IP Addressing: DHCP Configuration Guide, Cisco IOS Release 12.2SR

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

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

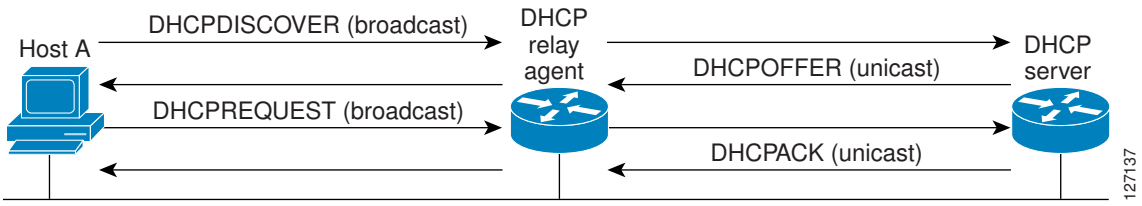
DHCP provides a framework for passing configuration information dynamically to hosts on a TCP/IP network. A DHCP client is an Internet host that uses DHCP to obtain configuration parameters such as an IP address.

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.

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for Configuring the DHCP Server

Before you configure the Cisco IOS 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 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 DHCP Address Allocation Using Option 82 Example, page 51
- Configuring a Static Route with the Next-Hop Dynamically Obtained Through DHCP Example, page 52

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

Pool 0 (Network 172.16.0.0)	Pool 1 (Subnetwork 172.16.1.0)	Pool 2 (Subnetwork 172.16.2.0)			
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
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
!
```

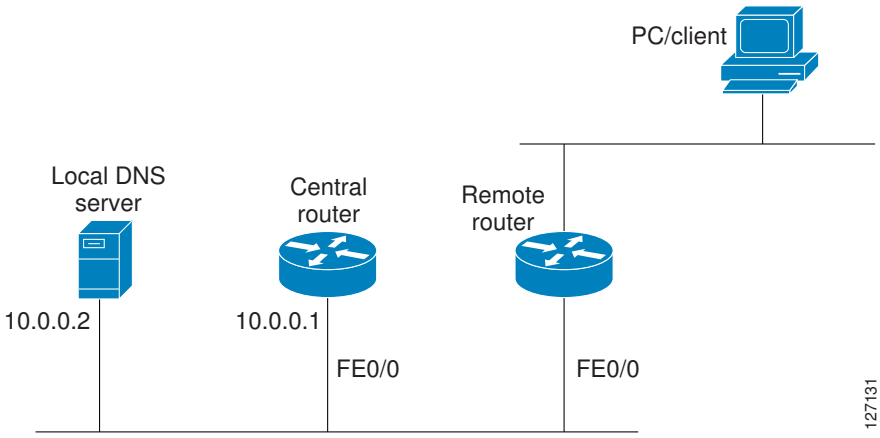
```
ip dhcp pool DEF
   network 10.0.18.0 255.255.255.0
!
ip cef
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
 ip address 10.0.18.68 255.255.255.0
 duplex half
!
interface Ethernet1/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 172.16.1.1
 duplex 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 000000000000000000000FF
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*

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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**.

Feature Name	Releases	Feature Configuration Information
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**.
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**.

DHCP Server MIB

The DHCP Server MIB feature provides Simple Network Management Protocol (SNMP) access to and control of Cisco IOS Dynamic Host Configuration Protocol (DHCP) server software on a Cisco router by an external network management device.

Finding Feature Information

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

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

Prerequisites for the DHCP Server MIB

SNMP must be enabled on the router before DHCP server trap notifications can be configured.

Information About the DHCP Server MIB

SNMP Overview

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that is used for monitoring and managing devices in a network.

SNMP defines two main types of entities: managers and agents. The SNMP manager is a system that controls and monitors the activities of network hosts using SNMP. The agent is the software component within a remote networking device that maintains the data and reports this data, as needed, to the manager. The manager and agent share a Management Information Base (MIB) that defines the information that the agent can make available to the manager.

An important feature of SNMP is the capability to generate unsolicited notifications from an SNMP agent. These trap notifications are messages alerting the SNMP manager to conditions on the network. Traps are considered an agent-to-manager function and a request for confirmation of receipt from the SNMP manager is not required.

