IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15.0SY

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 DHCP.

Information About DHCP

DHCP Overview

Cisco routers running Cisco IOS software include DHCP server and relay agent software. The Cisco IOS 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 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 DHCP

The Cisco IOS 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.

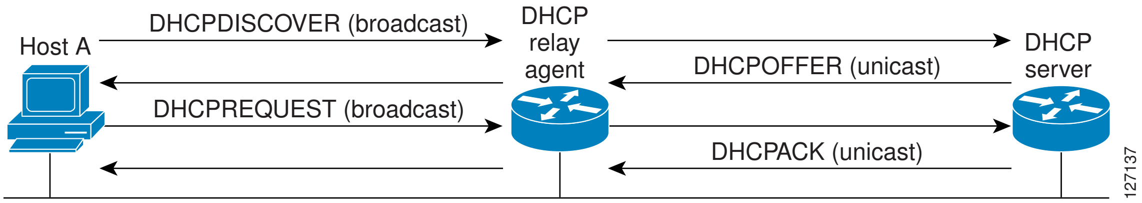
DHCP Server Relay Agent and Client Operation

DHCP provides a framework for passing configuration information dynamically to hosts on a TCP/IP network. A DHCP client is an Internet host that uses 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. In 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 a DHCPNAK denial broadcast message to the client, which means that 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 nonvolatile 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 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 DHCP implementation also allows most DHCP server options to be customized. For example, the TFTP server, which stores the Cisco IOS image, can be customized with option 150 to support intelligent IP phones.

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 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” appendix in the *Network Registrar User’s Guide* , Release 6.2.

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.

DHCP Option Name	DHCP Option Code	Description
NetBIOS over TCP/IP name server option	44	Specifies a list of RFC 1001/1002 NetBIOS name servers listed in order of 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.

The table below lists the option codes that are not used for DHCP pool configuration:

Table 2 DHCP Server Options--Not Used for DHCP Pool Configuration

Macro Name	DHCP Option Code
DHCPOPT_PAD	0
DHCPOPT_SUBNET_MASK	1
DHCPOPT_DEFAULT_ROUTER	3
DHCPOPT_DOMAIN_NAME_SERVER	6
DHCPOPT_HOST_NAME	12
DHCPOPT_DOMAIN_NAME	15
DHCPOPT_NETBIOS_NAME_SERVER	44
DHCPOPT_NETBIOS_NODE_TYPE	46
DHCPOPT_REQUESTED_ADDRESS	50
DHCPOPT_LEASE_TIME	51
DHCPOPT_OPTION_OVERLOAD	52
DHCPOPT_MESSAGE_TYPE	53

Macro Name	DHCP Option Code
DHCPOPT_SERVER_IDENTIFIER	54
DHCPOPT_RENEWAL_TIME	58
DHCPOPT_REBINDING_TIME	59
DHCPOPT_CLIENT_IDENTIFIER	61
DHCPOPT_RELAY_INFORMATION	82
DHCPOPT_END	255

DHCP Server On-Demand Address Pool Management Overview

The Cisco IOS 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 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 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.

DHCP Services for Accounting and Security Overview

Cisco IOS software supports several new capabilities that enhance DHCP accounting, reliability, and security in Public Wireless LANs (PWLANs). This functionality can also 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 a Service Selection Gateway (SSG). This additional security can help to prevent unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases.

Three other features have been designed and implemented to address the security concerns in PWLANs. The first feature secures ARP table entries to DHCP leases in the DHCP database. The secure ARP functionality prevents IP spoofing by synchronizing the database of the DHCP server with the ARP table to avoid address hijacking. Secure ARP 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.

The second feature is DHCP authorized ARP. This functionality provides a complete solution by addressing the need for DHCP to explicitly know when a user logs out. Before the introduction of DHCP authorized ARP, there was no mechanism to inform the DHCP server if a user had left the system ungracefully, which could result in excessive billing for a customer that had logged out but the system had not detected the log out. To prevent this problem, DHCP authorized ARP sends periodic ARP messages on a per-minute basis to determine if a user is still logged in. Only authorized users can respond to the ARP request. ARP responses from unauthorized users are blocked at the DHCP server providing an extra level of security.

In addition, DHCP authorized ARP disables dynamic ARP learning on an interface. The address mapping can be installed only by the authorized component specified by the **arp authorized** interface configuration command. DHCP is the only authorized component currently allowed to install ARP entries.

The third feature is ARP autologoff, which adds finer control for probing when authorized users log out. The **arp probe interval** command specifies when to start a probe (the timeout), how frequent a peer is probed (the interval), and the maximum number of retries (the count).

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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 DHCP Server” module
DHCP relay agent configuration	“Configuring the Cisco IOS DHCP Relay Agent” module
DHCP client configuration	“Configuring the Cisco IOS 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
DHCP enhancements for edge-session management	“Configuring DHCP Enhancements for Edge-Session Management” module
DHCP options	“DHCP Options” appendix in the *Network Registrar User’s Guide* , Release 6.1.1

Standards

Standard	Title
No new or modified standards are supported.	--

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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 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 DHCP Server

Cisco routers running Cisco IOS software include Dynamic Host Configuration Protocol (DHCP) server and relay agent software. The Cisco IOS 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 DHCP server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 DHCP server, you should understand the concepts documented in the “DHCP Overview” module.

The Cisco IOS 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.

Port 67 (the server port) is closed in the Cisco IOS DHCP/BOOTP default configuration. There are two logical parts to the **service dhcp** command: service enabled and service running. The DHCP service is enabled by default, but port 67 is not opened until the DHCP service is running. If the service is running, the **show ip sockets details** or **show sockets detail** command displays port 67 as open.

The Cisco IOS 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 DHCP Server

Overview of the DHCP Server

TheCisco IOS 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 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.

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 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 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 DHCP server can also use option 82 as a means to provide additional information to properly allocate IP addresses to DHCP clients.

How to Configure the Cisco IOS DHCP Server

- Configuring Manual Bindings, page 27
- Configuring DHCP Static Mapping, page 29
- Customizing DHCP Server Operation, page 34
- Configuring a Remote Router to Import DHCP Server Options from a Central DHCP Server, page 35
- Configuring DHCP Address Allocation Using Option 82, page 38
- Configuring a Static Route with the Next Hop Dynamically Obtained Through DHCP, page 43
- Clearing DHCP Server Variables, page 44

Configuring a DHCP Database Agent or Disabling Conflict Logging

Perform this task to configure a DHCP database agent.

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.

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.

Note We strongly recommend using database agents. However, the Cisco IOS 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	Do one of the following:
	• **ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*]
	• or
	• **no ip dhcp conflict logging**
	Example:
	`Router(config)# ip dhcp database ftp://user:password@172.16.1.1/`
	`router-dhcp timeout 80`
	Example:
	Example:
	`Router(config)# no ip dhcp conflict logging`
		Configures a DHCP server to save automatic bindings on a remote host called a database agent.
		or
		Disables DHCP address conflict logging.

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 nonoverlapping set of addresses in the shared subnet. See the "Configuring Manual Bindings Example" section 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp excluded-address** *low-address* [*high-address*] **Example:** `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.

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 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 the "Configuring Manual Bindings" task.

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 nonzero), 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 pools that contain the subnets 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 DHCP server software supports advanced capabilities for IP address allocation. See the "Configuring DHCP Address Allocation Using Option" section for more information.

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
    - DNS servers
    - NetBIOS name server
    - Primary subnet
    - Secondary subnets and subnet-specific default router lists (see "Configuring a DHCP Address Pool with Secondary Subnets" for information on secondary subnets).
- 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 "Configuring Manual Bindings".

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `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	**utilization mark high** *percentage-number* [**log**] **Example:** `Router(dhcp-config)# utilization mark high 80 log`	(Optional) Configures the high utilization mark of the current address pool size. • The **log** keyword enables the logging of a system message. A system message will be generated for a DHCP pool when the pool utilization exceeds the conigured high utilization threshold.
Step 5	**utilization mark low** *percentage-number* [**log**] **Example:** `Router(dhcp-config)# utilization mark low 70 log`	(Optional) Configures the low utilization mark of the current address pool size. • The **log** keyword enables the logging of a system message. A system message will be generated for a DHCP pool when the pool utilization falls below the configured low utilization threshold.
Step 6	**network** *network-number* [{*mask* | */prefix-length*} [**secondary**]] **Example:** `Router(dhcp-config)# network 172.16.0.0 /16`	Specifies the subnet network number and mask of the DHCP address pool.
Step 7	**domain-name** *domain* **Example:** `Router(dhcp-config)# domain-name cisco.com`	Specifies the domain name for the client.
Step 8	**dns-server** *address* [*address2 ... address8]* **Example:** `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. • One IP address is required; however, you can specify up to eight IP addresses in one command line. • Servers should be listed in order of preference.
Step 9	**bootfile** *filename* **Example:** `Router(dhcp-config)# bootfile xllboot`	(Optional) Specifies the name of the default boot image for a DHCP client. • 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.

	Command or Action	Purpose
Step 10	**next-server** *address* [*address2 ... address8]* **Example:** `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. • 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. • If this command is not configured, DHCP uses the server specified by the **ip helper address** command as the boot server.
Step 11	**netbios-name-server** *address* [*address2 ... address8]* **Example:** `Router(dhcp-config)# netbios-name-server 172.16.1.103 172.16.2.103`	(Optional) Specifies the NetBIOS WINS server that is available to a Microsoft DHCP client. • One address is required; however, you can specify up to eight addresses in one command line. • Servers should be listed in order of preference.
Step 12	**netbios-node-type** *type* **Example:** `Router(dhcp-config)# netbios-node-type h-node`	(Optional) Specifies the NetBIOS node type for a Microsoft DHCP client.
Step 13	**default-router** *address* [*address2 ... address8]* **Example:** `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. • The IP address should be on the same subnet as the client. • One IP address is required; however, you can specify 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. • 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 14	**option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*}
	Example:
	`Router(dhcp-config)# option 19 hex 01`
		(Optional) Configures DHCP server options.

	Command or Action	Purpose

Step 15	**lease** {*days* [*hours* [*minutes*]] | **infinite**}
	Example:
	`Router(dhcp-config)# lease 30`
		(Optional) Specifies the duration of the lease.
		• The default is a one-day lease.
		• The **infinite** keyword specifies that the duration of the lease is unlimited.

Step 16	**end**
	Example:
	`Router(dhcp-config)# end`
		Returns to global configuration mode.

Configuring a DHCP Address Pool with Secondary Subnets

Perform this task to configure a DHCP address pool with secondary subnets.

For any DHCP pool, you can configure a primary subnet and any number of secondary subnets. Each subnet is a range of IP addresses that the router uses to allocate an IP address to a DHCP client. The DHCP server multiple subnet functionality enables a Cisco IOS DHCP server address pool to manage additional IP addresses by adding the addresses to a secondary subnet of an existing DHCP address pool (instead of using a separate address pool).

Configuring a secondary DHCP subnetwork places the router in DHCP pool secondary subnet configuration mode--identified by the (config-dhcp-subnet-secondary)# prompt--from which you can configure a default address list that is specific to the secondary subnet. You can also specify the utilization rate of the secondary subnet, which allows pools of IP addresses to dynamically increase or reduce in size depending on the address utilization level. This setting overrides the global utilization rate.

If the DHCP server selects an address pool that contains multiple subnets, the DHCP server allocates an IP address from the subnets as follows:

- When the DHCP server receives an address assignment request, it looks for a free address in the primary subnet.
- When the primary subnet is exhausted, the DHCP server automatically looks for a free address in any secondary subnets maintained by the DHCP server (even though the giaddr does not necessarily match the secondary subnet). The server inspects the subnets for address availability in the order in which the subnets were added to the pool.
- If the giaddr matches a secondary subnet in the pool, the DHCP server allocates an IP address from that secondary subnet (even if IP addresses are available in the primary subnet and irrespective of the order in which secondary subnets where added).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **utilization mark high** *percentage-number* [**log**]
5. **utilization mark low** *percentage-number* [**log**]
6. **network** *network-number* [*mask* | / *prefix-length*]
7. **domain-name** *domain*
8. **dns-server** *address* [*address2 ... address8]*
9. **bootfile** *filename*
10. **next-server** *address* [*address2 ... address8]*
11. **netbios-name-server** *address* [*address2 ... address8]*
12. **netbios-node-type** *type*
13. **default-router** *address* [*address2 ... address8]*
14. **option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*}
15. **lease** *{days* [*hours*] [*minutes*]| **infinite**}
16. **network** *network-number* [{*mask* | / *preix-length*} [**secondary**]]
17. **override default-router** *address* [*address2 ... address8*]
18. **override utilization high** *percentage-numer*
19. **override utilization low** *percentage-number*
20. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `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	**utilization mark high** *percentage-number* [**log**] **Example:** `Router(dhcp-config)# utilization mark high 80 log`	(Optional) Configures the high utilization mark of the current address pool size. • The **log** keyword enables the logging of a system message. A system message will be generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold.
Step 5	**utilization mark low** *percentage-number* [**log**] **Example:** `Router(dhcp-config)# utilization mark low 70 log`	(Optional) Configures the low utilization mark of the current address pool size. • The **log** keyword enables the logging of a system message. A system message will be generated for a DHCP pool when the pool utilization falls below the configured low utilization threshold.
Step 6	**network** *network-number* [*mask* | / *prefix-length*] **Example:** `Router(dhcp-config)# network 172.16.0.0 /16`	Specifies the subnet network number and mask of the DHCP address pool.
Step 7	**domain-name** *domain* **Example:** `Router(dhcp-config)# domain-name cisco.com`	Specifies the domain name for the client.
Step 8	**dns-server** *address* [*address2 ... address8]* **Example:** `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. • One IP address is required; however, you can specify up to eight IP addresses in one command line. • Servers should be listed in order of preference.
Step 9	**bootfile** *filename* **Example:** `Router(dhcp-config)# bootfile xllboot`	(Optional) Specifies the name of the default boot image for a DHCP client. • 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.

	Command or Action	Purpose
Step 10	**next-server** *address* [*address2 ... address8]* **Example:** `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. • 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. • If this command is not configured, DHCP uses the server specified by the **ip helper address** command as the boot server.
Step 11	**netbios-name-server** *address* [*address2 ... address8]* **Example:** `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. • One address is required; however, you can specify up to eight addresses in one command line. • Servers should be listed in order of preference.
Step 12	**netbios-node-type** *type* **Example:** `Router(dhcp-config)# netbios-node-type h-node`	(Optional) Specifies the NetBIOS node type for a Microsoft DHCP client.
Step 13	**default-router** *address* [*address2 ... address8]* **Example:** `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. • The IP address should be on the same subnet as the client. • 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. • 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 14	**option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*}
	Example:
	`Router(dhcp-config)# option 19 hex 01`
		(Optional) Configures DHCP server options.

	Command or Action	Purpose

Step 15	**lease** *{days* [*hours*] [*minutes*]| **infinite**}
	Example:
	`Router(dhcp-config)# lease 30`
		(Optional) Specifies the duration of the lease.
		• The default is a one-day lease.
		• The **infinite** keyword specifies that the duration of the lease is unlimited.

Step 16	**network** *network-number* [{*mask* | / *preix-length*} [**secondary**]] **Example:** `Router(dhcp-config)# network 10.10.0.0 255.255.0.0 secondary`	(Optional) Specifies the network number and mask of a secondary DHCP server address pool. • Any number of secondary subnets can be added to the DHCP server address pool. • During execution of this command, the configuration mode changes to DHCP pool secondary subnet configuration mode, which is identified by the (config-dhcp-subnet-secondary)# prompt. In this mode, the administrator can configure a default router list that is specific to the subnet. • See "Troubleshooting Tips" if you are using secondary IP addresses under a loopback interface with DHCP secondary subnets.
Step 17	**override default-router** *address* [*address2 ... address8*] **Example:** `Router(config-dhcp-subnet-secondary)# override default-router 10.10.0.100 10.10.0.101`	(Optional) Specifies the default router list that is used when an IP address is assigned to a DHCP client from this secondary subnet. • If this subnet-specific override value is configured, it is used when assigning an IP address from the subnet; the network-wide default router list is used only to set the gateway router for the primary subnet. • If this subnet-specific override value is not configured, the network-wide default router list is used when assigning an IP address from the subnet. • See "Configuring a DHCP Address Pool with Multiple Disjoint Subnets Example" for an example configuration.
Step 18	**override utilization high** *percentage-numer* **Example:** `Router(config-dhcp-subnet-secondary)# override utilization high 60`	(Optional) Sets the high utilization mark of the subnet size. • This command overrides the global default setting specified by the **utilization mark high** global configuration command.
Step 19	**override utilization low** *percentage-number* **Example:** `Router(config-dhcp-subnet-secondary)# override utilization low 40`	(Optional) Sets the low utilization mark of the subnet size. • This command overrides the global default setting specified by the **utilization mark low** global configuration command.

	Command or Action	Purpose

Step 20	**end**
	Example:
	`Router(config-dhcp-subnet-secondary)# end`
		Returns to privileged EXEC mode.

