11** | radius-server retransmit number-of-retries<br>**Example:**<br>`Router(config)# radius-server retransmit 3` | Specifies the number of times that Cisco IOS XE software will look for RADIUS server hosts. |

- Troubleshooting Tips, page 146

## Troubleshooting Tips

To monitor and troubleshoot the configuration of RADIUS accounting, use the following command:

| Command | Purpose |
|---|---|
| **debug radius accounting**<br>`Router# debug radius accounting` | The debug radius command is used to display RADIUS events on the console of the router. These events provide information about RADIUS processes. DHCP accounting information can be filtered with the accounting keyword. START and STOP accounting message information will also be displayed. |

# Configuring DHCP Accounting

Perform this task to configure DHCP accounting.

DHCP accounting is enabled with the accounting DHCP pool configuration command. This command configures DHCP to operate with AAA and RADIUS to enable secure START and STOP accounting messages. This configuration adds a layer of security that allows DHCP lease assignment and termination to be triggered for the appropriate RADIUS START and STOP accounting records so that the session state is properly maintained by upstream devices, such as the SSG.

DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis.

You must configure an SSG for client authentication. AAA and RADIUS must be enabled before DHCP accounting will operate.

**Note** The following restrictions apply to DHCP accounting:

- DHCP accounting can be configured only for DHCP network pools in which bindings are created automatically and destroyed upon lease termination or when the client sends a DHCPRELEASE message.
- DHCP bindings are destroyed when the clear ip dhcp binding or no service dhcp commands are entered, which also triggers an accounting STOP message. You should exercise caution when entering these commands if a pool is configured with DHCP accounting, as these commands will clear active leases.

>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **accounting** *method-list-name*

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip dhcp pool** *pool-name*<br>**Example:**<br>`Router(config)# ip dhcp pool WIRELESS-POOL` | Configures a DHCP address pool and enters DHCP pool configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **accounting** *method-list-name*<br>**Example:**<br>`Router(dhcp-config)# accounting RADIUS-GROUP1` | Enables DHCP accounting if the specified server group is configured to run RADIUS accounting.<br>• The example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group. See Step 7 in the "Configuring AAA and RADIUS for DHCP Accounting" configuration task table for more details. |

# Verifying DHCP Accounting

Perform this task to verify the DHCP accounting configuration.

The debug radius, debug ip dhcp server events, debug aaa accounting, debug aaa id commands do not need to be issued together or in the same session as there are differences in the information that is provided. These commands, however, can be used to display DHCP accounting start and stop events, AAA accounting messages, and information about AAA and DHCP hosts and clients. See the "RADIUS Accounting Attributes" section of this module for a list of AAA attributes that have been introduced by DHCP accounting. The show running-config | begin dhcp command can be used to display the local DHCP configuration including the configuration of DHCP accounting.

### SUMMARY STEPS

1. **enable**
2. **debug radius accounting**
3. **debug ip dhcp server events**
4. **debug aaa accounting**
5. **debug aaa id**
6. **show running-config | begin dhcp**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables higher privilege levels, such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **debug radius accounting**<br>**Example:**<br>`Router# debug radius accounting` | Displays RADIUS events on the console of the router.<br>• These events provide information about RADIUS processes. DHCP accounting information can be filtered with the accounting keyword. START and STOP accounting messages will be displayed in the output. |

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **debug ip dhcp server events**<br>**Example:**<br>`Router# debug ip dhcp server events` | Displays DHCP IP address assignments, DHCP lease expirations, and DHCP database changes. |
| Step 4 | **debug aaa accounting**<br>**Example:**<br>`Router# debug aaa accounting` | Displays AAA accounting events.<br>• START and STOP accounting messages will be displayed in the output. |
| Step 5 | **debug aaa id**<br>**Example:**<br>`Router# debug aaa id` | Displays AAA events as they relate to unique AAA session IDs. |
| Step 6 | **show running-config \| begin dhcp**<br>**Example:**<br>`Router# show running-config \| begin dhcp` | The show running-config command is used to display the local configuration of the router. The sample output is filtered with the begin keyword to start displaying output at the DHCP section of the running configuration. |

# Securing ARP Table Entries to DHCP Leases

Perform this task to secure ARP table entries to DHCP leases in the DHCP database.