DHCP Server Trap Notifications

DHCP server trap notifications are sent to the SNMP manager for the following events:

- Address utilization for a subnet has risen above or fallen below a configurable threshold.
- Address utilization for an address pool has risen above or fallen below a configurable threshold.
- A lease limit violation is detected. The lease limit configuration allows you to control the number of subscribers per interface.
- The DHCP server has started or stopped.
- A duplicate IP address is detected.

The DHCP Server MIB feature does not send the same type of trap notification back-to-back for the same threshold event. For example, if the low threshold value for available free addresses becomes equal to or less than the configured value, a free address low event trap notification on the subnet or pool is generated. This same trap notification will not be resent until the value for the available free addresses has exceeded the value of the free high threshold and vise versa. This threshold control mechanism applies to all trap notifications concerning thresholds in addition to the trap notifications for the DHCP server start and stop time and the lease limit violation. The duplicate IP address trap notification is not subject to this threshold control mechanism.

Tables and Objects in the DHCP Server MIB

The DHCP Server MIB consists of the following tables and objects. The first character of a row in the table begins with “c” (Cisco) and is mapped to the object defined in the IETF draft RFC, *Dynamic Host Configuration Protocol for IPv4 Server MIB.* If the information is not currently available in Cisco IOS software, the value in the second column is displayed as 0 (zero).

- cDhcpv4SrvSystemsObjects (see Table 7)--System description and object IDs
- cBootpHCCounterObjects (see Table 8)--BOOTP counter information
- cDhcpv4HCCounterObjects (see Table 9)--DHCPv4 counter information
- cDhcpv4ServerSharedNetTable (see Table 10)--DHCP address pool information
- cDhcpv4ServerSubnetTable (see Table 11)--Additional DHCP address pool subnet information including secondary subnet information
- cDhcpv4SrvExtSubnetTable (see Table 12)--Additional DHCP address pool subnet information

- cDhcpv4ServerNotifyObjectsGroup (see Table 13)--This objects group is used by the cDhcpv4ServerNotificationsGroup notifications group.
- cDhcpv4ServerNotificationsGroup (see Table 14)--This notifications group consists of all traps defined in the Cisco IOS DHCP server.
- cDhcpv4SrvExtNotifyGroup (see Table 15)--This notifications group consists of all traps not defined in the draft DHCPv4 Server MIB RFC.

Table 7 cDhcpv4SrvSystemsObjects and Descriptions

Name	Description
cDhcpv4SrvSystemDescr	Contains a textual description of the server (full name and version identification).
cDhcpv4SrvSystemObjectID	Cisco experiment node for the DHCP Server MIB. For example, 1.3.6.1.4.1.9.10.102...

Table 8 cBootpHCCounterObjects and Descriptions

Name	Description
cBootpHCCountRequests	The number of packets received that do contain a BOOTREQUEST message type in the first octet.
cBootpHCCountInvalids	0
cBootpHCCountReplies	The number of packets received that contain a BOOTREPLY message type in the first octet.
cBootpHCCountDroppedUnknown Clients	0
cBootpHCCountDroppedNotServingSubnet	0

Table 9 cDhcpv4HCCounterObjects and Descriptions

Name	Description
cDhcpv4HCCountDiscovers	The number of DHCPDISCOVER packets received.
cDhcpv4HCCountOffers	The number of DHCPOFFER packets sent.
cDhcpv4HCCountRequests	The number of DHCPREQUEST packets sent.
cDhcpv4HCCountDeclines	The number of DHCPDECLINE packets sent.
cDhcpv4HCCountAcks	The number of DHCPACK packets sent.
cDhcpv4HCCountNaks	The number of DHCPNACK packets sent.
cDhcpv4HCCountReleases	The number of DHCPRELEASE packets sent.
cDhcpv4HCCountInforms	The number of DHCPINFORM packets sent.