Troubleshooting Tips

If you are using secondary IP addresses under a single loopback interface and using secondary subnets under a DHCP pool, use one DHCP pool to configure networks for all the secondary subnets instead of one pool per secondary subnet. The **network** *network-number* [{*mask* | /*prefix-length*} [**secondary**]] command must be configured under a single DHCP address pool rather than multiple DHCP address pools.

The following is the correct configuration:

```
!
ip dhcp pool dhcp_1
 network 172.16.1.0 255.255.255.0
 network 172.16.2.0 255.255.255.0 secondary
 network 172.16.3.0 255.255.255.0 secondary
 network 172.16.4.0 255.255.255.0 secondary
!
interface Loopback111
 ip address 172.16.1.1 255.255.255.255 secondary
 ip address 172.16.2.1 255.255.255.255 secondary
 ip address 172.16.3.1 255.255.255.255 secondary
 ip address 172.16.4.1 255.255.255.255 secondary
```

The following is the incorrect configuration:

```
!
ip dhcp pool dhcp_1
 network 172.16.1.0 255.255.255.0
 lease 1 20 30
 accounting default
!
ip dhcp pool dhcp_2
 network 172.16.2.0 255.255.255.0
 lease 1 20 30
 accounting default
!
ip dhcp pool dhcp_3
 network 172.16.3.0 255.255.255.0
 lease 1 20 30
 accounting default
!
ip dhcp pool dhcp_4
 network 172.16.4.0 255.255.255.0
 lease 1 20 30
 accounting default
!
interface Loopback111
 ip address 172.16.1.1 255.255.255.255 secondary
 ip address 172.16.2.1 255.255.255.255 secondary
 ip address 172.16.3.1 255.255.255.255 secondary
 ip address 172.16.4.1 255.255.255.255 secondary
```

Verifying the DHCP Address Pool Configuration

Perform this task to verify the DHCP address pool configuration. These show commands need not be entered in any specific order.

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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip dhcp pool** [*name*] **Example:** `Router# show ip dhcp pool`	(Optional) Displays information about DHCP address pools.
Step 3	**show ip dhcp binding** [*address*] **Example:** `Router# show ip dhcp binding`	(Optional) Displays a list of all bindings created on a specific DHCP server. • 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. • 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*] **Example:** `Router# show ip dhcp conflict`	(Optional) Displays a list of all address conflicts.
Step 5	**show ip dhcp database** [*url*] **Example:** `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*] **Example:** `Router# show ip dhcp server statistics`	(Optional) Displays count information about server statistics and messages sent and received.

Configuring Manual 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 configure only 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, store a copy of the automatic binding information 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 DHCP server can function without database agents.

Some DHCP clients send a client identifier (DHCP option 61) in the DHCP packet. To configure manual bindings for such clients, you must enter the **client-identifier** DHCP pool configuration command with the appropriate hexadecimal values identifying the DHCP client. To configure manual bindings for clients who do not send a client identifier option, you must enter the **hardware-address** DHCP pool configuration command with the appropriate hexadecimal hardware address of the client.

In Cisco IOS Release 12.4(22)T and later releases the DHCP server sends infinite lease time to the clients for which manual bindings are configured.

In Cisco IOS Release 15.1(1)S1 and later releases, the DHCP server sends lease time configured using the **lease** command to the clients for which manual bindings are configured.

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* [*protocol-type* | *hardware-number*]
7. **client-name** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool pool1`	Creates a name for the DHCP server address pool and places you in DHCP pool configuration mode.
Step 4	**host** *address* [*mask*| / *prefix-length*] **Example:** `Router(dhcp-config)# host 172.16.0.1`	Specifies the IP address and subnet mask of the client. • There is no limit on the number of manual bindings but you can configure only one manual binding per host pool.

	Command or Action	Purpose
Step 5	**client-identifier** *unique-identifier* **Example:** `Router(dhcp-config)# client-identifier 01b7.0813.8811.66`	Specifies the unique identifier for DHCP clients. • This command is used for DHCP requests. • 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. • See the "Troubleshooting Tips" section for information on how to determine the client identifier of the DHCP client. **Note** The identifier specified here is considered for the DHCP clients who send a client identifier in the packet.
Step 6	**hardware-address** *hardware-address* [*protocol-type* | *hardware-number*] **Example:** `Router(dhcp-config)# hardware-address b708.1388.f166 ethernet`	Specifies a hardware address for the client. • This command is used for BOOTP requests. **Note** The hardware address specified here is considered for the DHCP clients who do not send a client identifier in the packet.
Step 7	**client-name** *name* **Example:** `Router(dhcp-config)# client-name client1`	(Optional) Specifies the name of the client using any standard ASCII character. • The client name should not include the domain name. For example, the name client1 should not be specified as client1.cisco.com.

- Troubleshooting Tips, page 29

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.
.
.
.
```

Configuring DHCP Static Mapping

The DHCP--Static Mapping feature enables assignment of static IP addresses without creating numerous host pools with manual bindings by using a customer-created text file that the DHCP server reads. The benefit of this feature is that it eliminates the need for a long configuration file and reduces the space required in NVRAM to maintain address pools.

This section contains the following task:

A DHCP database contains the mappings between a client IP address and hardware address, referred to as a binding. There are two types of bindings: manual bindings that map a single hardware address to a single IP address, and automatic bindings that dynamically map a hardware address to an IP address from a pool of IP addresses. Manual (also known as static) bindings can be configured individually directly on the router or, by using the DHCP--Static Mapping feature, these static bindings can be read from a separate static mapping text file. The static mapping text files are read when a router reloads or the DHCP service restarts. These files are read-only.

The read static bindings are treated just like the manual bindings, in that they are:

- Retained across DHCPRELEASEs from the clients.
- Not timed out.
- Deleted only upon deletion of the pool.
- Provided appropriate exclusions for the contained addresses, which are created at the time of the read.

Just like automatic bindings and manual bindings, the static bindings from the static mapping text file are also displayed by using the **show ip dhcp binding** command.

Perform this task to create the static mapping text file. You will input your addresses in the text file, which is stored in the DHCP database for the DHCP server to read. There is no limit on the number of addresses in the file. The file format has the following elements:

- Time the file was created
- Database version number
- IP address
- Hardware type
- Hardware address
- Lease expiration
- End-of-file designator

See the table below for more details about the format of the text file.

The following is a sample static mapping text file:

```
*time* Jan 21 2005 03:52 PM
*version* 2
!IP address    Type    Hardware address     Lease expiration
10.0.0.4 /24   1       0090.bff6.081e       Infinite
10.0.0.5 /28   id      00b7.0813.88f1.66    Infinite
10.0.0.2 /21   1       0090.bff6.081d       Infinite
*end*
```

Table 3 Static Mapping Text File Field Descriptions

Field	Description
time	Specifies the time the file was created. This field allows DHCP to differentiate between newer and older database versions when multiple agents are configured. The valid format of the time is Mm dd yyyy hh:mm AM/PM.
version 2	Database version number.
IP address	Static IP address. If the subnet mask is not specified, a natural mask is assumed depending on the IP address. There must be a space between the IP address and mask.

Field	Description
Type	Specifies the hardware type. For example, type "1" indicates Ethernet. The type "id" indicates that the field is a DHCP client identifier. Legal values can be found online at http://www.iana.org/assignments/arp-parameters in the "Number Hardware Type" list.
Hardware address	Specifies the hardware address. When the type is numeric, it refers to the hardware media. Legal values can be found online at http://www.iana.org/assignments/arp-parameters in the "Number Hardware Type" list. When the type is "id," this means that we are matching on the client identifier. For more information about the client identifier, please see RFC 2132, *DHCP Options and BOOTP Vendor Extensions* , section 9.14, located at http://www.ietf.org/rfc/rfc2132.txt , or the **client-identifier** command reference page. . If you are unsure what client identifier to match on, use the **debug dhcp detail** command to display the client identifier being sent to the DHCP server from the client.
Lease expiration	Specifies the expiration of the lease. "Infinite" specifies that the duration of the lease is unlimited.
end	End of file. DHCP uses the *end* designator to detect file truncation.

- Configuring the DHCP Server to Read a Static Mapping Text File, page 31

Configuring the DHCP Server to Read a Static Mapping Text File

Perform this task to configure the DHCP server to read the static mapping text file.

The administrator should create the static mapping text file in the correct format and configure the address pools before performing this task.

Before editing the file, you must disable the DHCP server using the **no service dhcp** command.

Note The static bindings must not be deleted when a DHCPRELEASE is received or must not be timed out by the DHCP timer. The static bindings should be treated just like manual bindings created by using the **ip dhcp pool** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **origin file** *url*
5. **end**
6. **show ip dhcp binding** [*address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool pool1`	Assigns a name to a DHCP pool and enters DHCP configuration mode. **Note** If you have already configured the IP DHCP pool name using the **ip dhcp pool** command and the static file URL using the **origin file** command, you must perform a fresh read using the **no service dhcp**command and **service dhcp** command.

Step 4	**origin file** *url*
	Example:
	`Router(dhcp-config)# origin file tftp://`
	`10.1.0.1/static-bindings`
		Specifies the URL from which the DHCP server can locate the text file.

Step 5	**end**
	Example:
	`Router(dhcp-config)# end`
		Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show ip dhcp binding** [*address*] **Example:** `Router# show ip dhcp binding`	(Optional) Displays a list of all bindings created on a specific DHCP server.

Examples

The following example shows the address bindings that have been configured:

```
Router# show ip dhcp binding
00:05:14:%SYS-5-CONFIG_I: Configured from console by console
Bindings from all pools not associated with VRF:
IP address  Client-ID/            Ls expir   Type    Hw address           User name
10.9.9.4/8  0063.7363.2d30.3036.  Infinite   Static  302e.3762.2e39.3634. 632d.4574.8892.
10.9.9.1/24 0063.6973.636f.2d30.  Infinite   Static  3036.302e.3437.3165. 2e64.6462.342d.
```

The following sample shows each entry in the static mapping text file:

```
*time* Jan 21 2005 22:52 PM
!IP address     Type        Hardware address                              Lease expiration
10.19.9.1 /24    id          0063.6973.636f.2d30.3036.302e.3437
10.9.9.4         id          0063.7363.2d30.3036.302e.3762.2e39.3634.632d  Infinite
*end*
```

The following sample debug output shows the reading of the static mapping text file from the TFTP server:

```
Router# debug ip dhcp server
Loading abc/static_pool from 10.19.192.33 (via Ethernet0):
[OK - 333 bytes]
*May 26 23:14:21.259: DHCPD: contacting agent tftp://10.19.192.33/abc/static_pool
(attempt 0)
*May 26 23:14:21.467: DHCPD: agent tftp://10.19.192.33/abc/static_pool is responding.
*May 26 23:14:21.467: DHCPD: IFS is ready.
*May 26 23:14:21.467: DHCPD: reading bindings from                              tftp://
10.19.192.33/abc/static_pool.
*May 26 23:14:21.707: DHCPD: read 333 / 1024 bytes.
*May 26 23:14:21.707: DHCPD: parsing text line
*time* Apr 22 2002 11:31 AM
*May 26 23:14:21.707: DHCPD: parsing text line ““
*May 26 23:14:21.707: DHCPD: parsing text line
!IP address Type Hardware address Lease expiration
*May 26 23:14:21.707: DHCPD: parsing text line
“10.9.9.1 /24 id 0063.6973.636f.2d30.3036.302e.3437”
*May 26 23:14:21.707: DHCPD: creating binding for 10.9.9.1
*May 26 23:14:21.707: DHCPD: Adding binding to radix tree (10.9.9.1)
*May 26 23:14:21.707: DHCPD: Adding binding to hash tree
*May 26 23:14:21.707: DHCPD: parsing text line
“10.9.9.4 id 0063.7363.2d30.3036.302e.3762.2e39.3634.632d”
*May 26 23:14:21.711: DHCPD: creating binding for 10.9.9.4
*May 26 23:14:21.711: DHCPD: Adding binding to radix tree (10.9.9.4)
*May 26 23:14:21.711: DHCPD: Adding binding to hash tree
*May 26 23:14:21.711: DHCPD: parsing text line “Infinite”
*May 26 23:14:21.711: DHCPD: parsing text line “”
*May 26 23:14:21.711: DHCPD: parsing text line
!IP address Interface-index Lease expiration VRF
*May 26 23:14:21.711: DHCPD: parsing text line “*end*”
*May 26 23:14:21.711: DHCPD: read static bindings from tftp://10.19.192.33/abcemp/
static_pool.
```

Customizing DHCP Server Operation

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.

You can configure the DHCP server to ignore and not reply to received Bootstrap Protocol (BOOTP) requests. This functionality is beneficial when there is a mix of BOOTP and DHCP clients in a network segment and there is a BOOTP server and a Cisco IOS DHCP server servicing the network segment. The BOOTP server is configured with static bindings for the BOOTP clients and the BOOTP clients are intended to obtain their addresses from the BOOTP server. However, because a DHCP server can also respond to a BOOTP request, an address offer may be made by the DHCP server causing the BOOTP clients to boot with the address from the DHCP server, instead of the address from the BOOTP server. Configuring the DHCP server to ignore BOOTP requests means that the BOOTP clients will receive address information from the BOOTP server and will not inadvertently accept an address from a DHCP server.

The Cisco IOS software can forward these ignored BOOTP request packets to another DHCP server if the **ip helper-address** interface configuration command is configured on the incoming interface.

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip dhcp ping packets** *number* **Example:** `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. • 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* **Example:** `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.
Step 5	**ip dhcp bootp ignore** **Example:** `Router(config)# ip dhcp bootp ignore`	(Optional) Allows the DHCP server to selectively ignore and not reply to received BOOTP requests. • The **ip dhcp bootp ignore** command applies to all DHCP pools configured on the router. BOOTP requests cannot be selectively ignored on a per-DHCP pool basis.

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 35
- Configuring the Remote Router to Import DHCP Options, page 36

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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `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*] **Example:** `Router(dhcp-config)# network 172.16.0.0 /16`	Specifies the subnet network number and mask of the DHCP address pool.
Step 5	**dns-server** *address* [*address2* ... *address8*] **Example:** `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. • One IP address is required; however, you can specify up to eight IP addresses in one command line. • 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool pool1`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 4	**network** *network-number* [*mask*	/ *prefix-length*] **Example:** `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**
	Example:
	`Router(dhcp-config)# import all`
		Imports DHCP option parameters into the DHCP server database.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(dhcp-config)# exit`	Exits DHCP pool configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/0`	Configures an interface and enters interface configuration mode.
Step 8	**ip address dhcp** **Example:** `Router(config-if)# ip address dhcp`	Specifies that the interface acquires an IP address through DHCP.

Step 9	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Step 10	**show ip dhcp import** **Example:** `Router# show ip dhcp import`	Displays the options that have been imported from the central DHCP server.

Configuring DHCP Address Allocation Using Option 82

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 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.

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.

The Cisco IOS 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 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.

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 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp use class** **Example:** `Router(config)# ip dhcp use class`	Controls whether DHCP classes are used for address allocation. • This functionality is enabled by default. • 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** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp class** *class-name* **Example:** `Router(config)# ip dhcp class CLASS1`	Defines a DHCP class and enters DHCP class configuration mode.
Step 4	**relay agent information** **Example:** `Router(dhcp-class)# relay agent information`	Enters relay agent information option configuration mode. - 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*] **Example:** `Router(dhcp-class-relayinfo)# relay-information hex 01030a0b0c02050000000123`	(Optional) Specifies a hexadecimal value for the full relay information option. - The *pattern* argument creates a pattern that is used to match to the DHCP class. - 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. - 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

Use 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Router# ip dhcp pool ABC`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode. • 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*] **Example:** `Router(dhcp-config)# network 10.0.20.0`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

Step 5	**class** *class-name*
	Example:
	`Router(dhcp-config)# class CLASS1`
		Associates a class with a pool and enters DHCP pool class configuration mode.
		• 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* **Example:** `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. • 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 nonphysical 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 of the DHCP packet.

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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} **dhcp** [*distance*] **Example:** `Router(config)# ip route 209.165.200.225 255.255.255.255 dhcp`	Assigns a static route for the default next-hop router when the DHCP server is accessed for an IP address. • 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**
	Example:
	`Router(config)# end`
		Returns to privileged Exec mode.

Step 5	**show ip route** **Example:** `Router# show ip route`	(Optional) Displays the current state of the routing table. • 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** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip dhcp binding** {*address* | *****} **Example:** `Router# clear ip dhcp binding *`	Deletes an automatic address binding from the DHCP database. • 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* | *****} **Example:** `Router# clear ip dhcp conflict 172.16.1.103`	Clears an address conflict from the DHCP database. • 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** **Example:** `Router# clear ip dhcp server statistics`	Resets all DHCP server counters to 0.

Configuration Examples for the Cisco IOS 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 4 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	172.16.1.100 172.16.1.101	Default routers	172.16.2.100 172.16.2.101
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 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 a DHCP Address Pool with Multiple Disjoint Subnets Example

Multiple disjoint subnets in a DHCP pool can be used in any of the following network topologies:

- IP address pooling--The DHCP client and server reside on the same subnet.
- DHCP relay--The DHCP client and DHCP server communicate through a DHCP relay agent where the relay interface is configured with secondary IP addresses.
- Hierarchical DHCP--The DHCP server is configured as the DHCP subnet allocation server, and the DHCP client and DHCP subnet allocation server communicate through an on-demand address pool (ODAP) router.

In the following example, one DHCP address pool named pool3 is created; the primary subnet is 172.16.0.0/16, one secondary subnet is 172.16.1.0/24, and another secondary subnet is 172.16.2.0/24.

- When the IP addresses in the primary subnet are exhausted, the DHCP server inspects the secondary subnets in the order in which the subnets were added to the pool.
- When the DHCP server allocates an IP address from the secondary subnet 172.16.1.0/24, the server uses the subnet-specific default router list that consists of IP addresses 172.16.1.100 and 172.16.1.101. When the DHCP server allocates an IP address from the subnet 172.16.2.0/24, however, the server uses the pool-wide list that consists of the four IP addresses from 172.16.0.100 to 172.16.0.103.
- Other attributes from the primary subnet 172.16.0.0/16--such as the domain name, DNS server, NetBIOS name server, and NetBIOS node type--are inherited in both of the secondary subnets.
- DHCP clients are granted 30-day leases on IP addresses in the pool. All addresses in each subnet, 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 the DHCP address pool that consists of three disjoint subnets.

Table 5 DHCP Address Pool Configuration with Multiple Disjoint Subnets Example

Primary Subnet (172.16.0.0/16)	**First Secondary Subnet (172.16.1.0/24)**	**Second Secondary Subnet (172.16.2.0/24)**			
Device	IP Address	Device	IP Address	Device	IP Address
Default routers	172.16.0.100	Default routers	172.16.1.100	Default routers	172.16.0.100
	172.16.0.101		172.16.1.101		172.16.0.101
	172.16.0.102				172.16.0.102
	172.16.0.103				172.16.0.103

Primary Subnet (172.16.0.0/16)	First Secondary Subnet (172.16.1.0/24)	Second Secondary Subnet (172.16.2.0/24)			
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 database ftp://user:password@172.16.4.253/router-dhcp write-delay 120
ip dhcp excluded-address 172.16.0.100 172.16.1.103
ip dhcp excluded-address 172.16.1.100 172.16.1.101
!
ip dhcp pool pool3
 network 172.16.0.0 /16
 default-router 172.16.0.100 172.16.2.101 172.16.0.102 172.16.0.103
 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
 lease 30
!
 network 172.16.1.0 /24 secondary
  override default-router 172.16.1.100 172.16.1.101
  end
!
 network 172.16.2.0 /24 secondary
```