When the **update arp** command is used, ARP table entries and their corresponding DHCP leases are secured automatically for all new leases and DHCP bindings. However, existing active leases are not secured. These leases are still insecure until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically. If this command is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool -name*
4. **update arp**
5. **renew deny unknown**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip dhcp pool** *pool -name*<br>**Example:**<br>`Router(config)# ip dhcp pool WIRELESS-POOL` | Configures a DHCP address pool and enters DHCP pool configuration mode. |
| **Step 4** | **update arp**<br>**Example:**<br>`Router(dhcp-config)# update arp` | Secures insecure ARP table entries to the corresponding DHCP leases.<br>• Existing active DHCP leases will not be secured until they are renewed. Using the no update arp command will change secured ARP table entries back to dynamic ARP table entries. |
| **Step 5** | **renew deny unknown**<br>**Example:**<br>`Router(dhcp-config)# renew deny unknown` | (Optional) Configures the renewal policy for unknown clients.<br>• See the Troubleshooting Tips, page 146 section for information about when to use this command. |

- Troubleshooting Tips, page 150

## Troubleshooting Tips

In some usage scenarios, such as a wireless hotspot, where both DHCP and secure ARP are configured, a connected client device might go to sleep or suspend for a period of time. If the suspended time period is greater than the secure ARP timeout (default of 91 seconds), but less than the DHCP lease time, the client can awake with a valid lease, but the secure ARP timeout has caused the lease binding to be removed because the client has been inactive. When the client awakes, the client still has a lease on the client side but is blocked from sending traffic. The client will try to renew its IP address but the DHCP server will ignore the request because the DHCP server has no lease for the client. The client must wait for the lease to expire before being able to recover and send traffic again.

To remedy this situation, use the **renew deny unknown** command in DHCP pool configuration mode. This command forces the DHCP server to reject renewal requests from clients if the requested address is present at the server but is not leased. The DHCP server sends a DHCPNAK denial message to the client, which forces the client back to its initial state. The client can then negotiate for a new lease immediately, instead of waiting for its old lease to expire.

# Configuring a DHCP Lease Limit to Control the Number of Subscribers on an Interface

Perform this task to limit the number of DHCP leases allowed on an interface.

This feature allows an ISP to limit the number of leases available to clients per household or connection on an interface.

If this feature is enabled on the Cisco IOS XE DHCP server directly connected to clients through unnumbered interfaces, the server allocates addresses and increments the number of leases per subinterface. If a new client tries to obtain an IP address, the server will not offer an IP address if the number of leases on the subinterface has already reached the configured lease limit.

**Note** This feature is not supported on numbered interfaces. The lease limit can be applied only to ATM with RBE unnumbered interfaces or serial unnumbered interfaces.

>

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease log**
4. **interface** *type number*
5. **ip dhcp limit lease** *lease-limit*
6. **end**
7. **show ip dhcp limit lease** [*type number*]
8. **show ip dhcp server statistics** [*type number*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **ip dhcp limit lease log**<br>**Example:**<br>`Router(config)# ip dhcp limit lease log` | (Optional) Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded.<br>• If this command is configured, any lease limit violations will display in the output of the **show ip dhcp limit lease** command. |
| **Step 4** | **interface** *type number*<br>**Example:**<br>`Router(config)# interface Serial0/0/0` | Enters interface configuration mode. |
| **Step 5** | **ip dhcp limit lease** *lease-limit*<br>**Example:**<br>`Router(config-if)# ip dhcp limit lease 6` | Limits the number of leases offered to DHCP clients per interface.<br>• The interface configuration will override any global setting specified by the **ip dhcp limit lease per interface** global configuration command. |
| **Step 6** | **end**<br>**Example:**<br>`Router(config-if)# end` | Exits the configuration mode and returns to privileged EXEC mode. |
| **Step 7** | **show ip dhcp limit lease** [*type number*]<br>**Example:**<br>`Router# show ip dhcp limit lease Serial0/0/0` | (Optional) Displays the number of times the lease limit threshold has been violated.<br>• You can use the **clear ip dhcp limit lease** privileged EXEC command to manually clear the stored lease violation entries. |
| **Step 8** | **show ip dhcp server statistics** [*type number*]<br>**Example:**<br>`Router# show ip dhcp server statistics Serial0/0/0` | (Optional) Displays DHCP server statistics. |

- Troubleshooting Tips, page 152

## Troubleshooting Tips

You can use the **debug ip dhcp server packet** and **debug ip server events** commands to troubleshoot the DHCP lease limit.