Name	Description
cDhcpv4HCCountForcedRenews	0
cDhcpv4HCCountInvalids	The number of DHCP packets received whose DHCP message type is not understood or handled by the DHCP server.
cDhcpv4HCCountDropUnknownClient	0
cDhcpv4HCCountDropNotServingSubnet	0

Table 10 cDhcpv4ServerSharedNetTable and Descriptions

Name	Description
cDhcpv4ServerSharedNetName	The DHCP address pool name.
cDhcpv4ServerSharedNetFreeAddr LowThreshold	This entry value corresponds to the **utilization mark high** command in DHCP pool configuration mode multiplied by the total pool addresses then divided by 100.
cDhcpv4ServerSharedNetFreeAddrHighThreshold	This entry value corresponds to the **utilization mark low** command in DHCP pool configuration mode multiplied by the total subnet addresses then divided by 100.
cDhcpv4ServerSharedNetFree Addresses	The number of IPv4 addresses that are available within this shared network.
cDhcpv4ServerSharedNetReserved Addresses	The number of IP addresses that are reserved for the pool (not available for assignment). This entry corresponds to the **ip dhcp excluded-address** global configuration command. The value is zero if no excluded addresses are defined for the pool.
cDhcpv4ServerSharedNetTotal Addresses	The number of IP addresses that are available within this shared network.

Table 11 cDhcpv4ServerSubnetTable and Descriptions

Name	Description
cDhcpv4ServerSubnetAddress	The IP address of the subnet entry in the table.
cDhcpv4ServerSubnetMask	The subnet mask of the subnet.
cDhcpv4ServerSubnetSharedNetworkName	The DHCP address pool name to which the subnet belongs.

Name	Description
cDhcpv4ServerSubnetFreeAddrLowThreshold	This entry value corresponds to the **override utilization high** command in DHCP pool secondary subnet configuration mode multiplied by the total subnet addresses then divided by 100.
cDhcpv4ServerSubnetFreeAddrHighThreshold	This entry value corresponds to the **override utilization low** command in DHCP pool secondary subnet configuration mode multiplied by the total subnet addresses then divided by 100.
cDhcpv4ServerSubnetFree Addresses	The number of free IP addresses that are available in the subnet.

Table 12 cDhcpv4SrvExtSubnetTable and Descriptions

Name	Description
cDhcpv4ServerDefaultRouterAddress	The entry corresponds to the **override default-router** command in DHCP pool secondary subnet configuration mode.
cDhcpv4ServerSubnetStartAddress	The first subnet IP address.
cDhcpv4ServerSubnetEndAddress	The last subnet IP address.

Table 13 cDhcpv4ServerNotifyObjectsGroups and Descriptions

Name	Description
cDhcpv4ServerNotifyDuplicateIpAddr	The IP address is found to be a duplicate. Duplicates are detected by servers who send a PING before offering an IP address lease or by a client sending a gratuitous ARP message reported through a DHCPDECLINE message.
cDhcpv4ServerNotifyDuplicateMac	The offending MAC address that caused a duplicate IPv4 address to be detected, if captured by the server, otherwise set to 00-00-00-00-00-00.
cDhcpv4ServerNotifyClientOrServerDetected	This object is set by the server to client if the client used DHCPDECLINE to mark the offered address as in use, or to server if the server discovered that address was in use by a client before offering it.
cDhcpv4ServerNotifyServerStart	The date and time when the server began operation, which is controlled by the **service dhcp** command.
cDhcpv4ServerNotifyServerStop	The date and time when the server ceased operation, which is controlled by **no service dhcp** command.

Table 14 cDhcpv4ServerNotificationsGroup and Descriptions

Name	Description
cDhcpv4ServerFreeAddressLow	This notification signifies that the number of available IP addresses for a DHCP address pool has fallen below the defined low threshold. This notification corresponds to the **snmp-server enable traps dhcp** global configuration command.
cDhcpv4ServerFreeAddressHigh	This notification signifies that the number of available IP addresses for a DHCP address pool has risen above the defined high threshold. This notification corresponds to the **snmp-server enable traps dhcp** global configuration command.
cDhcpv4ServerStartTime	This notification signifies that the server has started. This notification corresponds to the **service dhcp** and **snmp-server enable traps dhcp time**global configuration commands.
cDhcpv4ServerStopTime	This notification signifies that the server has stopped normally. This notification corresponds to the **no service dhcp** and **snmp-server enable traps dhcp time**global configuration commands.
cDhcpv4ServerDuplicateAddress	This notification signifies that a duplicate IP address has been detected. This notification corresponds to the **snmp-server enable traps dhcp duplicate**global configuration command.