Configuring Manual Bindings Example

The following example shows how to create a manual binding for a client named example1.cisco.com that sends a client identifier in the DHCP packet. 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 pool1
 host 172.16.2.254
 client-identifier  01b7.0813.8811.66
 client-name example1
```

The following example shows how to create a manual binding for a client named example2.cisco.com that do not send a client identifier in the DHCP packet. The MAC address of the client is 02c7.f800.0422 and the IP address of the client is 172.16.2.253.

```
ip dhcp pool pool2
 host 172.16.2.253
 hardware-address 02c7.f800.0422 ethernet
 client-name example1
```

Because attributes are inherited, the two preceding configurations are equivalent to the following:

```
ip dhcp pool pool1
 host 172.16.2.254 255.255.255.0
 hardware-address 02c7.f800.0422 ieee802
 client-name client1
 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
```

Configuring Static Mapping Example

The following example shows how to restart the DHCP server, configure the pool, and specify the URL at which the static mapping text file is stored:

```
no service dhcp
service dhcp
ip dhcp pool abcpool
 origin file tftp://10.1.0.1/staticfilename
```

Note The static mapping text file can be copied to flash memory on the router and served by the TFTP process of the router. In this case, the IP address in the origin file line must be an address owned by the router and one additional line of configuration is required on the router:**tftp-server flash** *static-filename*

Configuring the Option to Ignore all BOOTP Requests Example

The following example shows two DHCP pools that are configured on the router and that the router’s DHCP server is configured to ignore all received BOOTP requests. If a BOOTP request is received from subnet 10.0.18.0/24, the request will be dropped by the router (because the **ip helper-address** command is not configured). If there is a BOOTP request from subnet 192.168.1.0/24, the request will be forwarded to 172.16.1.1 via the **ip helper-address** command.

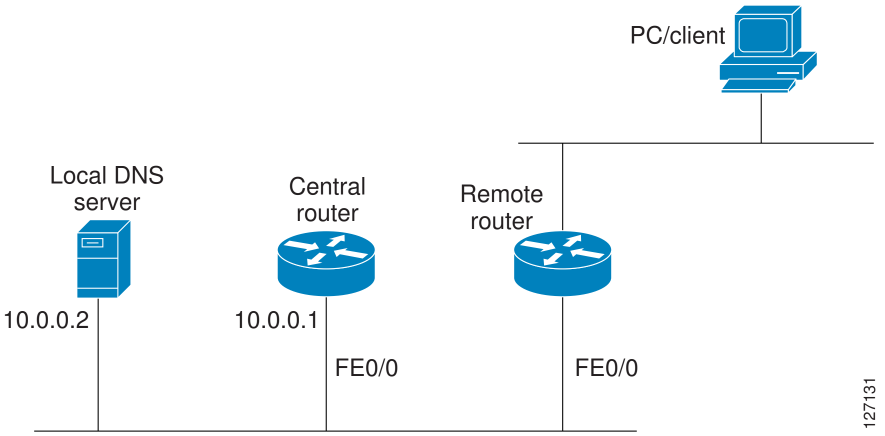
```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
ip subnet-zero
!
ip dhcp bootp ignore
!
ip dhcp pool ABC
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.3
   lease 2
!
ip dhcp pool DEF
   network 10.0.18.0 255.255.255.0
!
ip cef
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
 ip address 10.0.18.68 255.255.255.0
 duplex half
!
interface Ethernet1/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 172.16.1.1
 duplex half
!
interface Ethernet1/2
```

```
 shutdown
 duplex half
!
interface Ethernet1/3
 no ip address
 shutdown
 duplex half
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
!
ip route 172.16.1.1 255.255.255.255 e1/0
no ip http server
no ip pim bidir-enable
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

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 FastEthernet0/0
 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 172.16.2.254 255.255.255.0
!
interface FastEthernet0/0
 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 subnets. 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 be used only 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 172.64.2.2 255.255.255.0
 class CLASS1
  address range 172.64.2.3 172.64.2.10
 class CLASS2
```

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

The following example shows how to configure two Ethernet 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 ethernet 1 dhcp
```

Additional References

The following sections provide references related to configuring the Cisco IOS 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 DHCP Relay Agent” module
DHCP server on-demand address pools	“Configuring the DHCP Server On-Demand Address Pool Manager” module
DHCP client configuration	“Configuring the Cisco IOS DHCP Client” module
DHCP advanced features	“Configuring DHCP Services for Accounting and Security” module
DHCP enhancements for edge-session management	“Configuring DHCP Enhancements for Edge-Session Management” module
DHCP options	“DHCP Options” appendix in the *Network Registrar User’s Guide* , Release 6.1.1

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 releases, and feature sets, use Cisco MIB Locator found at the following URL: 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 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. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the Cisco IOS 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 6 Feature Information for the Cisco IOS DHCP Server

Feature Name	Releases	Feature Configuration Information
DHCP Address Allocation Using Option 82	12.3(4)T 12.2(28)SB 12.2(33)SRB	The Cisco IOS DHCP server can allocate dynamic IP addresses based on the relay information option (option 82) information sent by the relay agent. The following commands were introduced or modified: **address range**, **class**, **ip dhcp class**, **ip dhcp use class**, **relay agent information**, **relay-information hex**.
DHCP Server Import All Enhancement	12.2(15)T 12.2(33)SRC	The feature is an enhancement to the **import all** global configuration command. Before this feature was introduced, the options imported through the **import all** command were overwritten by those imported by another subsystem. Through this feature, options imported by multiple subsystems can coexist in the DHCP address pool. When the session is terminated or the lease is released, the imported options are cleared.
DHCP Server Multiple Subnet	12.4(15)T 12.2(33)SRB	This feature enables multiple subnets to be configured under the same DHCP address pool. The following commands were introduced or modified: **network**(DHCP), **override default-router**.

Feature Name	Releases	Feature Configuration Information
DHCP Server Option to Ignore all BOOTP Requests	12.2(8)T 12.2(28)SB	This feature allows the Cisco IOS DHCP server to selectively ignore and not reply to received Bootstrap Protocol (BOOTP) request packets. The following command was introduced or modified: **ip dhcp bootp ignore**.
DHCP Static Mapping	12.3(11)T 12.2(28)SB 12.2(33)SRC	Configuring static mapping pools enables the DHCP server to read the static bindings from a separate text file (similar in format to the DHCP database file) that is stored in these special pools. The following command was introduced or modified: **origin**.
DHCP Statically Configured Routes Using a DHCP Gateway	12.3(8)T 12.2(28)S 12.2(33)SRC	This feature enables the configuration of static routes that point to an assigned DHCP next-hop router. The following commands were introduced or modified: **ip route**, **show ip route**.

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 DHCP Relay Agent

All Cisco routers that run Cisco software include a DHCP server and the relay agent software. A DHCP relay agent is any host or IP router that forwards DHCP packets between clients and servers. This module describes the concepts and tasks needed to configure the Cisco IOS DHCP relay agent.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 Cisco IOS DHCP Relay Agent

- Before you configure the DHCP relay agent, you should understand the concepts documented in the "DHCP Overview" module.
- The Cisco IOS DHCP server and relay agent are enabled by default. You can verify whether 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 DHCP relay agent will be enabled on an interface only when the **ip helper-address** command 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 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. In contrast, when relay agents receive DHCP messages, the agents generate a new DHCP message to send out through another interface. The relay agent sets the gateway IP address (the giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (option 82) to the packet and forwards the packet to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

The Cisco IOS DHCP relay agent supports the use of unnumbered interfaces, including the use of smart relay agent forwarding. For DHCP clients that are connected though unnumbered interfaces, the DHCP relay agent automatically adds a static host route after 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.

How to Configure the DHCP Relay Agent

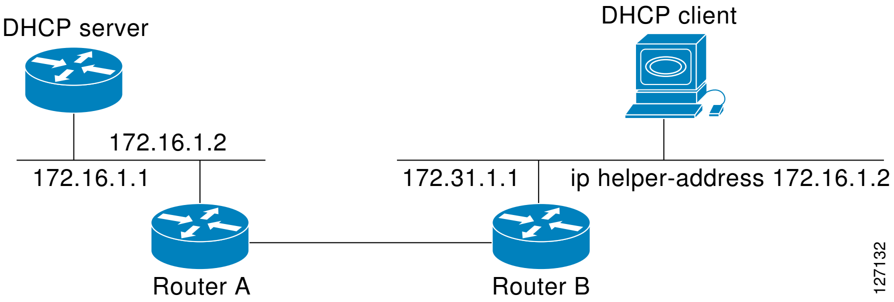
Specifying the Packet Forwarding Address

DHCP clients need to use UDP broadcasts to send their initial DHCPDISCOVER messages because the clients do not 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 are not usually forwarded because most routers are configured to not forward broadcast traffic. When the DHCP client broadcasts a DHCPDISCOVER message, the relay agent sends the broadcast message toward the server, which may create Address Resolution Protocol (ARP) entries due to unnecessary ARP checks performed by the client after receiving the ACK message. If there are two entries in the ARP table, one times out after the ARP timeout. 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 acts as a DHCP relay agent. The Cisco router implementation of the DHCP relay agent is provided through 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 packet. The DHCP relay agent sends the local broadcast, through IP unicast, to the DHCP server address 172.16.1.2 that is specified by the **ip helper-address** interface configuration command.

Figure 3 Forwarding UDP Broadcasts to a DHCP Server Using a Helper 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*
5. **exit**
6. **ip dhcp relay prefer known-good-server**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface FastEthernet0/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip helper-address** *address* **Example:** `Device(config-if)# ip helper-address 172.16.1.2`	Forwards UDP broadcasts, including BOOTP and DHCP. • 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. The network address enables other servers to respond to DHCP requests. • If you have multiple servers, you can configure one helper address for each server.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**ip dhcp relay prefer known-good-server** **Example:** `Device(config)# ip dhcp relay prefer known-good-server`	(Optional) Reduces the frequency with which the DHCP clients change their addresses and forwards client requests to the server that handled the previous request. • The DHCP relay agent deletes the ARP entries for addresses offered to the DHCP client on unnumbered interfaces.
Step 7	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring Support for the Relay Agent Information Option

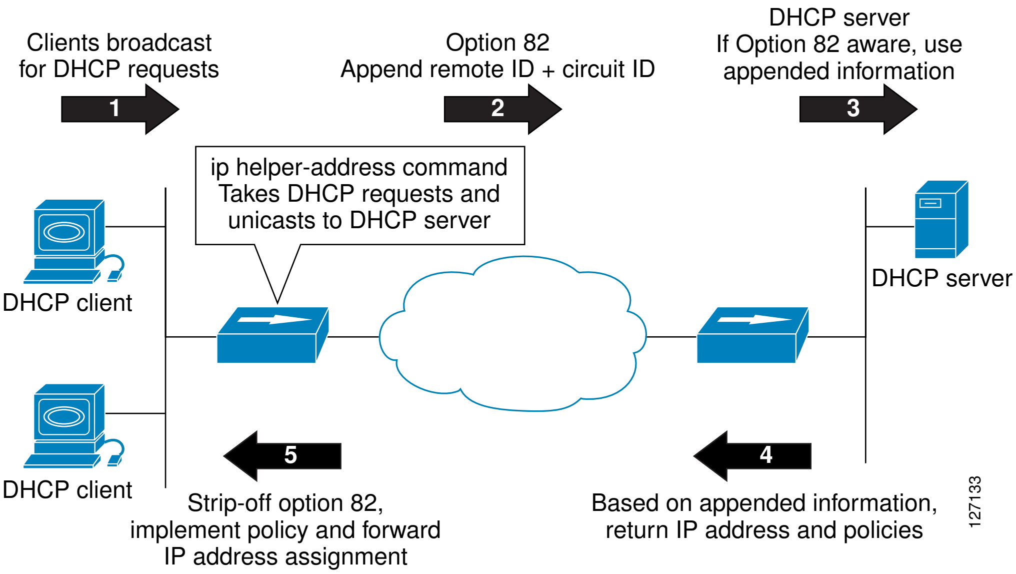
Automatic DHCP address allocation is typically based on an IP address, which may be either the gateway IP address (giaddr field of the DHCP packet) or the incoming interface IP address. In some networks, additional information may be required to further determine the IP addresses that need to be allocated. By using the relay agent information option (option 82), the Cisco IOS relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server. Cisco software 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) into the packet. The relay agent information option contains related suboptions.
3. The DHCP relay agent unicasts the DHCP packet to the DHCP server.
4. The DHCP server receives the packet, uses the suboptions to assign IP addresses and other configuration parameters to the packet, and forwards the packet back to the client.
5. The suboption fields are stripped off of the packet by the relay agent while forwarding the packet to the client.

Figure 4 Operation of the Relay Agent Information Option



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, disable the relay agent information check by using the **no ip dhcp relay information check** global configuration command.

It is important to understand how DHCP options work. See the "DHCP Overview" module for more information.

Note

- If the **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 the **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 the **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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip dhcp relay information option** **Example:** `Device(config)# ip dhcp relay information option`	Enables the system to insert the DHCP relay agent information option (option-82 field) in BOOTREQUEST messages forwarded to a DHCP server. • This function is disabled by default.
Step 4	**ip dhcp relay information check** **Example:** `Device(config)# ip dhcp relay information check`	(Optional) Configures DHCP to check whether the relay agent information option in forwarded BOOTREPLY messages is valid. • By default, DHCP verifies whether the option-82 field in DHCP reply packets that it receives from the DHCP server is valid. If an invalid message is received, the relay agent drops the packet. 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**} **Example:** `Device(config)# ip dhcp relay information policy replace`	(Optional) Configures the reforwarding policy (that specifies what a relay agent should do if a message already contains relay information) for a DHCP relay agent.
Step 6	**ip dhcp relay information trust-all** **Example:** `Device(config)# ip dhcp relay information trust-all`	(Optional) Configures all interfaces on a router as trusted sources of the DHCP relay information option. • 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. • This command is useful if there is a switch placed between the client and the relay agent that may insert option 82. Use this command to ensure that these packets do not get dropped. • 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**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

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

Configuring Per-Interface Support for the Relay Agent Information Option

The interface configuration allows a Cisco router to reach subscribers with different DHCP option 82 requirements on different interfaces.