# Configuration Examples for DHCP Services for Accounting and Security

## Configuring AAA and RADIUS for DHCP Accounting Example

The following example shows how to configure AAA and RADIUS for DHCP accounting:

```
aaa new-model
aaa group server radius RGROUP-1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 exit
aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1
aaa session-id common
ip radius source-interface GigabitEthernet0/0/0
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
exit
```

## Configuring DHCP Accounting Example

DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis. The following example shows how to configure DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group.

```
ip dhcp pool WIRELESS-POOL
 accounting RADIUS-GROUP1
 exit
```

## Verifying DHCP Accounting Example

DHCP accounting is enabled after both RADIUS and AAA for DHCP are configured. DHCP START and STOP accounting generation information can be monitored with the **debug radius accounting** and **debug ip dhcp server events**commands. See the "RADIUS Accounting Attributes" section of this module for a list of AAA attributes that have been introduced by DHCP accounting.

The following is sample output from the **debug radius accounting**command. The output shows the DHCP lease session ID, the MAC address, and the IP address of the client interface.

```
00:00:53: RADIUS: Pick NAS IP for uid=2 tableid=0 cfg_addr=10.0.18.3 best_addr=0.0.0.0
00:00:53: RADIUS(00000002): sending
00:00:53: RADIUS(00000002): Send to unknown id 21645/1 10.1.1.1 :1646, Accounting-
Request, len 76
00:00:53: RADIUS: authenticator C6 FE EA B2 1F 9A 85 A2 - 9A 5B 09 B5 36 B5 B9 27
00:00:53: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:00:53: RADIUS: Framed-IP-Address [8] 6 10.0.0.10
00:00:53: RADIUS: Calling-Station-Id [31] 16 "00000c59df76"
00:00:53: RADIUS: Acct-Status-Type [40] 6 Start [1]
00:00:53: RADIUS: Service-Type [6] 6 Framed [2]
00:00:53: RADIUS: NAS-IP-Address [4] 6 10.0.18.3
00:00:53: RADIUS: Acct-Delay-Time [41] 6 0
```

The following is sample output from the **debug ip dhcp server events**command. The output was generated on a DHCP server and shows an exchange of DHCP messages between the client and server to negotiate a DHCP lease. The acknowledgment that confirms to the DHCP server that the client has accepted the assigned IP address triggers the accounting START message. It is shown in the last line of the following output:

```
00:45:50:DHCPD:DHCPDISCOVER received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 on
interface GigabitEthernet0/0/0.
00:45:52:DHCPD:assigned IP address 10.10.10.16 to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.
00:45:52:DHCPD:Sending DHCPOFFER to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31(10.10.10.16)
00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.
00:45:52:DHCPD:DHCPREQUEST received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.
00:45:52:DHCPD:Sending DHCPACK to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31
(10.10.10.16).
00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.
00:45:52:DHCPD:triggered Acct Start for 0001.42c9.ec75 (10.10.10.16).
```

The following is sample output from the **debug ip dhcp server events**command. The output was generated on a DHCP server and shows the receipt of an explicit release message from the DHCP client. The DHCP server triggers an accounting STOP message and then returns the IP address to the DHCP pool. Information about the accounting STOP message is shown in the third line of the following output:

```
00:46:26:DHCPD:DHCPRELEASE message received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 (10.10.10.16)
00:46:26:DHCPD:triggered Acct Stop for (10.10.10.16).
00:46:26:DHCPD:returned 10.10.10.16 to address pool WIRELESS-POOL.
```

## Configuring a DHCP Lease Limit Examples

In the following example, 5 DHCP clients are allowed to receive IP addresses. If a sixth client tries to obtain an IP address, the DHCPDISCOVER messages will not be forwarded to the DHCP server and a trap will be sent to the SNMP manager.

```
ip dhcp limit lease log
!
ip dhcp pool pool1
 network 10.1.1.0 255.255.255.0
!
interface loopback0
 ip address 10.1.1.1 255.255.255.0
!
interface serial 0/0.2 point-to-point
 ip dhcp limit lease 5
 ip unnumbered loopback0
 exit
snmp-server enable traps dhcp interface
```

# Additional References

The following sections provide references related to configuring DHCP services for accounting and security.