Table 15 cDhcpv4SrvNotifyGroup and Descriptions

Name (not in the RFC draft)	Description
cDhcpv4ServerIfLeaseLimitExceeded	This notification signifies that a per interface lease limit is exceeded. This notification corresponds to the **snmp-server enable traps dhcp interface**global configuration command.
cDhcpv4ServerSubnetFreeAddressLow	This notification signifies that the number of available IP addresses for a subnet has fallen below the defined low threshold. This notification corresponds to the **snmp-server enable traps dhcp subnet**global configuration command.
cDhcpv4ServerSubnetFreeAddressHigh	This notification signifies that the number of available IPv4 addresses for a subnet has risen above the defined high threshold. This notification corresponds to the **snmp-server enable traps dhcp subnet**global configuration command.

How to Enable DHCP Trap Notifications

Configuring the Router to Send SNMP Trap Notifications About DHCP

DHCP trap notifications are disabled by default. The trap notification is disabled if the corresponding trap configuration is not enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps dhcp duplicate**] [**interface**] [**pool**] [**subnet**] [**time**
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	**snmp-server enable traps dhcp duplicate**] [**interface**] [**pool**] [**subnet**] [**time** **Example:** `Router(config)# snmp-server enable traps dhcp`	Enables the sending of DHCP SNMP trap notifications. • **duplicate** --Sends notification about duplicate IP addresses. • **interface** --Sends notification that a per interface lease limit is exceeded. • **pool** --Sends notification when address utilization for an address pool has risen above or fallen below a configurable threshold. • **subnet** --Sends notification when address utilization for a subnet has risen above or fallen below a configurable threshold. • **time** --Sends notification that the DHCP server has started or stopped. • If you specify the **snmp-server enables traps dhcp** command without any of the optional keywords, all DHCP trap notifications are enabled.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Returns the router to privileged EXEC mode.

- Troubleshooting Tips, page 64

Troubleshooting Tips

You can troubleshoot DHCP server SNMP events by using the **debug ip dhcp server snmp** privileged EXEC command.

Configuration Examples for the DHCP Server MIB

DHCP Server MIB--Secondary Subnet Trap Example

The following example configures 192.0.2.0/24 as the subnetwork number and mask of the DHCP pool named pool2 and then adds the DHCP pool secondary subnet specified by the subnet number and mask 192.0.4.0/30. The IP addresses in pool2 consist of two disjoint subnets: the addresses from 192.0.2.1 to 192.0.2.254 and the addresses from 192.0.4.1 to 192.0.4.2.

The address pool utilization mark, configured at the global level, will be overridden at the secondary subnet level. A trap is sent to the SNMP manager if the subnet size of the secondary subnet exceeds or goes below the level specified by the **override utilization** commands.

The **utilization mark**{**high**| **low**}**log** command enables a system message to be generated for a DHCP address pool or secondary subnet when the utilization exceeds the configured high utilization threshold or falls below the configured low utilization threshold.

```
!
ip dhcp pool pool2
 utilization mark high 80 log
 utilization mark low 70 log
 network 192.0.2.0 255.255.255.0
 network 192.0.4.0 255.255.255.252 secondary
 override utilization high 40
 override utilization low 30
!
snmp-server enable traps dhcp subnet
```

DHCP Server MIB--Address Pool Trap Example

In the following example, if the address utilization exceeds the high threshold or drops below the low threshold, an SNMP trap will be sent to the SNMP manager and a system message will be generated.

```
ip dhcp pool pool3
 utilization mark high 80 log
 utilization mark low 70 log
!
snmp-server enable traps dhcp pool
```

DHCP Server MIB--Lease Limit Violation Trap Example

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

```
ip dhcp limit lease log
interface Serial 0/0
 ip dhcp limit lease 4
 exit
snmp-server enable traps dhcp interface
```