It is important to understand how DHCP options work. See the "DHCP Overview" module for more information.

Note

- If the **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 the **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 the **ip dhcp relay information** command is not configured in global configuration mode but is configured in interface configuration mode, only the interface on which the configuration option is 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface FastEthernet0/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip dhcp relay information option-insert** [**none**] **Example:** `Device(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. • This function is disabled by default. However, if support for the relay agent information option is configured in global configuration mode, but not configured in interface configuration mode, the interface inherits the global configuration. • 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**] **Example:** `Device(config-if)# ip dhcp relay information check-reply`	Configures a DHCP server to validate the relay information option in forwarded BOOTREPLY messages. • By default, DHCP verifies whether the option-82 field in the DHCP reply packets that it receives from the DHCP server is valid. If an invalid message is received, the relay agent drops the packet. 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. • 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**} **Example:** `Device(config-if)# ip dhcp relay information policy-action replace`	Configures the information reforwarding policy (that specifies what a relay agent should do if a message already contains relay information) for a DHCP relay agent.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 8	Repeat Steps 3 through 7 to configure relay agent information settings on different interfaces.	—

Configuring the Subscriber Identifier Suboption of the Relay Agent Information Option

Perform this task to enable an 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, assign specific actions to that subscriber (for example, assignment of the host IP address, subnet mask, and domain name system [DNS]), and trigger accounting.

Before the introduction of the subscriber identifier suboption, if a subscriber moved from one Network Access Server to another, 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 the subscriber identifier suboption, if a subscriber moves from one Network Access Server to another, there is no need for a change in the configuration on the DHCP server or the ISPs.

You should configure a unique identifier for each subscriber.

The new configurable subscriber identifier suboption should be configured on the interface that is connected to the client. When a subscriber moves from one Network Access Server to another, 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*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp relay information option** **Example:** `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. • This function is disabled by default.
Step 4	**interface** *type number* **Example:** `Device(config)# interface atm4/0.1`	Configures an interface and enters interface configuration mode.
Step 5	**ip dhcp relay information option subscriber-id** *string* **Example:** `Device(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. **Note** The **ip dhcp relay information option subscriber-id** command is disabled by default to ensure backward capability.

Step 6	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

Configuring DHCP Relay Class Support for Client Identification

DHCP relay class support for client identification allows the Cisco relay agent to forward client-generated DHCP messages to different DHCP servers based on the content of the following four options:

- Option 60: vendor class identifier

- Option 77: user class
- Option 124: vendor-identifying vendor class
- Option 125: vendor-identifying vendor-specific information

Each option identifies the type of client that is sending the DHCP message.

Relay pools provide a method to define DHCP pools that are not used for address allocation. These relay pools can specify that DHCP messages from clients on a specific subnet should be forwarded to a specific DHCP server. These relay pools can be configured with relay classes inside the pool that help determine the forwarding behavior.

For example, after receiving the option in a DHCP DISCOVER message, the relay agent will match and identify the relay class from the relay pool and then direct the DHCP DISCOVER message to the DHCP server associated with that identified relay class.

In an example application, a Cisco router acting as a DHCP relay agent receives DHCP requests from two VoIP services (H.323 and the Session Initiation Protocol [SIP]). The requesting devices are identified by option 60.

Both VoIP services have a different back-office infrastructure, so they cannot be serviced by the same DHCP server. Requests for H.323 devices must be forwarded to the H.323 server, and requests from SIP devices must be forwarded to the SIP server. The solution is to configure the relay agent with relay classes that are configured to match option 60 values sent by the client devices. Based on the option value, the relay agent will match and identify the relay class, and forward the DHCP DISCOVER message to the DHCP server associated with the identified relay class.

The Cisco IOS DHCP server examines the relay classes that are applicable to a pool and then uses the exact match class regardless of the configuration order. If the exact match is not found, the DHCP server uses the first default match found.

It is important to understand how DHCP options work. See the “DHCP Overview” module for more information.

You must know the hexadecimal value of each byte location in the options to be able to configure the **option hex** command. The 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. **option** *code* **hex** *hex-pattern* [*****][**mask** *bit-mask-pattern*]
5. **exit**
6. Repeat Steps 3 through 5 for each DHCP class that you need to configure.
7. **ip dhcp pool** *name*
8. **relay source** *ip-address subnet-mask*
9. **class** *class-name*
10. **relay target** [**vrf** *vrf-name* | **global**] *ip-address*
11. **exit**
12. Repeat Steps 9 through 11 for each DHCP class that you need to configure.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp class** *class-name* **Example:** `Device(config)# ip dhcp class SIP`	Defines a DHCP class and enters DHCP class configuration mode.
Step 4	**option** *code* **hex** *hex-pattern* [*****][**mask** *bit-mask-pattern*] **Example:** `Device(dhcp-class)# option 60 hex 010203`	Enables the relay agent to make forwarding decisions based on DHCP options inserted in the DHCP message.
Step 5	**exit** **Example:** `Device(dhcp-class)# exit`	Exits DHCP class configuration mode.
Step 6	Repeat Steps 3 through 5 for each DHCP class that you need to configure.	—
Step 7	**ip dhcp pool** *name* **Example:** `Device(config)# ip dhcp pool ABC`	Configures a DHCP pool on a DHCP server and enters DHCP pool configuration mode.

	Command or Action	Purpose
Step 8	**relay source** *ip-address subnet-mask* **Example:** `Device(dhcp-config)# relay source 10.2.0.0 255.0.0.0`	Configures the relay source. • This command is similar to the **network** command in a normal DHCP network pool, because it restricts the use of the address pool to packets arriving on the interface whose configured IP address and mask match the relay source configuration.

Step 9	**class** *class-name*
	Example:
	`Device(dhcp-config)# class SIP`
		Associates a class with a DHCP pool and enters DHCP pool class configuration mode.

Step 10	**relay target** [**vrf** *vrf-name* | **global**] *ip-address* **Example:** `Device(config-dhcp-pool-class)# relay target 10.21.3.1`	Configures an IP address for a DHCP server to which packets are forwarded.
Step 11	**exit** **Example:** `Device(config-dhcp-pool-class)# exit`	Exits DHCP pool class configuration mode.
Step 12	Repeat Steps 9 through 11 for each DHCP class that you need to configure.	—

Configuring DHCP Relay Agent Support for MPLS VPNs

DHCP relay support for Multiprotocol Label Switching (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.

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 inform the DHCP server about the VPN for every DHCP request that the relay agent passes on to the DHCP server; the VPN identifier suboption 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 VPN routing and forwarding (VRF) name but not the VPN ID, the VRF name is used as the VPN identifier suboption. If the interface is in the global routing space, VPN suboptions are not added.

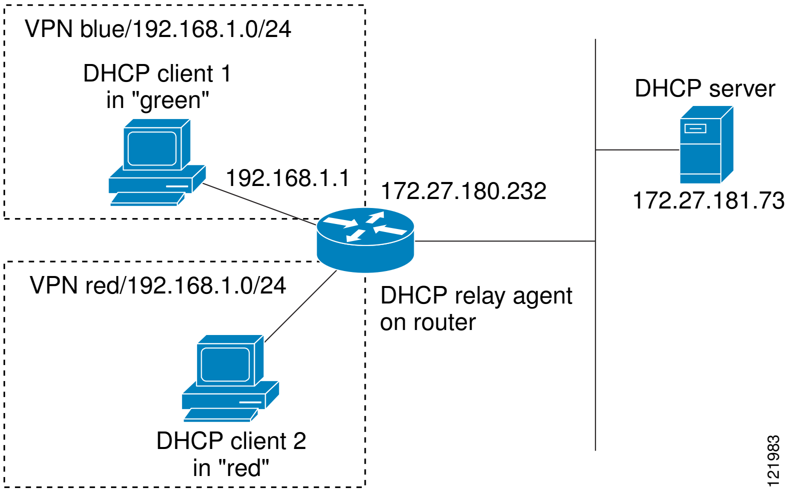
The subnet selection suboption allows the separation of the subnet, where the client resides, from the IP address used to communicate with the relay agent. In typical DHCP processing, the gateway address specifies both the subnet on which a DHCP client resides and the IP address that the server can use 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 that 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 the VPN suboptions to the packets and forwards the 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 from the packets 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 within which each client resides. 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 5 VPN DHCP Configuration



Before configuring DHCP relay support for Multiprotocol Label Switching (MPLS) VPNs, you must configure standard MPLS VPNs.

Note

- If the **ip dhcp relay information option vpn** global configuration command is configured and the **ip dhcp relay information option vpn-id** interface configuration command is not configured, the global configuration is applied to all interfaces.
- If the **ip dhcp relay information option vpn** global configuration command is configured and the **ip dhcp relay information option vpn-id** interface configuration command is also configured, the interface configuration command takes precedence over the global configuration command. However, the global configuration is applied to interfaces without the interface configuration.
- If the **ip dhcp relay information option vpn** global configuration command is not configured and the **ip dhcp relay information option vpn-id** interface configuration command is configured, only the interface on which the configuration option is applied is affected. All other interfaces are not impacted by the configuration.

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*
6. **ip dhcp relay information option vpn-id** [**none**]
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip dhcp relay information option vpn** **Example:** `Device(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. • The VPN suboptions are also added to the BOOTP broadcast packets when the command is configured.
Step 4	**interface** *type number* **Example:** `Device(config)# interface FastEthernet0/0`	Configures an interface and enters interface configuration mode.
Step 5	**ip helper-address vrf** *name* [**global**] *address* **Example:** `Device(config-if)# ip helper-address vrf vrf1 172.27.180.232`	Forwards UDP broadcasts, including BOOTP, received on an interface. • If the DHCP server resides in a different VRF or global space that is different from the VPN, the **vrf** *name* or **global** options allow you to specify the name of the VRF or the global space in which the DHCP server resides.
Step 6	**ip dhcp relay information option vpn-id** [**none**] **Example:** `Device(config-if)# ip dhcp relay information option vpn-id`	(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. • The VPN suboptions are also added to the BOOTP broadcast packets when the command is configured. • The **ip dhcp relay information option vpn-id none** command allows you to disable the VPN functionality on the interface. The only time you need to use this command is when the **ip dhcp relay information option vpn** global configuration command is configured and you want to override the global configuration. • The **no ip dhcp relay information option vpn-id** command removes the configuration from the running configuration. In this case, the interface inherits the global configuration, which may or may not be configured to insert VPN suboptions.

Step 7	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

Configuring Support for Relay Agent Information Option Encapsulation

When two relay agents are relaying messages between the DHCP client and the DHCP server, the 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, in a situation where an Intelligent Services 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.

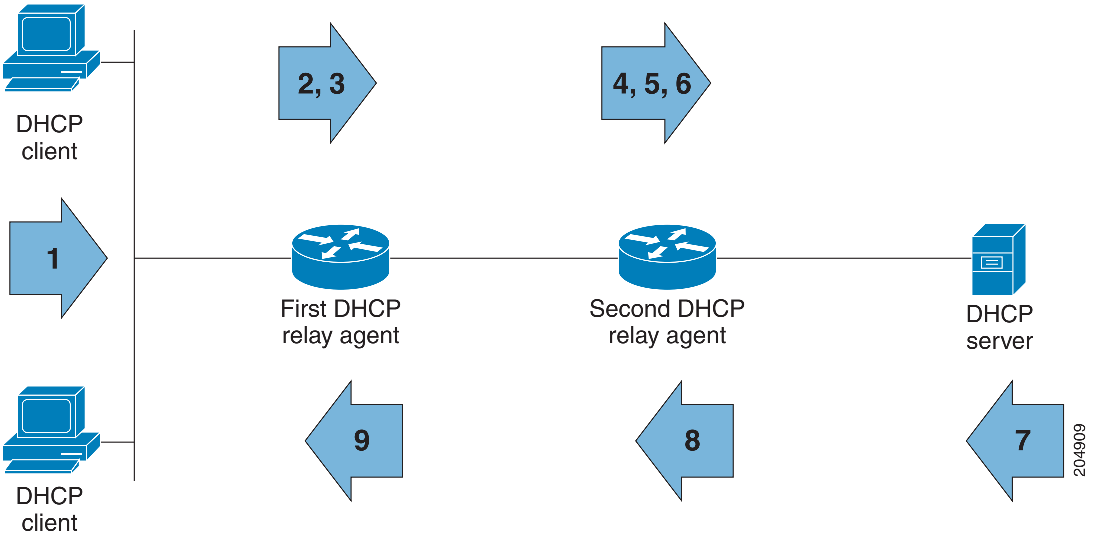
The DHCP Relay Option 82 Encapsulation feature allows the second relay agent to encapsulate option 82 information in a received message from the first relay agent if the second relay agent is configured to add its own option 82 information. This configuration allows the DHCP server to use option 82 information 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.

The figure below 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 agent, 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 first relay agent strips option 82 off from the packet before forwarding the packet to the client.

Figure 6 Processing DHCP Relay Agent Information Option Encapsulation Support



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**
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip dhcp relay information option** **Example:** `Device(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. • This function is disabled by default.
Step 4	**ip dhcp relay information option vpn** **Example:** `Device(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. • The VPN suboptions are also added to the BOOTP broadcast packets when the command is configured.
Step 5	**ip dhcp relay information policy encapsulate** **Example:** `Device(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. • Option 82 information from both relay agents will be forwarded to the DHCP server.
Step 6	**interface** *type number* **Example:** `Device(config)# interface FastEthernet0/0`	(Optional) Configures an interface and enters interface configuration mode. • If you configure the global configuration command, there is no need to configure the interface configuration command unless you want to apply a different configuration on a specific interface.
Step 7	**ip dhcp relay information policy-action encapsulate** **Example:** `Device(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. • This function is disabled by default. This command has precedence over the global configuration command. However, if 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.

Step 8	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

Setting the Gateway Address of the DHCP Broadcast to a Secondary Address Using 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. You only need to configure the **ip dhcp smart-relay** command if you have secondary addresses on that interface and you want the router to step through each IP network when forwarding DHCP requests. If smart relay agent forwarding is not 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 that 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**
4. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Configuring Support for Private and Standard Suboption Numbers

Some features that are not standardized will use the private Cisco relay agent suboption numbers. After the features are standardized, the relay agent suboptions are assigned the Internet Assigned Numbers Authority (IANA) numbers. Cisco software supports both private and IANA numbers for these suboptions.

Perform this task to configure the DHCP client to use private or IANA standard relay agent suboption numbers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp compatibility suboption link-selection** {**cisco** | **standard**}
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp compatibility suboption link-selection** {**cisco** | **standard**} **Example:** `Device(config)# ip dhcp compatibility suboption link-selection standard`	Configures the DHCP client to use private or IANA standard relay agent suboption numbers.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config)# exit`	(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting the DHCP Relay Agent

The **show ip route dhcp** command is useful to help troubleshoot issues with the DHCP relay agent that adds routes to clients from unnumbered interfaces. This command displays all routes added to the routing table by the DHCP server and the relay agent.

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** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip route dhcp** **Example:** `Device# show ip route dhcp`	Displays all routes added by the Cisco IOS DHCP server and relay agent.
Step 3	**show ip route dhcp** *ip-address* **Example:** `Device# show ip route dhcp 172.16.1.3`	Displays all routes added by the Cisco IOS DHCP server and relay agent associated with the specified IP address.

	Command or Action	Purpose
Step 4	**show ip route vrf** *vrf-name* **dhcp** **Example:** `Device# show ip route vrf vrf1 dhcp`	Displays all routes added by the Cisco IOS DHCP server and relay agent associated with the named VRF.
Step 5	**clear ip route** [**vrf** *vrf-name*] **dhcp** [*ip-address*] **Example:** `Device# clear ip route dhcp`	Removes routes from the routing table added by the DHCP server and relay agent for DHCP clients on unnumbered interfaces.