### Related Documents

| Related Topic | Document Title |
|---|---|
| ARP commands: complete command syntax, command modes, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |
| DHCP commands: complete command syntax, command modes, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |
| DHCP conceptual information | “DHCP Overview” module |
| DHCP server configuration | “Configuring the Cisco IOS XE DHCP Server” module |
| DHCP ODAP configuration | “Configuring the DHCP Server On-Demand Address Pool Manager” module |
| DHCP client configuration | “Configuring the Cisco IOS XE DHCP Client” module |
| DHCP relay agent configuration | “Configuring the Cisco IOS XE DHCP Relay Agent” module |
| AAA and RADIUS configuration tasks | *Cisco IOS Security Configuration Guide* |
| AAA and RADIUS commands: complete command syntax, command mode, defaults, usage guidelines, and examples | *Cisco IOS Security Command Reference* |

### Standards

| Standards | Title |
|---|---|
| No new or modified standards are supported by this functionality. | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | -- |

# Technical Assistance

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

# Feature Information for DHCP Services for Accounting and Security

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 12 Feature Information for DHCP Services for Accounting and Security*

| Feature Name | Releases | Feature Configuration Information |
|---|---|---|
| DHCP Per Interface Lease Limit and Statistics | Cisco IOS XE Release 2.1 | This feature limits the number of DHCP leases offered to DHCP clients on an interface. DHCP server statistics reporting was enhanced to display interface-level statistics.<br>The following commands were introduced or modified by this feature: **ip dhcp limit lease**, **ip dhcp limit lease log**, **clear ip dhcp limit lease**, **show ip dhcp limit lease**, and **show ip dhcp server statistics**. |
| DHCP Accounting | Cisco IOS XE Release 2.1 | DHCP accounting introduces AAA and RADIUS support for DHCP configuration.<br>The following command was introduced by this feature: **accounting**. |
| DHCP Secured IP Address Assignment | Cisco IOS XE Release 2.3 | DHCP secure IP address assignment provides the capability to secure ARP table entries to DHCP leases in the DHCP database. This feature secures and synchronizes the MAC address of the client to the DHCP binding, preventing unauthorized clients or hackers from spoofing the DHCP server and taking over a DHCP lease of an authorized client.<br>The following command was introduced by this feature: **update arp**.<br>The following command was modified by this feature: **show ip dhcp server statistics**. |

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

# ISSU and SSO--DHCP High Availability Features

Cisco IOS XE Release 2.1 and 2.3 introduce the following series of Dynamic Host Configuration Protocol (DHCP) High Availability features:

- ISSU--DHCP Server
- SSO--DHCP Server
- ISSU--DHCP Relay on Unnumbered Interface
- SSO--DHCP Relay on Unnumbered Interface
- ISSU--DHCP Proxy Client
- SSO--DHCP Proxy Client
- ISSU--DHCP ODAP Client and Server
- SSO--DHCP ODAP Client and Server

These features are enabled by default when the redundancy mode of operation is set to Stateful Switchover (SSO).

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Prerequisites for DHCP High Availability

- The Cisco IOS XE In-Service Software Upgrade (ISSU) process must be configured and working properly. See the “Cisco IOS XE In-Service Software Upgrade Process” feature module for more information.
- Stateful Switchover (SSO) must be configured and working properly. See the “Stateful Switchover” feature module for more information.
- Nonstop Forwarding (NSF) must be configured and working properly. See the “Cisco Nonstop Forwarding” feature module for more information.

# Restrictions for DHCP High Availability

The DHCP high availability features do not support DHCP accounting or DHCP authorized Address Resolution Protocol (ARP).

# Information About DHCP High Availability

## ISSU

The ISSU process allows Cisco IOS XE software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS XE software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

## SSO

SSO refers to the implementation of Cisco IOS XE software that allows applications and features to maintain a defined state between an active and standby Route Processor (RP).