Additional References

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

Related Documents

Related Topic	Document Title
SNMP configuration tasks	“Configuring SNMP Support” module
DHCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP server configuration tasks including subnet utilization tasks	“Configuring the Cisco IOS DHCP Server” module
DHCP per interface lease limit functionality	“Configuring DHCP Services for Accounting and Security” module
DHCP ODAP tasks including address pool utilization tasks	“Configuring the DHCP Server On-Demand Address Pool Manager” module

Standards

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

MIBs

MIB	MIBs Link
• CISCO-IETF-DHCP-SERVER-MIB • CISCO-IETF-DHCP-SERVER-EXT-MIB	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

RFC	Title
Draft RFC: draft-ietf-dhc-server-mib-10.txt	Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Server MIB

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 MIB

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 16 Feature Information for DHCP Server MIB

Feature Name	Releases	Feature Information
DHCP Server MIB	12.2(33)SRC	The DHCP Server MIB feature provides SNMP access to and control of Cisco IOS DHCP server software on a Cisco router by an external network management device. The following commands were introduced by this feature: **snmp-server enable traps dhcp**and **debug ip dhcp server snmp**.

Configuring the DHCP Server On-Demand Address Pool Manager

The Cisco IOS Dynamic Host Configuration Protocol (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. A DHCP pool configured in the router can also be used as an IP address pooling mechanism. The IP address pooling mechanism is configured in the router to specify the source of IP addresses for PPP peers.

Finding Feature Information

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

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

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

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

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

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

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

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

Information About the DHCP Server On-Demand Address Pool Manager

ODAP Manager Operation

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

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

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

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

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

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

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

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

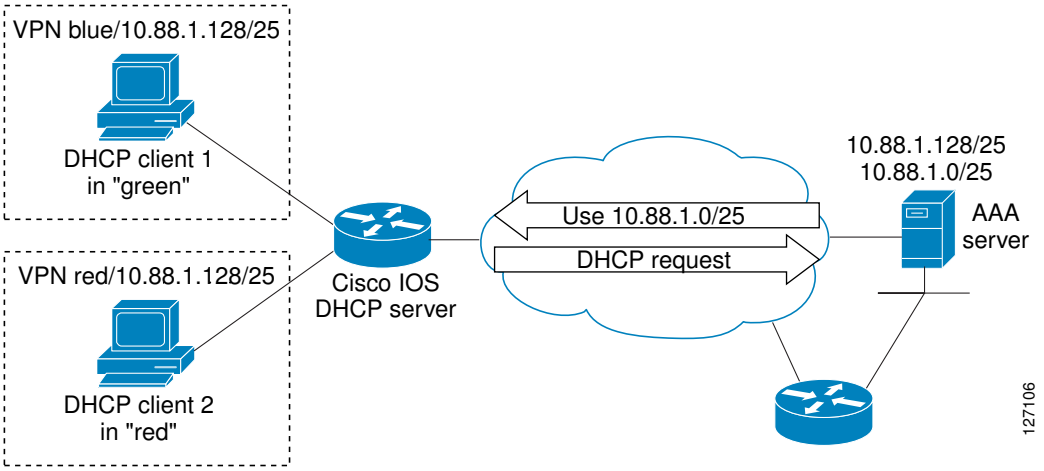
When a DHCP pool receives multiple subnets from an upstream DHCP server, an address from each subnet is automatically configured on the client connected interface so that the addresses within the subnets can be requested by DHCP clients.

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

The figure below shows an ODAP manager configured on the Cisco IOS DHCP server. The ODAP requests an initial pool from the AAA server. Clients make DHCP requests and the DHCP server fulfills requests from the pool. When the utilization rate meets 90 percent, the ODAP manager requests an

expansion and the AAA server allocates another subnet from which the ODAP manager can allocate addresses.