Configuration Examples for the Cisco IOS DHCP Relay Agent

Example: Configuring Support for the Relay Agent Information Option

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 DHCP server is enabled by default. In this example, the DHCP server is disabled:

```
! Reenables the DHCP server.
service dhcp
ip dhcp relay information option
!
interface ethernet0/0
 ip address 192.168.100.1 255.255.255.0
 ip helper-address 10.55.11.3
```

Example: Configuring Per-Interface Support for the Relay Agent Information Option

The following example shows that for subscribers who are being serviced by the same aggregation router, the relay agent information option for ATM subscribers must be processed differently from that for 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 the packet to the client. For Ethernet subscribers, the connected device provides the relay agent information option, and the option 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 ATM3/0
 no ip address
!
interface ATM3/0.1
 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 Ethernet4
 no ip address
!
interface Ethernet4/0.1
 encapsulation 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 of the Relay Agent Information Option

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 ATM4/0
 no ip address
!
interface ATM4/0.1 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 Class Support for Client Identification

In the following example, DHCP messages are received from DHCP clients on subnet 10.2.2.0. The relay agent will match and identify the relay class from the relay pool and forward the DHCP message to the appropriate DHCP server identified by the **relay target** command.

```
!
ip dhcp class H323
 option 60 hex 010203
!
ip dhcp class SIP
 option 60 hex 040506
!
! The following is the relay pool:
ip dhcp pool pool1
 relay source 10.2.2.0 255.255.255.0
 class H323
  relay target 192.168.2.1
  relay target 192.168.3.1
!
 class SIP
  relay target 192.168.4.1
```

Example: Configuring DHCP Relay Agent Support for MPLS VPNs

In the following example, the DHCP relay agent receives a DHCP request on Ethernet interface 0/1 and sends the request to the DHCP server located at IP helper address 10.44.23.7, which is associated with the VRF named vrf1:

```
ip dhcp relay information option vpn
!
interface ethernet 0/1
 ip helper-address vrf vrf1 10.44.23.7
!
```

Example: Configuring Support for Relay Agent Information Option Encapsulation

In the following example, DHCP relay agent 1 is configured globally to insert the relay agent information option into the DHCP packet. DHCP relay agent 2 is configured to add its own relay agent information option, including the VPN information, and to encapsulate the relay agent information option received from DHCP relay agent 1. The DHCP server receives the relay agent information options from both the relay agents, uses this information to assign IP addresses and other configuration parameters, and forwards them back to the client.

DHCP Relay Agent 1

```
ip dhcp relay information option
```

DHCP Relay Agent 2

```
ip dhcp relay information option
ip dhcp relay information option vpn
ip dhcp relay information option encapsulation
```

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

In the following example, the router will forward the DHCP broadcast received on Ethernet interface 0/0 to the DHCP server (10.55.11.3), by 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, the server 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 does not get a response, the router will move on and start using 172.16.31.254 in the giaddr field instead. Without the smart relay functionality, the router uses only 192.168.100.1 in the giaddr field.

```
ip dhcp smart-relay
!
interface ethernet0/0
 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	
DHCP conceptual information	"DHCP Overview" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP server configuration	"Configuring the Cisco IOS DHCP Server" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP client configuration	"Configuring the Cisco IOS DHCP Client" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP server on-demand address pool manager configuration	"Configuring the DHCP Server On-Demand Address Pool Manager" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP advanced features	"Configuring DHCP Services for Accounting and Security" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP enhancements for edge-session management configuration	"Configuring DHCP Enhancements for Edge-Session Management" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP options	" DHCP Options" appendix in the *Network Registrar User's Guide*, Release 6.1.1
DHCP for IPv6	"Implementing DHCP for IPv6" module in the *Cisco IOS IPv6 Configuration Guide*

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 releases, and feature sets, use Cisco MIB Locator found at the following URL: 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*
RFC 5460	DHCPv6 Bulk Leasequery

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for the Cisco IOS 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 7 Feature Information for the Cisco IOS DHCP Relay Agent

Feature Name	Releases	Feature Information
DHCP Relay Option 82 Encapsulation	12.2(33)SRD	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. The following commands were modified by this feature:**ip dhcp relay information policy**, **ip dhcp**

Feature Name	Releases	Feature Information
		relay information policy-action.
DHCP Class Support for Client Identification	12.4(11)T	This feature enhances the DHCP class mechanism to support options 60, 77, 124, and 125. These options identify the type of client sending the DHCP message. The DHCP relay agent can make forwarding decisions based on the content of the options in the DHCP message sent by the client. The following command was introduced by this feature: **option hex**.

Feature Name	Releases	Feature Information
DHCPv4 Relay per Interface VPN ID Support	12.4(11)T	The DHCPv4 Relay per Interface VPN ID Support feature allows the Cisco IOS DHCP relay agent to be configured per interface to override the global configuration of the **ip dhcp relay information option vpn** command. This feature allows subscribers with different relay information option VPN ID requirements on different interfaces to be reached from one Cisco router. The following command was introduced by this feature: **ip dhcp relay information option vpn-id**.

Feature Name	Releases	Feature Information
DHCP Relay Option 82 per Interface Support	12.4(6)T 12.2(31)SB2 12.2(33)SRC	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. 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 Information
DHCP Subscriber Identifier Suboption of Option 82	12.3(14)T 12.2(28)SB 12.2(33)SRB	This feature enables an ISP to add a unique identifier to the subscriber-identifier suboption of the relay agent information option. The following command was introduced by this feature: **ip dhcp relay information option subscriber-id**.

Feature Name	Releases	Feature Information
DHCP Relay MPLS VPN Support	12.2(8) 12.2(28)SB 12.2(33)SRC	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. The following commands were modified by this feature: **ip dhcp relay information option**, **ip helper address**.

Feature Name	Releases	Feature Information
DHCPv6 Bulk Lease query	15.1(1)S	Cisco IOS DHCPv6 relay agent supports bulk lease query in accordance with RFC 5460. The following commands were introduced or modified by this feature: **debug ipv6 dhcp relay** , **ipv6 dhcp-relay bulk-lease**.

Glossary

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

DHCP—Dynamic Host Configuration Protocol. A network protocol that automatically provides an IP host with an IP address and other related configuration information (for example, subnet mask and default gateway).

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. 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—A 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 Provider Edge (PE) router. Each VPN that is 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 DHCP Client

Cisco IOS 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 DHCP client. It includes information on the Cisco DHCP FORCERENEW feature, which provides entity authentication and message authentication.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 Configuring the DHCP Client

The DHCP client can be configured on Ethernet interfaces and on PPP over ATM (PPPoA) and certain ATM interfaces. The DHCP client works with ATM point-to-point interfaces and will accept any encapsulation type. For ATM multipoint interfaces, the DHCP client is supported using only the aal5snap encapsulation type combined with Inverse Address Resolution Protocol (ARP). Inverse ARP, which builds an ATM map entry, is necessary to send unicast packets to the server (or relay agent) on the other end of the connection. Inverse ARP is supported only for the aal5snap encapsulation type.

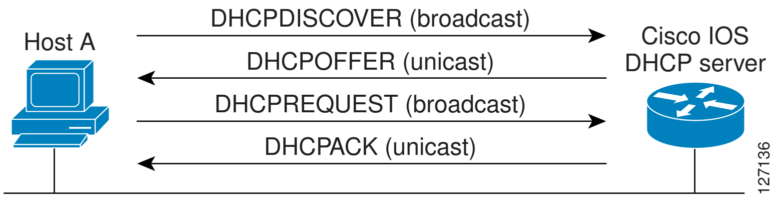
For multipoint interfaces, an IP address can be acquired using other encapsulation types because broadcast packets are used. However, unicast packets to the other end will fail because there is no ATM map entry and thus DHCP renewals and releases also fail.

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 7 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 33--This option is used to configure a list of static routes in the client.
- 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.
- Option 120--This option is used to specify a 32-bit (binary) IPv4 address to be used by the Session Initiation Protocol (SIP) client to locate a SIP server.
- Option 121--This option is used to configure classless static routes by specifying classless network destinations in these routes: that is, each routing table entry includes a subnet mask.

Note If a request includes both static routes and classless static routes, the client uses only the classless static routes. If the DHCP server returns both a classless static route option and a router option, the DHCP client ignores the router option.

- Option 125--This option is used by DHCP clients and servers to exchange vendor-specific information.

DHCP Client on WAN Interfaces

The DHCP client on WAN interfaces allows a DHCP client to acquire an IP address over PPPoA and certain ATM interfaces. By using DHCP rather than the IP Control Protocol (IPCP), a DHCP client can acquire other useful information such as Domain Name System (DNS) addresses, the DNS default domain name, and the default route.

The configuration of PPPoA and Classical IP and ARP over ATM already allows for a broadcast capability over the interface (using the **broadcast** keyword on the ATM interface). Most changes in this feature are directed at removing already existing restrictions on what types of interfaces are allowed to send out DHCP packets (previously, dialer interfaces have not been allowed). This feature also ensures that DHCP RELEASE messages are sent out the interface before a connection is allowed to be broken.

DHCP FORCERENEW

The Cisco DHCP FORCERENEW feature provides entity authentication and message authentication, in accordance with RFC 3118, by which DHCP clients and servers authenticate the identity of other DHCP entities and verify that the content of a DHCP message has not been changed during delivery through the network.

The message authentication mechanism allows servers to determine whether a request for DHCP information comes from a client that is authorized to use the network. It also allows clients to verify that a DHCP server can be trusted to provide valid configuration.

The Cisco DHCP FORCERENEW feature requires authentication. All client-server exchanges must be authenticated: The **ip dhcp client authentication mode**and **key chain** commands must be configured.

When the client gets a FORCERENEW message, it does the following:

- Authenticates the message according to the authentication mode specified in the **ip dhcp client authentication mode** command. The Cisco DHCP FORCERENEW feature supports both token-based and Message Digest 5 (MD5)-based authentication.

  - Token-based authentication is useful only for basic protection against inadvertently instantiated DHCP servers. Tokens are transmitted in plain text; they provide weak authentication and do not provide message authentication.
  - MD5-based authentication provides better message and entity authentication because it contains a single-use value generated by the source as a message authentication code.
- Changes its state to RENEW.
- Tries to renew its lease according to normal DHCP procedures.

The client discards any multicast FORCERENEW message or message that fails authentication.

How to Configure the DHCP Client

- Configuring the DHCP Client, page 96
- Forcing a Release or Renewal of a DHCP Lease for a DHCP Client, page 98
- Enabling FORCERENEW-Message Handling, page 100

Configuring the DHCP Client

- DHCP Client Default Behavior, page 96
- Troubleshooting Tips, page 98

DHCP Client Default Behavior

Cisco routers running Cisco IOS 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** 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 take effect only after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp**EXECcommandshave 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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip dhcp client client-id** {*interface-name*| **ascii** *string*| **hex** *string*} **Example:** `Router(config-if)# ip dhcp client client-id ascii mytest1`	(Optional) Specifies the client identifier. • 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*} **Example:** `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*] **Example:** `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* **Example:** `Router(config-if)# ip dhcp client hostname router1`	(Optional) Specifies or modifies the hostname sent in the DHCP message.

	Command or Action	Purpose
Step 8	[**no**] **ip dhcp client request** *option-name* **Example:** `Router(config-if)# no ip dhcp client request tftp-server-address`	(Optional) Configures a DHCP client to request an option from a DHCP server. • 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** **Example:** `Router(config-if)# ip address dhcp`	Acquires an IP address on an interface from DHCP.

Troubleshooting Tips

To verify the configuration, you can use the **debug dhcp detail** 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.

The following are troubleshooting tips for DHCP clients on WAN interfaces:

- An ATM primary interface is always multipoint.
- An ATM subinterface can be multipoint or point-to-point.
- If you are using a point-to-point interface, the routing table determines when to send a packet to the interface and ATM map entries are not needed. Consequently, Inverse ARP, which builds ATM map entries, is not needed.
- If you are using a multipoint interface, you must use Inverse ARP to discover the IP address of the other side of the connection.
- You can specify Inverse ARP through the **protocol ip inarp**command. You must use the aal5snap encapsulation type when using Inverse ARP because it is the only encapsulation type that supports Inverse ARP.

Forcing a Release or Renewal of a DHCP Lease for a DHCP Client

Perform this task to force a release or renewal of a DHCP lease for a DHCP client.

Forcing a release or renewal of a DHCP lease for a DHCP client provides the ability to perform two independent operations from the command-line interface (CLI) in EXEC mode:

- Immediately release a DHCP lease for a DHCP client.
- Force a DHCP renewal of a lease for a DHCP client.

This functionality provides the following benefits:

- Eliminates the need to go into the configuration mode to reconfigure the router to release or renew a DHCP lease.
- Simplifies the release and renewal of a DHCP lease.
- Reduces the amount of time spent performing DHCP IP release and renewal configuration tasks.

DHCP Release and Renew CLI Operation

Release a DHCP Lease

The **release dhcp** command starts the process to immediately release a DHCP lease for the specified interface. After the lease is released, the interface address is deconfigured. The **release dhcp** command does not deconfigure the **ip address dhcp** command specified in the configuration file for the interface. During a write memory or show running configuration file action, or if the router is rebooted, the **ip address dhcp** command executes to acquire a DHCP address for the interface.

The original IP address for the interface must be assigned by the DHCP server. If the interface is not assigned an IP address by the DHCP server, the **release dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

Renew a DHCP Lease

The **renew dhcp** command advances the DHCP lease timer to the next stage, at which point one of the following occurs:

- If the lease is currently in a BOUND state, the lease is advanced to the RENEW state and a DHCP RENEW request is sent.
- If the lease is currently in a RENEW state, the timer is advanced to the REBIND state and a DHCP REBIND request is sent.

If there is no response to the RENEW request, the interface remains in the RENEW state. In this case, the lease timer will advance to the REBIND state and subsequently send a REBIND request.

If a NAK response is sent in response to the RENEW request, the interface is deconfigured.

The original IP address for the interface must be assigned by the DHCP server. If the interface is not assigned an IP address by the DHCP server, the **renew dhcp** command fails and displays the following error message:

```
Interface does not have a DHCP originated address
```

Note In Cisco IOS Release 15.0(1)M and later releases Cisco IOS DHCP clients do not accept packets with zero lease time or no lease time option.

The DHCP client must be assigned an IP address by the DHCP server.

Note If the DHCP client is not assigned an IP address by the DHCP server, the DHCP release and renew CLI commands will fail.

>

SUMMARY STEPS

1. **enable**
2. **release dhcp** *type number*
3. **renew dhcp** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**release dhcp** *type number* **Example:** `Router# release dhcp ethernet 3/1`	Performs an immediate release of the DHCP lease for the interface and deconfigures the IP address for the interface.
Step 3	**renew dhcp** *type number* **Example:** `Router# renew dhcp ethernet 3/1`	Forces the DHCP timer to advance to the next stage, at which point a subsequent action is taken: A DHCP REQUEST packet is sent to renew or rebind the lease.

Enabling FORCERENEW-Message Handling

Perform this task to specify the type of authentication to be used in DHCP messages on the interface, specify the key chain to be used in authenticating a request, and enable FORCERENEW-message handling on the DHCP client when authentication is enabled.

You must configure the same authentication mode, and the same secret ID and secret value that were configured in the **key chain** command, on both the client and the server.

SUMMARY STEPS

1. **interface** *type number*
2. **ip dhcp client authentication key-chain** *name*
3. **ip dhcp client authentication mode** *type*
4. **exit**
5. **key chain** *name-of-chain*
6. **exit**
7. **ip dhcp-client forcerenew**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *type number* **Example:** `Router(config)# interface Ethernet 1`	Configures an interface type and enters interface-configuration mode.
Step 2	**ip dhcp client authentication key-chain** *name* **Example:** `Router(config-if)# ip dhcp client authentication key-chain dhcp1`	Specifies the key chain to be used in authenticating a request.
Step 3	**ip dhcp client authentication mode** *type* **Example:** `Router(config-if)# ip dhcp client authentication mode md5`	Specifies the type of authentication to be used in DHCP messages on the interface.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.

	Command or Action	Purpose

Step 5	**key chain** *name-of-chain*
	Example:
	`Router(config-keychain)# key chain dhcp1`
	Example:
	`key 1234`
	Example:
	`key-string secret`
		Enters key-chain configuration mode and identifies the authentication strings to be used in the named key chain.

Step 6	**exit** **Example:** `Router(config-keychain)# exit`	Exits key-chain configuration mode and enters global configuration mode.
Step 7	**ip dhcp-client forcerenew** **Example:** `Router(config)# ip dhcp-client forcerenew`	Enables DHCP FORCERENEW-message handling on the DHCP client.

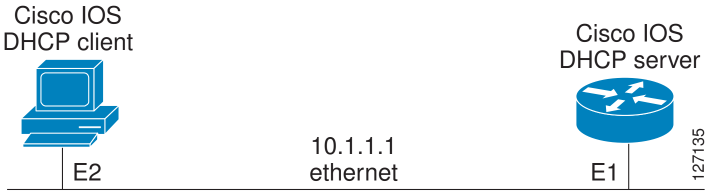
Step 8	**end**
	Example:
	`Router(config)# end`
		(Optional) Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for the DHCP Client

Example Configuring the DHCP Client

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

Figure 8 Topology Showing a DHCP Client with a Ethernet 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 E2:

```
interface Ethernet2
 ip address dhcp
```

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

Example Customizing the DHCP Client Configuration

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

```
interface Ethernet 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 host1
 no ip dhcp client request tftp-server-address
 ip address dhcp
```

Example Configuring an ATM Primary Interface (Multipoint) Using aal5snap Encapsulation and Inverse ARP

In the following example, the **protocol ip 255.255.255.255 broadcast** configuration is needed because there must be an ATM map entry to recognize the broadcast flag on the permanent virtual circuit (PVC). You can use any ATM map entry. The **protocol ip inarp** configuration is needed so that the ATM Inverse ARP can operate on the interface such that the system can be pinged once an address is assigned by DHCP.