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active RP while the other RP is designated as the standby RP, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

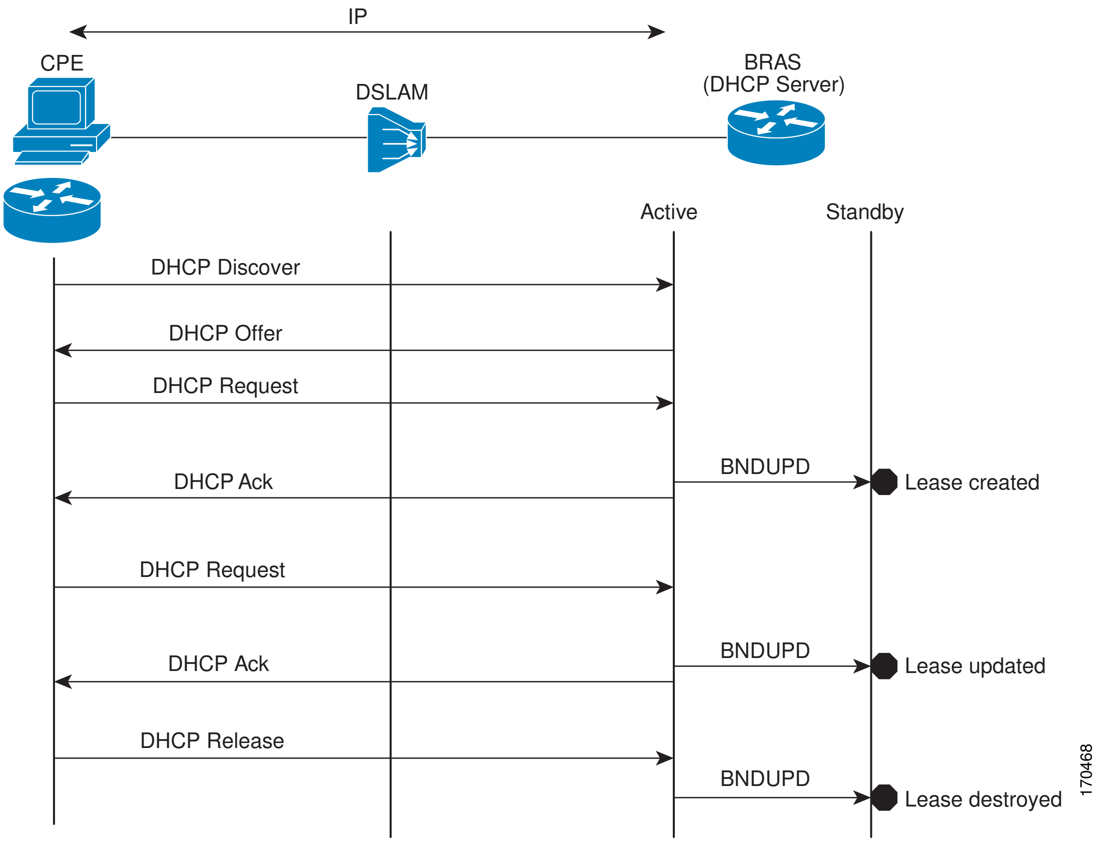
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

# ISSU and SSO--DHCP Server

The DHCP server that is ISSU and SSO aware is able to detect when a router is failing over to the standby RP and preserve the DHCP lease across a switchover event.

Each DHCP binding is synchronized and re-created from the active RP to the standby RP upon lease commit. The figure below illustrates this process. The lease extension and release are also synchronized to the standby RP.