Figure 3 ODAP Address Pool Management for MPLS VPNs



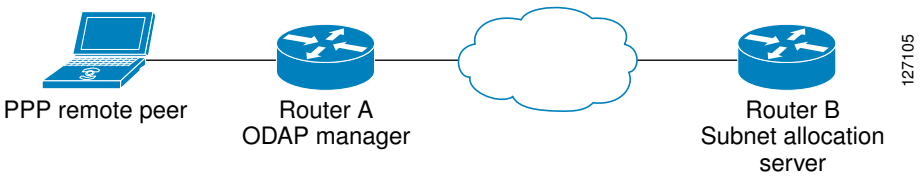
Subnet Allocation Server Operation

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

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

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

Figure 4 Subnet Allocation Server Topology



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

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

Benefits of Using ODAPs

Efficient Address Management

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

Efficient Route Summarization and Update

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

Multiple VRF and Independent Private Addressing Support

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

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

Specifying DHCP ODAPs as the Global Default Mechanism

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 address-pool dhcp-pool** **Example:** `Router(config)# ip address-pool dhcp-pool`	Specifies on-demand address pooling as the global default IP address mechanism. • For remote access (PPP) sessions into MPLS VPNs, IP addresses are obtained from locally configured VRF-associated DHCP pools. **Note** You must use two separate DHCP address pools for global configuration mode and VRF mode. If you change a global configuration pool to VRF mode, then all the IP addresses in the global pool will be lost. Hence make sure that you have a VRF pool for an interface in order to add an interface under a VRF.

Defining DHCP ODAPs on an Interface

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 Virtual-Template 1`	Specifies the interface and enters interface configuration mode.
Step 4	**peer default ip address dhcp-pool** [*pool-name*] **Example:** `Router(config)# peer default ip address dhcp-pool mypool`	Specifies an IP address from an on-demand address pool to be returned to a remote peer connecting to this interface. • The *pool-name* argument supports non-MPLS VPNs and is mandatory if the session is not associated with any VRF. Multiple pool names can be accepted but must be separated by blank spaces.

Configuring the DHCP Pool as an ODAP

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 4	**vrf** *name* **Example:** `Router(dhcp-config)# vrf vrf1`	(Optional) Associates the address pool with a VRF name. • Only use this command for MPLS VPNs.
Step 5	**origin** {**dhcp** | **aaa** | **ipcp**} [**subnet size initial** *size* [**autogrow** *size*]] **Example:** `Router(dhcp-config)# origin dhcp subnet size initial /16 autogrow /16`	Configures an address pool as an on-demand address pool. • If you do not configure the pool as an autogrow pool, the pool will not request additional subnets if one subnet is already in the pool. • You can enter size as either the subnet mask (*nnnn.nnnn.nnnn.nnnn*) or prefix size (/*nn*). The valid values are /0 and /4 to /30. • When a DHCP pool receives multiple subnets from an upstream DHCP server, an address from each subnet is automatically configured on the client connected interface so that the addresses within the subnets can be requested by DHCP clients. The first address in the first subnet is automatically assigned to the primary address on the interface. The first address of each subsequent subnet is assigned to secondary addresses on the interface. In addition, as client addresses are reclaimed, the count of lease addresses for that subnet is decremented. Once a lease counter for a subnet reaches zero (that is, lease expiry), the subnet is returned to the pool. The previous address on the interface is removed and the first secondary address on the interface is promoted as the primary address of the interface. • If the **origin aaa** option is configured, AAA must be configured.

	Command or Action	Purpose
Step 6	**utilization mark low** *percentage-number* **Example:** `Router(dhcp-config)# utilization mark low 40`	Sets the low utilization mark of the pool size. • This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured. • The default value is 0 percent.
Step 7	**utilization mark high** *percentage-number* **Example:** `Router(dhcp-config)# utilization mark high 60`	Sets the high utilization mark of the pool size. • This command cannot be used unless the **autogrow** *size* option of the **origin** command is configured. • The default value is 100 percent.
Step 8	**end** **Example:** `Router(dhcp-config)# end`	Returns to previleged EXEC mode.
Step 9	**show ip dhcp pool** [*pool-name*] **Example:** `Router# show ip dhcp pool`	(Optional) Displays information about DHCP address pools. • Information about the primary and secondary interface address assignment is also displayed.

Configuring ODAPs to Obtain Subnets Through IPCP Negotiation

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 red-pool`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 4	**import all** **Example:** `Router(dhcp-config)# import all`	Imports option parameters into the Cisco IOS DHCP server database.
Step 5	**origin ipcp** **Example:** `Router(dhcp-config)# origin ipcp`	Configures an address pool as an on-demand address pool using IPCP as the subnet allocation protocol.