```
interface atm0
 ip address dhcp
 pvc 1/100
  encapsulation aal5snap
  broadcast
  protocol ip 255.255.255.255 broadcast
     protocol ip inarp
```

Example Configuring an ATM Point-to-Point Subinterface Using aa15snap Encapsulation

The following example shows an ATM point-to-point subinterface configuration using aa15snap encapsulation:

```
interface atm0.1 point-to-point
 ip address dhcp
 pvc 1/100
  encapsulation aal5snap
  broadcast
```

Example Configuring an ATM Point-to-Point Subinterface Using aa15nlpid Encapsulation

The following example shows an ATM point-to-point subinterface configuration using aa15nlpid encapsulation:

```
interface atm0.1 point-to-point
 ip address dhcp
 pvc 1/100
  encapsulation aal5nlpid
  broadcast
```

Example Configuring an ATM Point-to-Point Subinterface Using aa15mux PPP Encapsulation

The following example shows an ATM point-to-point subinterface configuration using aa15mux PPP encapsulation:

```
interface atm0.1 point-to-point
 pvc 1/100
  encapsulation aal5mux ppp virtual-template1
  broadcast
!
interface virtual-template1
 ip address dhcp
```

Example Releasing a DHCP Lease

In the following example, a DHCP release is performed on an interface that was originally assigned an IP address by the DHCP server:

```
Router# release dhcp ethernet 3/1
```

In the following example, an attempt is made to release the DHCP lease on an interface that was not originally assigned an IP address by the DHCP server:

```
Router# release dhcp ethernet 3/1

Interface does not have a DHCP originated address
```

In the following example, the **release dhcp** command is executed without specifying the *type*and *number*arguments:

```
Router# release dhcp

Incomplete command.
```

Example Renewing a DHCP Lease

In the following example, the DHCP lease is renewed on an interface that was originally assigned an IP address by the DHCP server:

```
Router# renew dhcp ethernet 3/1
```

In the following example, an attempt is made to renew the DHCP lease on an interface that was not originally assigned an IP address by the DHCP server:

```
Router# renew dhcp ethernet 3/1

Interface does not have a DHCP originated address
```

In the following example, the **renew dhcp** command is executed without specifying the *type*and *number*arguments:

```
Router# renew dhcp

Incomplete command.
```

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 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 DHCP Relay Agent” module
DHCP advanced features	“Configuring DHCP Services for Accounting and Security” module
DHCP enhancements for edge-session management	“Configuring DHCP Enhancements for Edge-Session Management” 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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*
RFC 3118	*Authentication for DHCP Messages*
RFC 3203	*DHCP reconfigure extension*
RFC 3361	*DHCP-for-IPv4 Option for SIP Servers*
RFC 3442	*Classless Static Route Option for DHCPv4*
RFC 3925	*Vendor-Identifying Vendor Options for DHCPv4*

Technical Assistance

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

Feature Information for the 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 8 Feature Information for the Cisco IOS DHCP Client

Feature Name	Releases	Feature Information
Configurable DHCP Client	12.2(28)SB 12.3(8)T	The Configurable DHCP Client feature 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. The following commands were introduced: **ip dhcp client class-id**, **ip dhcp client client-id**, **ip dhcp client hostname**, **ip dhcp client lease**, **ip dhcp client request**.
DHCP Release and Renew CLI in EXEC Mode	12.2(28)SB 12.2(33)SRC 12.3(4)T	This feature provides the ability to perform two independent operations from the CLI: • Immediately release a DHCP lease for a DHCP client • Force a DHCP renewal of a lease for a DHCP client The following commands were introduced: **release dhcp**and **renew dhcp**.
DHCP Client on WAN Interfaces	12.2(8)T 12.2(28)SB	The DHCP Client on WAN Interfaces feature extends the DHCP to allow a DHCP client to acquire an IP address over PPP over ATM (PPPoA) and certain ATM interfaces. No commands were introduced or modified by this feature.

Feature Name	Releases	Feature Information
Cisco DHCP FORCERENEW	12.4(22)YB 15.0(1)M	This feature enhances security by providing entity authentication and message authentication. The following commands were introduced or modified: **ip dhcp client authentication key-chain**, **ip dhcp client authentication mode**, **ip dhcp-client forcerenew**, **ip dhcp client request**.

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 Port-Based Address Allocation

The DHCP Server Port-Based Address Allocation feature provides port-based address allocation support on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server for the Ethernet platform. The DHCP server provides address assignment support based on the point of attachment of the client network.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 Server Port-Based Address Allocation

The DHCP Server Port-Based Address Allocation feature does not support Virtual routing and forwarding (VRF) and virtual private network (VPNs).

Information About DHCP Server Port-Based Address Allocation

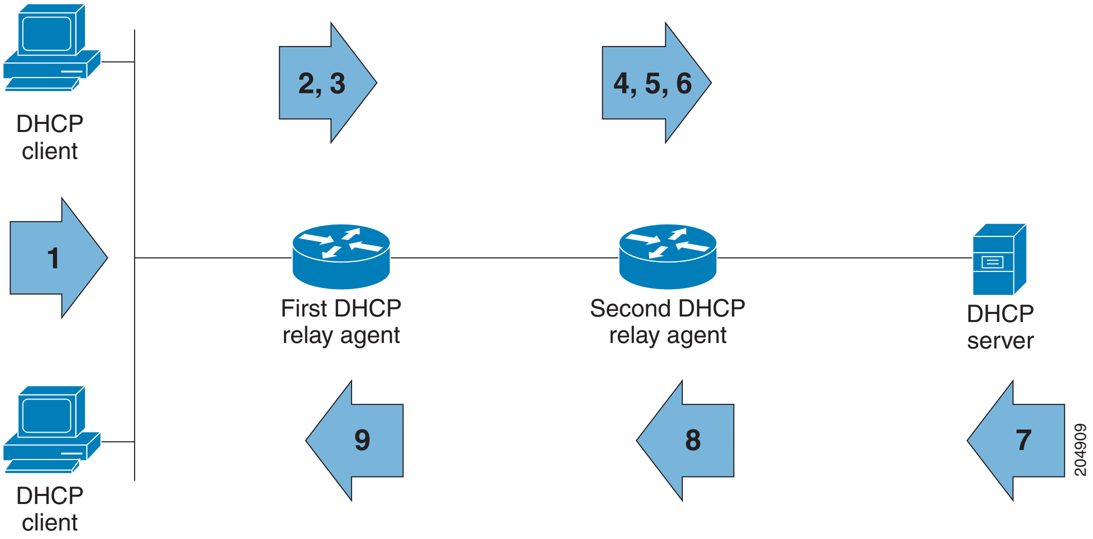
DHCP Server Port-Based Address Allocation Feature Design

When Cisco industrial Ethernet switches are deployed on the factory floor, they offer connectivity to the directly connected manufacturing devices. A failure manufacturing device must be repaired immediately in the existing network or replaced by a new device. The DHCP protocol recognizes DHCP clients by the client identifier (ID) option in the DHCP packet. Clients who do not include the client ID option are identified by the client hardware address. The DHCP Server Port-Based Address Allocation feature introduces the capability to ensure that the same IP address is always offered to the replacement device as the device being replaced. This IP address is always offered to the same connected port even as the client ID or client hardware address (chaddr) changes in the DHCP messages received on that port.

If this feature is configured, the port name of the interface overrides the information the client sends and the actual point of connection. Then a port on the switch becomes the client ID.

In all cases, if you connect the Ethernet cable to the same port, the same IP address is allocated through the DHCP to the attached device. The figure below shows an industrial Ethernet switch using DHCP to assign one IP address per port to directly connected manufacturing devices.

Figure 9 DHCP Server Port-Based Address Assignment to Directly Connected Manufacturing Devices



How to Configure DHCP Server Port-Based Address Allocation

- Automatically Generating a Subscriber Identifier for a DHCP Message Received on a Port, page 110
- Preassigning IP Addresses and Associating Them to a Client, page 112
- Preassigning IP Addresses and Associating Them to a Client, page 114

Automatically Generating a Subscriber Identifier for a DHCP Message Received on a Port

Perform this task to automatically generate a unique ID, called a subscriber ID for a DHCP message received on a port.

If the DHCP Server Port-Based Address Allocation feature is configured, the subscriber ID value is used in place of the client ID to provide stable IP address assignment. The subscriber ID value is based on the short name of the port to which the directly connected device is attached. If this device is removed and replaced with a new device, the new device maintains the same subscriber ID.

The subscriber ID is used at the same point where the client ID or the client MAC address is currently captured during the DHCP IP address assignment process.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp use subscriber-id client-id**
4. **interface type number**
5. **ip dhcp server use subscriber-id client-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp use subscriber-id client-id** **Example:** `Router(config)# ip dhcp use subscriber-id client-id`	Configures the DHCP server to globally use the subscriber ID as the client ID on all incoming DHCP messages. • DHCP uses the subscriber ID configured on the interface to generate the client ID. If no subscriber ID is configured then the client ID is automatically generated based on the short name of the interface. The client ID already present in the message is ignored. • For port based address allocation, do not configure any subscriber ID on the interface. It must be generated automatically from interface name.
Step 4	**interface type number** **Example:** `Router(config)# interface Ethernet 0/0`	(Optional) Configures an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 5	**ip dhcp server use subscriber-id client-id** **Example:** `Router(config-if)# ip dhcp server use subscriber-id client-id`	(Optional) Configures the DHCP server to use the subscriber ID as the client ID on all incoming DHCP messages on the interface.

- Troubleshooting Tips, page 112

Troubleshooting Tips

Use the following command to debug any errors that you may encounter when you configure DHCP to automatically generate a unique ID:

- **debug ip dhcp server packets**

Preassigning IP Addresses and Associating Them to a Client

Perform this task to preassign an IP address and associate it to a client identified by a client ID or MAC address.

For port-based address assignment, you must perform the task in the Automatically Generating a Subscriber Identifier for a DHCP Message Received on a Port, page 110 task to associate the client ID with the subscriber ID. The subscriber ID value is based on the short name of the port to which the directly connected device is attached.

Configure a normal DHCP pool by supplying any DHCP options and lease time. Preassigned addresses are automatically excluded from normal dynamic IP address assignment. Preassigned addresses cannot be used in host pools, but there can be multiple preassigned addresses per DHCP address pool.

Note

- Only one IP address can be assigned per port.
- Preassigned addresses (also called reserved addresses) cannot be cleared by using the **clear ip dhcp binding** command.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask* | / *prefix-length*]
5. **address** *ip-address* **client-id** *string* [**ascii**]
6. **address** *ip-address* **hardware-address** *mac-address* [*hardware-number*]
7. **end**
8. **show ip dhcp pool** [*name*]
9. **show ip dhcp binding**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool pool1`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 4	**network** *network-number* [*mask* | / *prefix-length*] **Example:** `Router(dhcp-config)# network 10.10.10.0 /24`	Specifies the subnet network number and mask of the DHCP address pool.
Step 5	**address** *ip-address* **client-id** *string* [**ascii**] **Example:** `Router(dhcp-config)# address 10.10.10.2 client-id Et1/0 ascii`	Reserves an IP address for a DHCP client identified by the client ID. • The *string* argument can be an ASCII value or a hexadecimal value. • For port-based address allocation the *string* argument must be the name of the port and the **ascii** keyword must be specified.

	Command or Action	Purpose
Step 6	**address** *ip-address* **hardware-address** *mac-address* [*hardware-number*] **Example:** `Router(dhcp-config)# address 10.10.10.3 hardware-address b708.1388.f166`	(Optional) Reserves an IP address for a client identified by the hardware address. • This command is used for clients identified by the hardware address included in the fixed-size header of the DHCP message.

Step 7	**end**
	Example:
	`Router(dhcp-config)# end`
		Returns to privileged EXEC mode.

Step 8	**show ip dhcp pool** [*name*] **Example:** `Router> show ip dhcp pool`	(Optional) Displays information about DHCP address pools.
Step 9	**show ip dhcp binding** **Example:** `Router> show ip dhcp binding` **Example:**	(Optional) Displays infinite binding for the configured addresses.

Preassigning IP Addresses and Associating Them to a Client

Note

Perform this task to restrict address assignments from the DHCP address pool only to preconfigured reservations.

When the DHCP Server Port-Based Address Allocation feature is configured on multiple switches, devices connected to one switch may also receive an IP address assignment from the neighboring switches rather than the local DHCP address pool switch. If you want the switch to serve only the client directly connected to the switch, you can configure a group of switches with pools that share a common IP subnet and ignore the requests from other clients (not connected to this switch).

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **reserved-only**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool pool1`	Configures a DHCP address pool on a DHCP server and enters DHCP pool configuration mode.
Step 4	**reserved-only** **Example:** `Router(dhcp-config)# reserved-only`	Restricts address assignments from the DHCP address pool only to the preconfigured reservations.

Configuration Examples for DHCP Server Port-Based Address Allocation

DHCP Server Port-Based Address Allocation Example

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client ID fields in the DHCP messages and use this subscriber ID as the client ID. The DHCP client is preassigned IP address 10.1.1.7.

```
!
```

```
ip dhcp use subscriber-id client-id
ip dhcp subscriber-id interface-name
ip dhcp excluded-address 10.1.1.1 10.1.1.3
!
ip dhcp pool dhcppool
 network 10.1.1.0 255.255.255.0
 address 10.1.1.7 client-id Et1/0 ascii
```

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

```
Router# show ip dhcp pool dhcppool
Pool test :
 Current index        IP address range                    Leased/Total
 10.1.1.1              10.1.1.1 - 10.1.1.254         0     / 254
 3 reserved addresses are currently in the pool :
Address          Client
 10.1.1.07         Et1/0
 10.1.1.20         xyz
 10.1.1.30         aabb.cc00.1501
```

Additional References

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*

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 or modified standards are supported by this feature and support for existing standards has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: 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 and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCP Server Port-Based Address Allocation

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 DHCP Port-Based Address Allocation

Feature Name	Releases	Feature Information
DHCP Server Port-Based Address Allocation	12.2(33)SXI4 Cisco IOS XE 3.1.0SG	The DHCP Server Port-Based Address Allocation feature provides port-based address allocation support on the Cisco IOS DHCP server for the industrial Ethernet platform. The DHCP server provides address assignment support based on the point of attachment of the client to the network. The following commands were introduced or modified: **address client-id**, **address hardware-address**, **ip dhcp server use subscriber-id client-id**, **ip dhcp subscriber-id interface-name**, **ip dhcp use subscriber-id client-id**, **reserved-only**, and **show ip dhcp pool**.

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.

IPv6 Access Services: DHCPv6 Relay Agent

A Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay agent, which may reside on the client's link, is used to relay messages between the client and the server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 IPv6 Access Services: DHCPv6 Relay Agent

DHCPv6 Relay Agent

A DHCPv6 relay agent, which may reside on the client’s link, is used to relay messages between the client and the server. The DHCPv6 relay agent operation is transparent to the client. A DHCPv6 client locates a DHCPv6 server using a reserved, link-scoped multicast address. For direct communication between the DHCPv6 client and the DHCPv6 server, both of them must be attached to the same link. However, in some situations where ease of management, economy, or scalability is a concern, it is desirable to allow a DHCPv6 client to send a message to a DHCPv6 server that is not connected to the same link.

DHCPv6 Relay Agent Notification for Prefix Delegation

DHCPv6 Relay Agent Notification for Prefix Delegation

The DHCPv6 relay agent notification for prefix delegation allows the router working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 RELAY-REPLY packet that is relayed by the relay agent to the client. When a prefix delegation option is found by the relay agent, the relay agent extracts the information about the prefix that is being delegated and inserts an IPv6 static route matching the prefix delegation information onto the relay agent. Future packets destined to that prefix via relay will be forwarded based on the information contained in the prefix delegation. The IPv6 static route is then left in the routing table until the prefix delegation lease time expires or the relay agent receives a release packet from the client releasing the prefix delegation.

No user configuration is required for this feature. Static route management is done automatically by the relay agent.

IPv6 routes are added when the relay agent relays a RELAY-REPLY packet, and IPv6 routes are deleted when the prefix delegation lease time expires or the relay agent receives a release message. An IPv6 static route in the routing table of the relay agent can be updated when the prefix delegation lease time is extended.

The DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation feature leaves a static IPv6 route on the routing table of the relay agent. The registered IPv6 address allows unicast reverse packet forwarding (uRPF) to work by allowing the router doing the reverse lookup to confirm that the IPv6 address on the relay agent is not malformed or spoofed. The static route that remains in the routing table of the relay agent can be redistributed to other routing protocols to advertise the subnets to other nodes. Static routes will be removed when a DHCP_DECLINE message is sent by the client.

DHCPv6 Relay SSO and ISSU

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

The Cisco IOS In Service Software Upgrade (ISSU) process allows Cisco IOS 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 the Cisco IOS software to be modified while packet forwarding continues. This increases network availability and reduces downtime caused by planned software upgrades.

The SSO and the ISSU use redundant hardware, with the active and standby RP each running an instance of the DHCPv6 relay agent. Both instances exchange run-time state data.

For further information about SSO and ISSU, see the “Stateful Switchover” and the “Cisco IOS In Service Software Upgrade Process” modules respectively, in the *Cisco IOS High Availability Configuration Guide*.

- DHCPv6 Relay Options: Remote ID for Ethernet Interfaces, page 120
- DHCPv6 Relay Options: Reload Persistent Interface ID Option, page 121

DHCPv6 Relay Options: Remote ID for Ethernet Interfaces

This feature adds the remote identification (remote-ID) option to relayed (RELAY-FORWARD) DHCPv6 packets.

The remote-ID option provides information to the DHCPv6 server, including port information, the system's DUID, and the VLAN ID. Collectively, this information can be used to uniquely identify both the relay and the port on the relay through which the client's packet arrived. The DHCPv6 server uses this information to select parameters specific to a particular user, host, or subscriber modem. This feature works only for Ethernet interfaces at this time.

This feature introduces no user configuration. Because the addition of the remote-ID option to the RELAY-FORWARD packet occurs automatically, no user configuration is necessary.

The DHCPv6 server does not need to echo the remote-ID option in the RELAY-REPLY packet. Internet Assigned Numbers Authority (IANA) has assigned the DHCPv6 option code 37 for the relay agent remote-ID option.

If the remote-ID option is included in the RELAY-REPLY packet, the option is stripped out of the packet before the packet is relayed to the client.

DHCPv6 Relay Options: Reload Persistent Interface ID Option

This feature makes the interface-ID option, which is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet, persistent. A persistent interface-ID option will not change if the router acting as a relay agent goes offline (such as during a reload or a power outage). When the router acting as a relay agent returns online, it is possible that changes to the internal interface index of the relay agent may have occurred in certain scenarios (such as cases where the relay agent reboots and has a change in the number of interfaces in the interface index, or the relay agents boots up and has more virtual interfaces than it did before the reboot). This feature prevents this scenario from causing any problems.

This feature changes the DHCPv6 interface-ID option to be expressed as simply the short form of the interface name. This syntax helps avoid potential problems that could arise due to physical or logical interfaces changing on the relay agent after a reload.

How to Configure IPv6 Access Services: DHCPv6 Relay Agent

- Configuring the DHCPv6 Relay Agent, page 121

Configuring the DHCPv6 Relay Agent

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 4/2`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*] **Example:** `Router(config-if) ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3`	Specifies a destination address to which client packets are forwarded and enables the DHCPv6 relay service on the interface.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Configuration Examples for IPv6 Access Services: DHCPv6 Relay Agent

Example: Configuring the DHCPv6 Relay Agent