***Figure 12 DHCP Server Maintaining States Between the Active and Standby Route Processor***



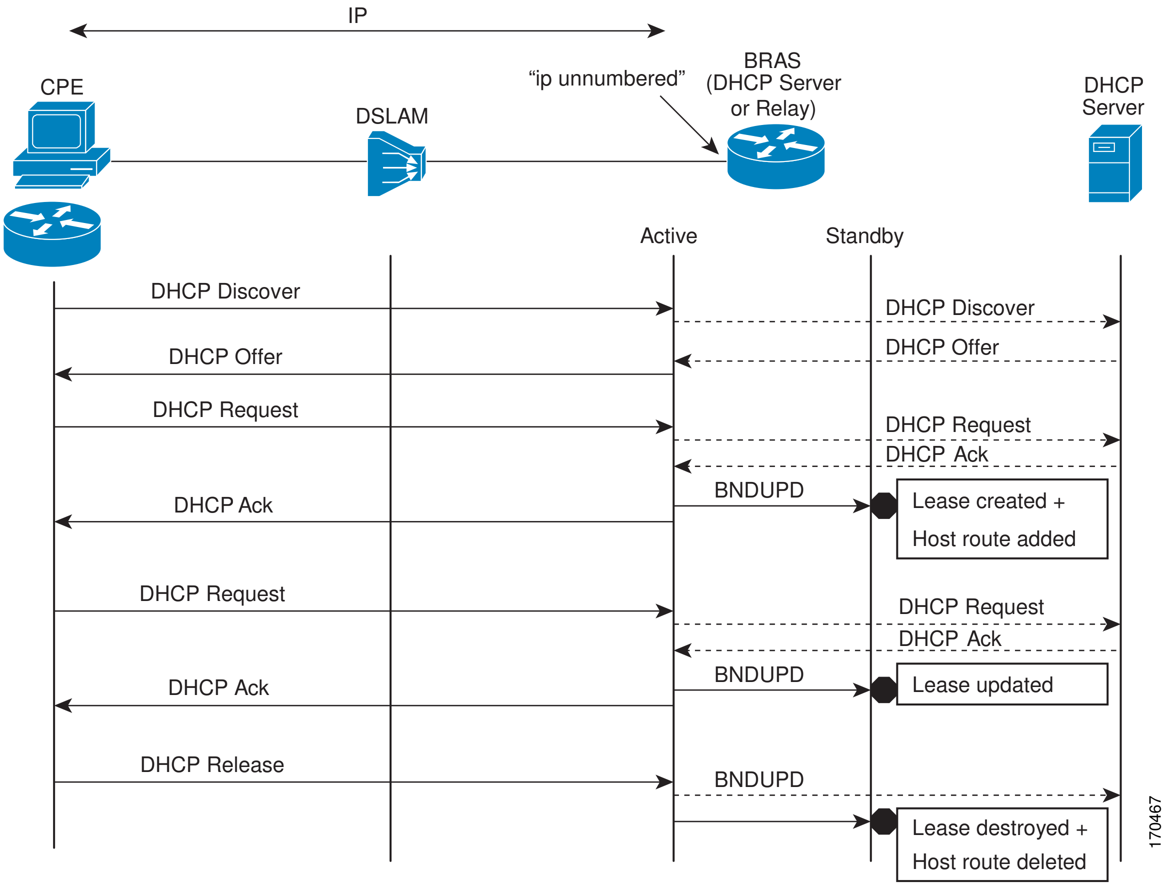
# ISSU and SSO--DHCP Relay on Unnumbered Interface

The DHCP relay agent supports the use of unnumbered interfaces. For DHCP clients connected through the unnumbered interfaces, the DHCP relay agent automatically adds a static host route once the DHCP client obtains an address, specifying the unnumbered interface as the outbound interface. The route is automatically removed once the lease time expires or when the client releases the address.

The **ip helper-address** interface configuration command must be configured on the unnumbered interface to enable the Cisco IOS XE DHCP relay agent on unnumbered interfaces. See the “Configuring the Cisco IOS XE DHCP Relay Agent” configuration module for more information.

The ISSU and SSO DHCP relay on unnumbered interface functionality adds high availability support for host routes to clients connected through unnumbered interfaces. The DHCP relay agent can now detect when a router is failing over to the standby RP and keep the states related to unnumbered interfaces. The figure below illustrates the process.