	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 ethernet 0`	Specifies the interface and enters interface configuration mode.
Step 8	**ip address pool** *pool-name* **Example:** `Router(config-if)# ip address pool red-pool`	Specifies that the interface IP address will be automatically configured from the named pool, when the pool is populated with a subnet from IPCP.

Configuring AAA

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization configuration default group radius**
5. **aaa accounting network default start-stop group radius**
6. **aaa session-id common**

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	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables AAA access control.
Step 4	**aaa authorization configuration default group radius** **Example:** `Router(config)# aaa authorization configuration default group radius`	Downloads static route configuration information from the AAA server using RADIUS.

	Command or Action	Purpose

Step 5	**aaa accounting network default start-stop group radius**
	
	Example:
	or
	
	Example:
	aaa accounting network default stop-only group radius
	
	Example:
	`Router(config)# aaa accounting network default start-stop group radius`
	
	Example:
	or
	
	Example:
	
	Example:
	`Router(config)# aaa accounting network default stop-only group radius`
		Enables AAA accounting of requested services for billing or security purposes when you use RADIUS, and sends a "start" accounting notice at the beginning of a process.
		or
		Enables AAA accounting of requested services for billing or security purposes when you use RADIUS, and sends a "stop" accounting notice at the end of the requested user process.

Step 6	**aaa session-id common** **Example:** `Router(config)# aaa session-id common`	Ensures that the same session ID will be used for each AAA accounting service type within a call.

Configuring RADIUS

ODAP AAA Profile

The AAA server sends the RADIUS Cisco attribute value (AV) pair attributes "pool-addr" and "pool-mask" to the Cisco IOS DHCP server in the access request and access accept. The pool-addr attribute is the

IP address and the pool-mask attribute is the network mask (for example,pool-addr=192.168.1.0 and pool-mask=255.255.0.0). Together, these attributes comprise a network address (address/mask) that is allocated by the AAA server to the Cisco IOS DHCP server.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 radius source-interface** *subinterface-name*
	
	Example:
	`Router(config)#`
	`ip radius source-interface Ethernet1/1`
		Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

Step 4	**radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number*
	
	Example:
	`Router(config)#`
	`radius-server host 172.16.1.1 auth-port 1645 acct-port 1646`
		Specifies a RADIUS server host.
		• The *ip-address* argument specifies the IP address of the RADIUS server host.

	Command or Action	Purpose

Step 5	**radius server attribute 32 include-in-access-req**
	
	Example:
	`Router(config)#`
	`radius server attribute 32 include-in-access-req`
		Sends RADIUS attribute 32 (NAS-Identifier) in an access request or accounting request.

Step 6	**radius server attribute 44 include-in-access-req**
	
	Example:
	`Router(config)#`
	`radius server attribute 44 include-in-access-req`
		Sends RADIUS attribute 44 (Accounting Session ID) in an access request or accounting request.

Step 7	**radius-server vsa send accounting**
	
	Example:
	`Router(config)#`
	`radius-server vsa send accounting`
		Configures the network access server (NAS) to recognize and use vendor-specific accounting attributes.

Step 8	**radius-server vsa send authentication**
	
	Example:
	`Router(config)#`
	`radius-server vsa send authentication`
		Configures the NAS to recognize and use vendor-specific authentication attributes.

Disabling ODAPs

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
Step 4	**no origin** {**dhcp** | **aaa** | **ipcp**} **Example:** `Router(dhcp-config)# no origin dhcp`	Disables the ODAP.

Verifying ODAP Operation

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

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

Example:

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

Step 2 **show ip dhcp binding** The following output shows the bindings from pool Green. The Type field shows On-demand, which indicates that the address binding was created for a PPP session. The Lease expiration field shows Infinite, which means that the binding is valid as long as the session is up. If a subnet must be released back to the leasing server while the session is still up, the session is reset so that it will be forced to obtain a new IP address. The Hardware address column for an On-demand entry shows the identifier for the session as detected by PPP. No bindings are shown under the Bindings from all pools not associated with VRF field because the Global pool has not allocated any addresses.