```
Device# show ipv6 dhcp interface

Ethernet1/0 is in relay mode
  Relay destinations:
    3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
Serial3/0 is in relay mode
  Relay destinations:
    3FFB:C00:C18:6:A8BB:CCFF:FE03:2600
    FE80::A8BB:CCFF:FE03:2801 on Serial3/0
    FF05::1:3
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Access Services: DHCPv6 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 10 Feature Information for IPv6 Access Services: DHCPv6 Relay Agent

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCPv6 Relay Agent	12.3(11)T 12.4 12.2(46)SE 12.2(50)SG 3.2.0SG 15.0(2)SG 12.2(33)SRC 12.2(33)SXI	A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and server. The following commands were introduced or modified: **ipv6 dhcp relay destination**, **show ipv6 dhcp interface**.
DHCP: DHCPv6 Relay SSO/ ISSU	12.2(33)SRE	SSO and ISSU use redundant hardware, with the active and standby RP each running an instance of the DHCP relay agent.
DHCPv6 Ethernet Remote ID Option	12.2(46)SE 12.2(52)SG 3.2.0SG 15.0(2)SG 12.2(33)SRC 12.2(33)SXI	This feature adds the remote-ID option to relayed (RELAY-FORWARD) DHCPv6 packets.
DHCPv6 Relay Agent Notification for Prefix Delegation	12.2(46)SE 12.2(33)SRC 12.2(33)SXI 15.0(1)S	DHCPv6 relay agent notification for prefix delegation allows the router working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 packet that is being relayed by the relay agent to the client.

Feature Name	Releases	Feature Information
DHCPv6 Relay: Reload Persistent Interface ID Option	12.2(46)SE 12.2(52)SG 3.2.0SG 15.0(2)SG 12.2(33)SRC 12.2(33)SXI	This feature makes the interface-ID option, which is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet, persistent.

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.

IPv6 Access Services: Stateless DHCPv6

The stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6) feature allows DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 IPv6 Access Services: Stateless DHCPv6

Information Refresh Server Option

The DHCPv6 information refresh option can specify an upper boundary for the length of time a client should wait before refreshing information retrieved from DHCPv6. This option is used with stateless DHCPv6, because there are no addresses or other entities with lifetimes that can tell the client when to contact the DHCPv6 server to refresh its configuration.

SIP Server Options

Session initiation protocol (SIP) server options contain either a list of domain names or IPv6 addresses that can be mapped to one or more SIP outbound proxy servers. One option carries a list of domain names, and the other option carries a list of 128-bit IPv6 addresses.

SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has several logical components: user agents, proxy servers, redirect servers, and registrars. User agents may contain SIP clients; proxy servers always contain SIP clients.

SNTP Server Option

The SNTP server option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. The clients use these SNTP servers to synchronize their system time to that of the standard time servers. The server may list the SNTP servers in decreasing order of preference, but clients must treat the list of SNTP servers as an ordered list.

How to Configure IPv6 Access Services: Stateless DHCPv6

- Configuring the Stateless DHCPv6 Function, page 128

Configuring the Stateless DHCPv6 Function

The server maintains no state related to clients; for example, no prefix pools and records of allocation are maintained. Therefore, this function is “stateless” DHCPv6.

- Configuring the Stateless DHCPv6 Server, page 128
- Configuring the Stateless DHCPv6 Client, page 130
- Enabling Processing of Packets with Source Routing Header Options, page 131
- Importing Stateless DHCPv6 Server Options, page 132

Configuring the Stateless DHCPv6 Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **dns-server** *ipv6-address*
5. **domain-name** *domain*
6. **exit**
7. **interface** *type number*
8. **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]
9. **ipv6 nd other-config-flag**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Router(config)# ipv6 dhcp pool dhcp-pool`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**dns-server** *ipv6-address* **Example:** `Router(config-dhcp) dns-server 2001:DB8:3000:3000::42`	Specifies the DNS IPv6 servers available to a DHCPv6 client.
Step 5	**domain-name** *domain* **Example:** `Router(config-dhcp)# domain-name domain1.com`	Configures a domain name for a DHCPv6 client.
Step 6	**exit** **Example:** `Router(config-dhcp)# exit`	Exits DHCPv6 pool configuration mode, and returns the router to global configuration mode.
Step 7	**interface** *type number* **Example:** `Router(config)# interface serial 3`	Specifies an interface type and number, and places the router in interface configuration mode.

	Command or Action	Purpose
Step 8	**ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**] **Example:** `Router(config-if)# ipv6 dhcp server dhcp-pool`	Enables DHCPv6 on an interface.
Step 9	**ipv6 nd other-config-flag** **Example:** `Router(config-if)# ipv6 nd other-config-flag`	Sets the “other stateful configuration” flag in IPv6 RAs.

Step 10	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Configuring the Stateless DHCPv6 Client

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address autoconfig** [**default**]
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface serial 3`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**ipv6 address autoconfig** [**default**] **Example:** `Router(config-if)# ipv6 address autoconfig`	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Enabling Processing of Packets with Source Routing Header Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 source-route**
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ipv6 source-route** **Example:** `Router(config)# ipv6 source-route`	Enables the processing of the IPv6 type 0 routing header.

Step 4	**end**
	Example:
	`Router(config)# end`
		Returns to privileged EXEC mode.

Importing Stateless DHCPv6 Server Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import dns-server**
5. **import domain-name**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Router(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.

	Command or Action	Purpose

Step 4	**import dns-server**
	Example:
	`Router(config-dhcp)# import dns-server`
		Imports the DNS recursive name server option to a DHCPv6 client.

Step 5	**import domain-name**
	Example:
	`Router(config-dhcp)# import domain-name`
		Imports the domain search list option to a DHCPv6 client.

Step 6	**end**
	Example:
	`Router(config-dhcp)# end`
		Returns to privileged EXEC mode.

- Configuring the SNTP Server, page 133
- Importing SIP Server Information, page 134
- Importing the SNTP Server, page 135

Configuring the SNTP Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **sntp address** *ipv6-address*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Router(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**sntp address** *ipv6-address* **Example:** `Router(config-dhcp)# sntp address 2001:DB8:2000:2000::33`	Specifies the SNTP server list to be sent to the client.

Step 5	**end**
	Example:
	`Router(config-dhcp)# end`
		Returns to privileged EXEC mode.

Importing SIP Server Information

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import sip address**
5. **import sip domain-name**
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Router(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.

Step 4	**import sip address**
	Example:
	`Router(config-dhcp)# import sip address`
		Imports the SIP server IPv6 address list option to the outbound SIP proxy server.

Step 5	**import sip domain-name**
	Example:
	`Router(config-dhcp)# import sip domain-name`
		Imports a SIP server domain-name list option to the outbound SIP proxy server.

Step 6	**end**
	Example:
	`Router(config-dhcp)# end`
		Returns to privileged EXEC mode.

Importing the SNTP Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import sntp address** *ipv6-address*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Router(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.

Step 4	**import sntp address** *ipv6-address*
	Example:
	`Router(config-dhcp)# import sntp address 2001:DB8:2000:2000::33`
		Imports the SNTP server option to a DHCPv6 client.

Step 5	**end**
	Example:
	`Router(config-dhcp)# end`
		Returns to privileged EXEC mode.

Configuration Examples for IPv6 Access Services: Stateless DHCPv6

Example: Configuring the Stateless DHCPv6 Function

The following example shows how to use the DHCPv6 function to configure clients with information about the name lookup system. The server is configured with a DHCP pool, which contains the name lookup information that is to be passed to clients. It does not need to contain a prefix pool. This DHCP pool is attached to the access link to customers (Ethernet0/0) using the **ipv6 dhcp server** command. The access link also has the **ipv6 nd other-config-flag** command enabled. RA messages sent from this interface will inform clients that they should use DHCPv6 for “other” (for example, nonaddress) configuration information.

```
ipv6 dhcp pool dhcp-pool
 dns-server 2001:DB8:A:B::1
 dns-server 2001:DB8:3000:3000::42
 domain-name example.com
!
interface Ethernet0/0
 description Access link down to customers
 ipv6 address 2001:DB8:1234:42::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server dhcp-pool
```

The client has no obvious DHCPv6 configuration. However, the **ipv6 address autoconfig** command on the uplink to the service provider (Ethernet 0/0) causes the following two events:

- Addresses are autoconfigured on the interface, based on prefixes in RA messages received from the server.
- If received RA messages have the “other configuration” flag set, the interface will attempt to acquire the other (for example, nonaddress) configuration from any DHCPv6 servers.

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Access Services: Stateless DHCPv6

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 11 Feature Information for IPv6 Access Services: Stateless DHCPv6

Feature Name	Releases	Feature Information
IPv6 Access Services: Stateless DHCPv6	12.2(33)SRA 12.2(18)SXE 12.3(4)T 12.4 12.4(2)T	Stateless DHCPv6 allows DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. The following commands were introduced or modified: **dns-server**, **domain-name**, **import dns-server**, **import domain-name**, **import sip address**, **import sip domain-name**, **import sntp address**, **ipv6 address autoconfig**, **ipv6 dhcp pool**, **ipv6 dhcp server**, **ipv6 nd other-config-flag**, **ipv6 source-route**, **sntp address**.

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.

IPv6 Access Services: DHCPv6 Prefix Delegation

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) prefix delegation feature can be used to manage link, subnet, and site addressing changes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 IPv6 Access Services: DHCPv6 Prefix Delegation

DHCPv6 Prefix Delegation

The IPv6 Access Services—DHCPv6 Prefix Delegation feature can be used to manage link, subnet, and site addressing changes. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) can be used in environments to deliver stateful and stateless information. The definitions are given below:

- Stateful prefix delegation—Address assignment is centrally managed and clients must obtain configuration information such as address autoconfiguration and neighbor discovery that is not available through protocols.

- Stateless prefix delegation—Stateless configuration parameters do not require a server to maintain any dynamic state for individual clients, such as Domain Name System (DNS) server addresses and domain search list options.

Extensions to DHCPv6 also enable prefix delegation, through which an ISP can automate the process of assigning prefixes to a customer for use within the customer's network. The prefix delegation occurs between a provider edge (PE) device and customer premises equipment (CPE) using the DHCPv6 prefix delegation option. Once the ISP has delegated prefixes to a customer, the customer may further subnet and assign prefixes to the links in the customer's network.

- Configuring Nodes Without Prefix Delegation, page 142
- Client and Server Identification, page 142
- Rapid Commit, page 142
- DHCPv6 Client, Server, and Relay Functions, page 142

Configuring Nodes Without Prefix Delegation

Stateless DHCPv6 allows DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. The use of stateless DHCPv6 is controlled by router advertisement (RA) messages multicasted by routers. The DHCPv6 client will invoke stateless DHCPv6 when it receives an RA. The DHCPv6 server will respond to a stateless DHCPv6 request with configuration parameters, such as the DNS servers and domain search list options.

Client and Server Identification

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is carried in client identifier and server identifier options. The DUID is unique across all DHCP clients and servers, and it is stable for any specific client or server. DHCPv6 uses DUIDs based on link-layer addresses for both the client and server identifier. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device.

When a DHCPv6 client requests two prefixes with the same DUID but with different identity association identifiers (IAIDs) on two different interfaces, these prefixes are considered to be for two different clients, and the interface information is maintained for both.

Rapid Commit

The DHCPv6 client can obtain configuration parameters from a server either through a rapid two-message exchange (solicit, reply) or through a four-message exchange (solicit, advertise, request, and reply). By default, the four-message exchange is used. When the rapid-commit option is enabled by both the client and the server, the two-message exchange is used.

DHCPv6 Client, Server, and Relay Functions

The DHCPv6 client, server, and relay functions are mutually exclusive on an interface. When one of these functions is enabled and a user tries to configure a different function on the same interface, one of the following messages is displayed: "Interface is in DHCP client mode," "Interface is in DHCP server mode," or "Interface is in DHCP relay mode."

The following sections describe these functions:

- Client Function, page 143
- Server Function, page 143

Client Function

The DHCPv6 client function can be enabled on individual IPv6-enabled interfaces.

The DHCPv6 client can request and accept those configuration parameters that do not require a server to maintain any dynamic state for individual clients, such as DNS server addresses and domain search list options.

The DHCPv6 client can also request the delegation of prefixes. The prefixes acquired from a delegating router will be stored in a local IPv6 general prefix pool. The prefixes in the general prefix pool can then be referred to from other applications; for example, the general prefix pool can be used to number router downstream interfaces.

Server Selection

A DHCPv6 client builds a list of potential servers by sending a solicit message and by collecting advertise message replies from servers. These messages are ranked based on the preference value, and servers may add a preference option to their advertise messages explicitly stating their preference value. If the client needs to acquire prefixes from servers, only servers that have advertised prefixes are considered.

IAPD and IAID

An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting router. A requesting router may have more than one IAPD; for example, one for each of its interfaces.

Each IAPD is identified by an IAID. The IAID is chosen by the requesting router and is unique among the IAPD IAIDs on the requesting router. IAIDs are made consistent across reboots by using information from the associated network interface, which is assumed to be permanently attached to the device.

Server Function

The DHCPv6 server function can be enabled on individual IPv6-enabled interfaces.

The DHCPv6 server can provide configuration parameters that do not require the server to maintain any dynamic state for individual clients, such as DNS server addresses and domain search list options. The DHCPv6 server may be configured to perform prefix delegation.

All the configuration parameters for clients are independently configured into DHCPv6 configuration pools, which are stored in the NVRAM. A configuration pool can be associated with a particular DHCPv6 server on an interface when it is started. Prefixes that are to be delegated to clients may be specified either as a list of preassigned prefixes for a particular client or as IPv6 local prefix pools that are also stored in the NVRAM. The list of manually configured prefixes or IPv6 local prefix pools can be referenced and used by DHCPv6 configuration pools.

The DHCPv6 server maintains an automatic binding table in memory to track the assignment of some configuration parameters, such as prefixes between the server and its clients. Automatic bindings can be stored permanently in the database agent, such as a remote TFTP server or a local NVRAM file system.

Configuration Information Pool

A DHCPv6 configuration information pool is a named entity that includes information about available configuration parameters and policies that the control assignment of the parameters to clients from the pool. A pool is configured independently and is associated with the DHCPv6 service through the CLI.