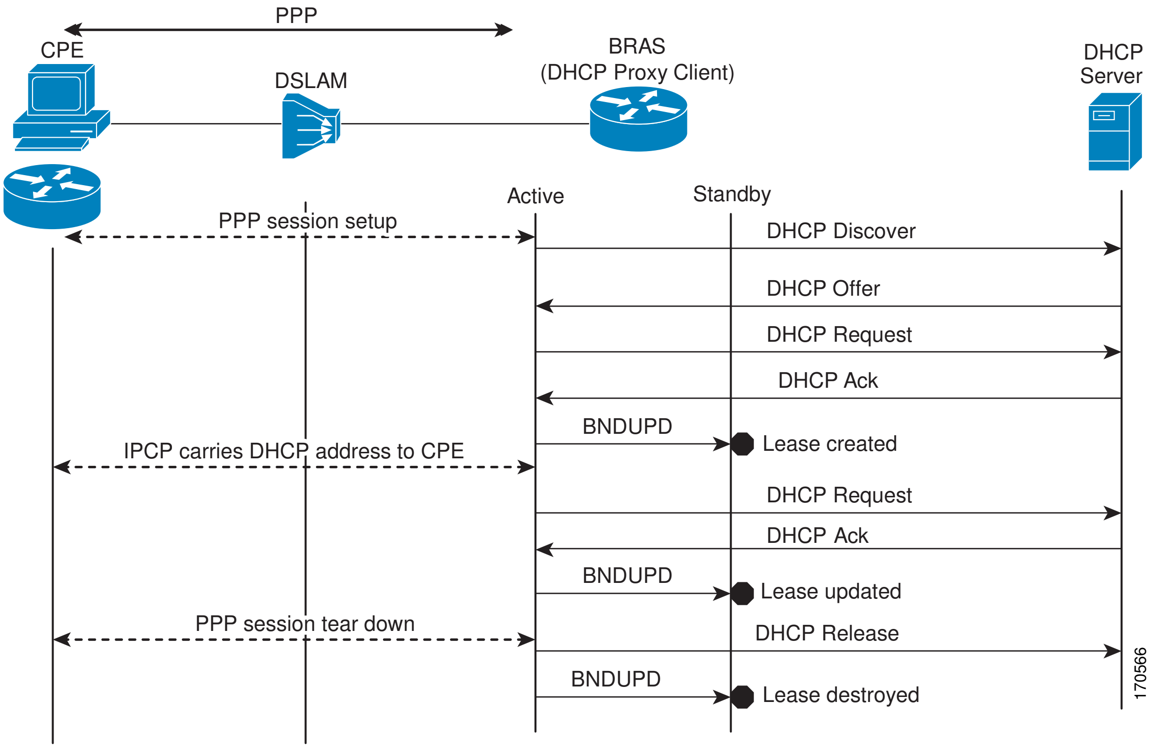
***Figure 13 DHCP Maintaining States with an IP Unnumbered Interface***



# ISSU and SSO--DHCP Proxy Client

The DHCP proxy client enables the router to obtain a lease for configuration parameters from a DHCP server for a remote Point-to-Point Protocol (PPP) client. The DHCP proxy client that is ISSU and SSO aware is able to request a lease from the DHCP server and the state of the lease is synchronized between the active and standby RP. The figure below illustrates the process.

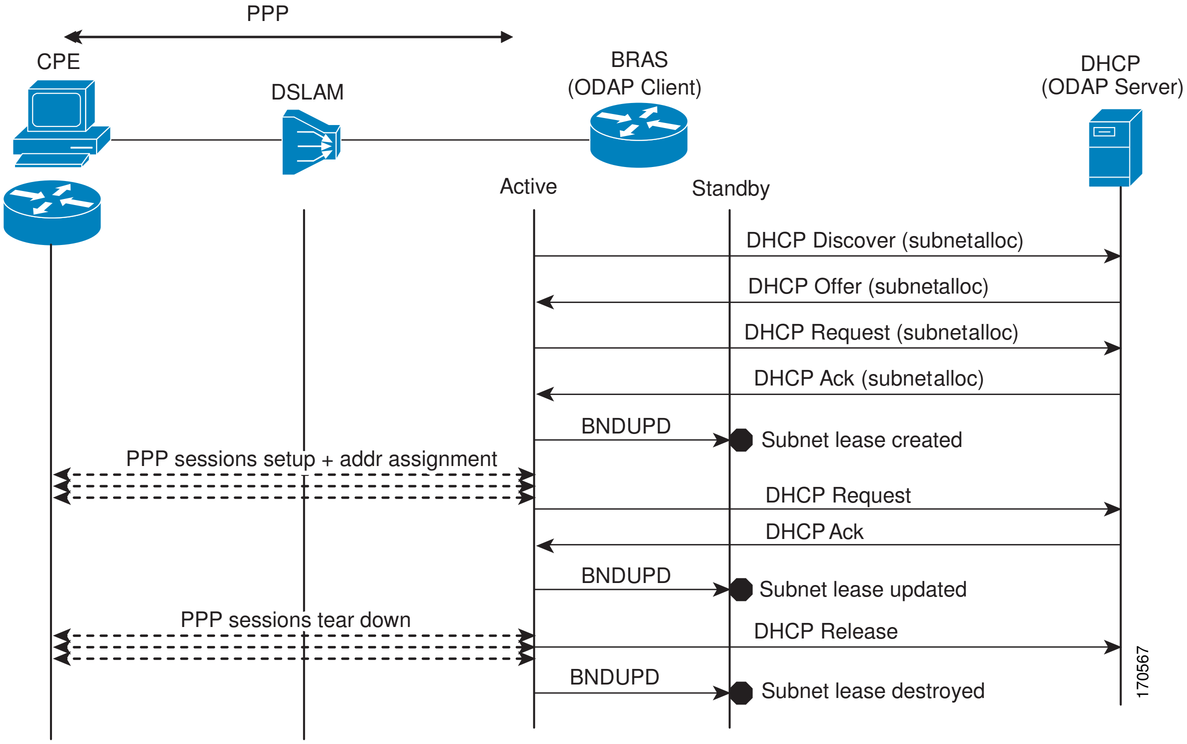
*Figure 14* *DHCP Proxy Client Lease Synchronization*



## ISSU and SSO--DHCP ODAP Client and Server

The DHCP on-demand address pool (ODAP) client that is ISSU and SSO aware can request a lease for a subnet from the DHCP ODAP server. After the DHCP ODAP server allocates the subnet to the client, the state of the lease is synchronized between the active and standby RP through binding updates. Following a switchover event, the DHCP ODAP client can continue to allocate IP addresses from the same subnets and also continue to renew the subnets from the DHCP ODAP server. The figure below illustrates the process.

***Figure 15 ODAP Subnet Lease Synchronization***



# How to Configure DHCP High Availability

There are no configuration tasks. The DHCP high availability features are enabled by default when the redundancy mode of operation is set to SSO.

# Configuration Examples for DHCP High Availability

There are no configuration examples for DHCP high availability features.

# Additional References

The following sections provide references related to DHCP high availability features.

### Related Documents

| Related Topic | Document Title |
|---|---|
| DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | *Cisco IOS IP Addressing Services Command Reference* |
| DHCP conceptual and configuration information | *Cisco IOS XE IP Addressing Services Configuration Guide* |
| In-Service Software Upgrade process conceptual and configuration information | "Cisco IOS XE In Service Software Upgrade Process" module |
| Nonstop Forwarding conceptual and configuration information | "Cisco Nonstop Forwarding" module |
| Stateful switchover conceptual and configuration information | "Stateful Switchover" module |

### Standards

| Standard | Title |
|---|---|
| No new or modified standards are supported by this feature. | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported by this feature. | -- |

### Technical Assistance

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

# Feature Information for DHCP High Availability Features

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 13 Feature Information for DHCP High Availability Features*

| Feature Name | Releases | Feature Information |
|---|---|---|
| ISSU--DHCP Server | Cisco IOS XE Release 2.1 | The DHCP server has been enhanced to support ISSU. |
| SSO--DHCP Server | Cisco IOS XE Release 2.1 | The DHCP server has been enhanced to support SSO. |
| ISSU--DHCP Relay on Unnumbered Interface | Cisco IOS XE Release 2.3 | The DHCP relay on unnumbered interface has been enhanced to support ISSU. |
| SSO--DHCP Relay on Unnumbered Interface | Cisco IOS XE Release 2.1 | The DHCP relay on unnumbered interface has been enhanced to support SSO. |
| ISSU--DHCP Proxy Client | Cisco IOS XE Release 2.3 | The DHCP proxy client has been enhanced to support ISSU. |
| SSO--DHCP Proxy Client | Cisco IOS XE Release 2.3 | The DHCP proxy client has been enhanced to support SSO. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| ISSU--DHCP ODAP Client and Server | Cisco IOS XE Release 2.3 | The DHCP ODAP client and server have been enhanced to support ISSU. |
| SSO--DHCP ODAP Client and Server | Cisco IOS XE Release 2.3 | The DHCP ODAP client and server have been enhanced to support SSO. |

# Glossary

**CPE** --customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the service provider, installed at customer sites, and connected to the network.

**DSLAM** --digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

**ISSU** --In Service Software Upgrade. ISSU is a process that allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues.

**ODAP** --On-Demand Address Pool. ODAPs enable pools of IP addresses to be dynamically increased or reduced in size depending on the address utilization level. Once configured, the ODAP is populated with one or more subnets leased from a source server and is ready to serve address requests from DHCP clients or from PPP sessions.

**RP** --Route Processor. A generic term for the centralized control unit in a chassis.

**SSO** --Stateful Switchover. SSO refers to the implementation of Cisco IOS software that allows applications and features to maintain a defined state between an active and standby RP. When a switching occurs, forwarding and sessions are maintained. SSO makes an RP failure undetectable to the network.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.