Each configuration pool can contain the following configuration parameters and operational information:

- Prefix delegation information, which includes:

    - A prefix pool name and associated preferred and valid lifetimes.
    - A list of available prefixes for a particular client and associated preferred and valid lifetimes.
- A list of IPv6 addresses of DNS servers
- A domain search list, which is a string containing domain names for the DNS resolution

DHCP for IPv6 Address Assignment

DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 clients. The DHCPv6 Individual Address Assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple prefix pools. Additional options, such as the default domain and DNS name-server address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

Prefix Assignment

A prefix-delegating router (DHCPv6 server) selects prefixes to be assigned to a requesting router (DHCPv6 client) upon receiving a request from the client. The server can select prefixes for a requesting client by using static and dynamic assignment mechanisms. Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID.

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client’s message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

The Cisco IOS DHCPv6 server can assign prefixes dynamically from an IPv6 local prefix pool. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes from the pool. After the client releases the previously assigned prefixes, the server returns them to the pool for reassignment.

An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute. For more information on this feature, see the Implementing ADSL and Deploying Dial Access for IPv6 module.

Automatic Binding

Each DHCPv6 configuration pool has an associated binding table. The binding table contains records of all prefixes in the configuration pool that have been explicitly delegated to clients. Each entry in the binding table contains the following information:

- Client DUID.
- Client IPv6 address.
- A list of IAPDs associated with the client.
- A list of prefixes delegated to each IAPD.
- Preferred and valid lifetimes for each prefix.
- The configuration pool to which this binding table belongs.
- The network interface on which the server that is using the pool is running.

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, and the entry is updated when the client renews, rebinds, or confirms the prefix delegation. A binding table entry is deleted when the client voluntarily releases all the prefixes in the binding, all prefixes’ valid lifetimes have expired, or administrators run the **clear ipv6 dhcp binding** command.

Binding Database

Each permanent storage to which the binding database is saved is called the database agent. A database agent can be a remote host, such as an FTP server, or a local file system, such as NVRAM.

Automatic bindings are maintained in the RAM and can be saved to some permanent storage so that information about configurations, such as prefixes assigned to clients, is not lost after a system reload. The bindings are stored as text records for easy maintenance. Each record contains the following information:

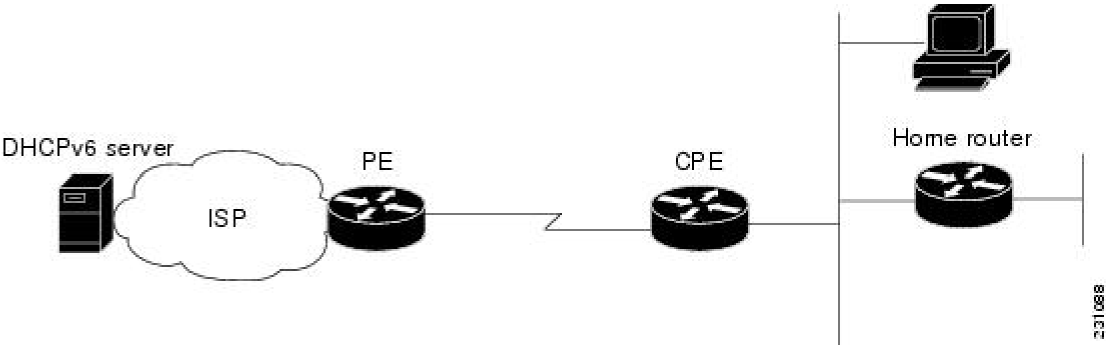
- DHCPv6 pool name from which the configuration was assigned to the client.
- Interface identifier from which the client requests were received.
- The client IPv6 address.
- The client DUID.
- IAID of the IAPD.
- Prefix delegated to the client.
- The prefix length.
- The prefix preferred lifetime in seconds.
- The prefix valid lifetime in seconds.
- The prefix expiration time stamp.
- Optional local prefix pool name from which the prefix was assigned.

DHCPv6 Server Stateless Autoconfiguration

Hierarchical DHCPv6 for stateless configuration parameters allows a stateless or stateful DHCPv6 client to export configuration parameters (DHCPv6 options) to a local DHCPv6 server pool. The local DHCPv6 server can then provide the imported configuration parameters to other DHCPv6 clients.

The figure below shows a typical broadband deployment.

Figure 10 Broadband Topology



The CPE interface towards the PE can be a stateless or stateful DHCPv6 client. In either case, the ISP-side DHCPv6 server may provide configuration parameters such as DNS server addresses, domain names, and Simple Network Time Protocol (SNTP) servers to the DHCP client on the CPE. Such information can be specific to ISPs.

In addition to being a DHCPv6 client (for example, towards the ISP), the CPE may act as a DHCPv6 server to the home network. For example, neighbor discovery followed by a stateless or stateful DHCPv6 client can occur on the link between the CPE and the home devices (such as the home router or PC). In some cases, the information to be provided to the home network is the same as that obtained from the ISP-side DHCPv6 server. Because this information can be dynamically changed, it cannot be hard-configured in the

CPE's configuration. Therefore, the DHCPv6 component on the CPE allows automatic importing of configuration parameters from the DHCPv6 client to the DHCPv6 server pool.

DHCPv6 supports the following options for IPv6 on the server:

Information Refresh Server Option

The DHCPv6 information refresh option can specify a maximum limit for the length of time a client should wait before refreshing the information retrieved from DHCPv6. This option is used with stateless DHCPv6 because there are no addresses or other entities with lifetimes that can tell the client when to contact the DHCPv6 server to refresh its configuration.

NIS- and NIS+-Related Server Options

Users can configure the network information service (NIS) or NIS plus (NIS+) address or domain name of a DHCPv6 server using NIS- and NIS+-related options, and then import that information to the DHCPv6 client.

SIP Server Options

Session Initiation Protocol (SIP) server options contain either a list of domain names or a list of IPv6 addresses that can be mapped to one or more SIP outbound proxy servers. One option carries a list of domain names, and the other option carries a list of 128-bit IPv6 addresses.

SIP is an application-layer control protocol that can establish, modify, and terminate multimedia sessions or calls. A SIP system has several logical components: user agents, proxy servers, redirect servers, and registrars. User agents may contain SIP clients; proxy servers always contain SIP clients.

SNTP Server Option

The SNTP server option provides a list of one or more IPv6 addresses of SNTP servers available to the client for synchronization. Clients use these SNTP servers to synchronize their system time to that of the standard time servers. The DHCPv6 server may list the SNTP servers in decreasing order of preference, but clients treat the list of SNTP servers as an ordered list.

How to Configure IPv6 Access Services: DHCPv6 Prefix Delegation

- Configuring the DHCPv6 Server Function, page 146
- Configuring the DHCPv6 Client Function, page 149
- Deleting Automatic Client Bindings from the DHCPv6 Binding Table, page 151

Configuring the DHCPv6 Server Function

- Configuring the DHCPv6 Configuration Pool, page 146
- Configuring a Binding Database Agent for the Server Function, page 149

Configuring the DHCPv6 Configuration Pool

Perform this task to create and configure the DHCPv6 configuration pool and associate the pool with a server on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **domain-name** *domain*
5. **dns-server** *ipv6-address*
6. **prefix-delegation** *ipv6-prefix* **/** *prefix-length client-duid* [**iaid** *iaid*] [*lifetime*]
7. **prefix-delegation pool** *poolname* [**lifetime** *valid-lifetime preferred-lifetime*]
8. **exit**
9. **interface** *type number*
10. **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**]
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Router(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**domain-name** *domain* **Example:** `Router(config-dhcp)# domain-name example.com`	Configures a domain name for a DHCPv6 client.

	Command or Action	Purpose
Step 5	**dns-server** *ipv6-address* **Example:** `Router(config-dhcp)# dns-server 2001:DB8:3000:3000::42`	Specifies the DNS IPv6 servers available to a DHCPv6 client.
Step 6	**prefix-delegation** *ipv6-prefix* / *prefix-length client-duid* [**iaid** *iaid*] [*lifetime*] **Example:** `Router(config-dhcp)# prefix-delegation 2001:DB8:1263::/48 0005000400F1A4D070D03`	Specifies a manually configured numeric prefix to be delegated to a specified client's IAPD.
Step 7	**prefix-delegation pool** *poolname* [**lifetime** *valid-lifetime preferred-lifetime*] **Example:** `Router(config-dhcp)# prefix-delegation pool pool1 lifetime 1800 60`	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCPv6 clients.
Step 8	**exit** **Example:** `Router(config-dhcp)# exit`	Exits DHCPv6 pool configuration mode, and returns the router to global configuration mode.
Step 9	**interface** *type number* **Example:** `Router(config)# interface serial 3`	Specifies an interface type and number, and enters interface configuration mode.
Step 10	**ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**] **Example:** `Router(config-if)# ipv6 dhcp server pool1`	Enables DHCPv6 on an interface.

Step 11	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Configuring a Binding Database Agent for the Server Function

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp database** *agent* [**write-delay** *seconds*] [**timeout** *seconds*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp database** *agent* [**write-delay** *seconds*] [**timeout** *seconds*] **Example:** `Router(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding`	Specifies DHCPv6 binding database agent parameters.

Step 4	**end**
	Example:
	`Router(config)# end`
		Returns to privileged EXEC mode.

Configuring the DHCPv6 Client Function

General prefixes can be defined dynamically from a prefix received by a DHCPv6 prefix delegation client. The delegated prefix is stored in a general prefix.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**] **Example:** `Router(config-if)# ipv6 dhcp client pd dhcp-prefix`	Enables the DHCPv6 client process and enables a request for prefix delegation through a specified interface.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Returns to privileged EXEC mode.

Deleting Automatic Client Bindings from the DHCPv6 Binding Table

SUMMARY STEPS

1. **enable**
2. **clear ipv6 dhcp binding** [*ipv6-address*] [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 dhcp binding** [*ipv6-address*] [**vrf** *vrf-name*] **Example:** `Router# clear ipv6 dhcp binding`	Deletes automatic client bindings from the DHCPv6 binding table.

Configuration Examples for IPv6 Access Services: DHCPv6 Prefix Delegation

Example: Configuring the DHCPv6 Server Function

DHCPv6 clients are connected to the DHCPv6 server on Ethernet interface 0/0. The server is configured to use parameters from the DHCP pool called dhcp-pool. This pool provides clients with the IPv6 address of a DNS server and the domain name to be used. It also specifies that prefixes can be delegated from the prefix pool called client-prefix-pool1. The prefixes delegated will have valid and preferred lifetimes of 1800 and 600 seconds respectively. The prefix pool named client-prefix-pool1 has a prefix of length /40 from which it will delegate (sub) prefixes of length /48.

```
ipv6 dhcp pool dhcp-pool
 prefix-delegation pool client-prefix-pool1 lifetime 1800 600
 dns-server 2001:DB8:3000:3000::42
 domain-name example.com
!
interface Ethernet0/0
```

```
 description downlink to clients
 ipv6 address FEC0:240:104:2001::139/64
 ipv6 dhcp server dhcp-pool
!
ipv6 local pool client-prefix-pool1 2001:DB8:1200::/40 48
```

The following example from the **show ipv6 dhcp command** shows the DUID of the device:

```
Device# show ipv6 dhcp

This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```

In the following example, the **show ipv6 dhcp binding command** shows information about two clients, including their DUIDs, IAPDs, prefixes, and preferred and valid lifetimes:

```
Device# show ipv6 dhcp binding

Client: FE80::202:FCFF:FEA5:DC39 (Ethernet2/1)
  DUID: 000300010002FCA5DC1C
  IA PD: IA ID 0x00040001, T1 0, T2 0
    Prefix: 3FFE:C00:C18:11::/68
            preferred lifetime 180, valid lifetime 12345
            expires at Nov 08 2002 02:24 PM (12320 seconds)
Client: FE80::202:FCFF:FEA5:C039 (Ethernet2/1)
  DUID: 000300010002FCA5C01C
  IA PD: IA ID 0x00040001, T1 0, T2 0
    Prefix: 3FFE:C00:C18:1::/72
            preferred lifetime 240, valid lifetime 54321
            expires at Nov 09 2002 02:02 AM (54246 seconds)
    Prefix: 3FFE:C00:C18:2::/72
            preferred lifetime 300, valid lifetime 54333
            expires at Nov 09 2002 02:03 AM (54258 seconds)
    Prefix: 3FFE:C00:C18:3::/72
            preferred lifetime 280, valid lifetime 51111
```

In the following example, the **show ipv6 dhcp database** command provides information on the binding database agents TFTP, NVRAM, and flash:

```
Device# show ipv6 dhcp database

Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
     write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
    write timer expires in 50 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2220
  failed write times 614
```

Example: Configuring the DHCPv6 Configuration Pool

In the following example, the **show ipv6 dhcp pool** command provides information on the configuration pool named svr-p1, including the static bindings, prefix information, the DNS server, and the domain names found in the svr-p1 pool:

```
Router# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
  Static bindings:
    Binding for client 000300010002FCA5C01C
      IA PD: IA ID 00040002,
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 604800, valid lifetime 2592000
      IA PD: IA ID not specified; being used by 00040001
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
  Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
  DNS server: 2001:DB8:1001::1
  DNS server: 2001:DB8:1001::2
  Domain name: example1.net
  Domain name: example2.net
  Domain name: example3.net
Active clients: 2
Current configuration : 22324 bytes
!
! Last configuration change at 14:59:38 PST Tue Jan 16 2001
! NVRAM config last updated at 04:25:39 PST Tue Jan 16 2001 by bird
!
hostname Router
!
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 cef accounting prefix-length
!
!
interface Ethernet0
 ip address 10.4.9.11 255.0.0.0
 media-type 10BaseT
 ipv6 address 2001:DB8:C18:1::/64 eui-64
```

Example: Configuring the DHCPv6 Client Function

This DHCPv6 client has three interfaces. Ethernet interface 0/0 is the upstream link to a service provider, which has a DHCPv6 server function enabled. The Fast Ethernet interfaces 0/0 and 0/1 are links to local networks.

The upstream interface, Ethernet interface 0/0, has the DHCPv6 client function enabled. Prefixes delegated by the provider are stored in the general prefix called prefix-from-provider.

The local networks, Fast Ethernet interfaces 0/0 and 0/1, both assign interface addresses based on the general prefix called prefix-from-provider. The bits on the left of the addresses come from the general prefix, and the bits on the right of the addresses are specified statically.

```
interface Ethernet 0/0
 description uplink to provider DHCP IPv6 server
 ipv6 dhcp client pd prefix-from-provider
!
interface FastEthernet 0/0
 description local network 0
 ipv6 address prefix-from-provider ::5:0:0:0:100/64
```

```
!
interface FastEthernet 0/1
 description local network 1
 ipv6 address prefix-from-provider ::6:0:0:0:100/64
```

Example: Configuring a Database Agent for the Server Function

The DHCPv6 server is configured to store table bindings to the file named dhcp-binding on the server at address 10.0.0.1 using the TFTP protocol. The bindings are saved every 120 seconds.

```
ipv6 dhcp database tftp://10.0.0.1/dhcp-binding write-delay 120
```

The following example shows how to specify DHCP for IPv6 binding database agent parameters and store binding entries in bootflash:

```
ipv6 dhcp database bootflash
```

Example: Displaying DHCP Server and Client Information on the Interface

The following is sample output from the **show ipv6 dhcp interface** command. In the first example, the command is used on a router that has an interface acting as a DHCPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCPv6 client:

```
Router1# show ipv6 dhcp interface

Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled

Router2# show ipv6 dhcp interface

Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
      IA PD: IA ID 0x00040001, T1 120, T2 192
        Prefix: 3FFE:C00:C18:1::/72
                preferred lifetime 240, valid lifetime 54321
                expires at Nov 08 2002 09:10 AM (54319 seconds)
        Prefix: 3FFE:C00:C18:2::/72
                preferred lifetime 300, valid lifetime 54333
                expires at Nov 08 2002 09:11 AM (54331 seconds)
        Prefix: 3FFE:C00:C18:3::/72
                preferred lifetime 280, valid lifetime 51111
                expires at Nov 08 2002 08:17 AM (51109 seconds)
      DNS server: 2001:DB8:1001::1
      DNS server: 2001:DB8:1001::2
      Domain name: example1.net
      Domain name: example2.net
      Domain name: example3.net
    Prefix name is cli-p1
    Rapid-Commit is enabled
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Access Services: DHCPv6 Prefix Delegation

Table 12 Feature Information for IPv6 Access Services: DHCPv6 Prefix Delegation

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCPv6 Prefix Delegation	12.0(32)S 12.2(28)SB 12.2(33)SRA 12.2(18)SXE 12.3(4)T 12.4 12.4(2)T 15.0(1)S	The DHCPv6 Prefix Delegation feature can be used to manage link, subnet, and site addressing changes. DHCPv6 can be used in environments to deliver stateful and stateless information. The following commands were introduced or modified: **clear ipv6 dhcp binding**, **dns-server**, **domain-name**, **ipv6 dhcp client pd**, **ipv6 dhcp database**, **ipv6 dhcp pool**, **ipv6 dhcp server**, **prefix-delegation**, **prefix-delegation pool**, **show ipv6 dhcp**, **show ipv6 dhcp binding**, **show ipv6 dhcp interface**, **show ipv6 dhcp pool**.

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.