Example:

```
Router# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address       Hardware address        Lease expiration        Type
Bindings from VRF pool Green:
```

```
IP address       Hardware address        Lease expiration        Type
172.16.0.1       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3930.39
172.16.0.2       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3839.31
172.16.0.3       5674.312d.7465.7374.    Infinite                On-demand
                 2d36.3432.34
172.16.0.4       5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3236.34
172.16.0.5       5674.312d.7465.7374.    Infinite                On-demand
                 2d34.3331.37
172.16.0.6       5674.312d.7465.7374.    Infinite                On-demand
                 2d37.3237.39
172.16.0.9       5674.312d.7465.7374.    Infinite                On-demand
                 2d39.3732.36
172.16.0.10      5674.312d.7465.7374.    Infinite                On-demand
                 2d31.3637
172.16.0.11      5674.312d.7465.7374.    Infinite                On-demand
                 2d39.3137.36
172.16.0.12      5674.312d.7465.7374.    Infinite                On-demand
                 2d37.3838.30
172.16.0.13      5674.312d.7465.7374.    Infinite                On-demand
                 2d32.3339.37
172.16.0.14      5674.312d.7465.7374.    Infinite                On-demand
                 2d31.3038.31
172.16.0.17      5674.312d.7465.7374.    Infinite                On-demand
                 2d38.3832.38
172.16.0.18      5674.312d.7465.7374.    Infinite                On-demand
                 2d32.3735.31
```

- Troubleshooting Tips, page 86

Troubleshooting Tips

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

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

Monitoring and Maintaining the ODAP

This task shows how to monitor and maintain the ODAP. These commands need not be entered in any specific order.

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip dhcp** [**pool** *pool-name*] **binding** {*****	*address*}	Clears an automatic address binding or objects from a specific pool from the DHCP server database. **Example:** `Router# clear ip dhcp binding *`
Step 3	**clear ip dhcp** [**pool** *pool-name*] **conflict** {*****	*address*}	Clears an address conflict or conflicts from a specific pool from the DHCP server database. **Example:** `Router# clear ip dhcp conflict *`

	Command or Action	Purpose
Step 4	**clear ip dhcp** [**pool** *pool-name*] **subnet** {***** | *address*} **Example:** `Router# clear ip dhcp subnet *`	Clears all currently leased subnets in the named DHCP pool or all DHCP pools if *pool-name* is not specified.
Step 5	**debug dhcp details** **Example:** `Router# debug dhcp details`	Monitors the subnet allocation/releasing in the on-demand address pools.
Step 6	**debug ip dhcp server events** **Example:** `Router# debug ip dhcp server events`	Reports DHCP server events, such as address assignments and database updates.
Step 7	**show ip dhcp import** **Example:** `Router# show ip dhcp import`	Displays the option parameters that were imported into the DHCP server database.
Step 8	**show ip interface** [*type number*] **Example:** `Router# show ip interface`	Displays the usability status of interfaces configured for IP.
Step 9	**show ip dhcp pool** *pool-name* **Example:** `Router# show ip dhcp pool green`	Displays DHCP address pool information.

Configuring DHCP ODAP Subnet Allocation Server Support

Configuring a Global Subnet Pool on a Subnet Allocation Server

Global Subnet Pools

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 GLOBAL-POOL`	Enters DHCP pool configuration mode and specifies the subnet pool name.

	Command or Action	Purpose
Step 4	**network** *network-number* [*mask*| / *prefix-length*] **Example:** `Router(dhcp-config)# network 10.0.0.0 255.255.255.0`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server. • The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length* argument.
Step 5	**subnet prefix-length** *prefix-length* **Example:** `Router(dhcp-config)# subnet prefix-length 8`	Configures the subnet prefix length. The range of the *prefix-length* argument is from 1 to 31. • This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation format.

Configuring a VRF Subnet Pool on a Subnet Allocation Server

VRF Subnet Pools

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 VRF-POOL`	Enters DHCP pool configuration mode and specifies the subnet pool name.
Step 4	**vrf** *vrf-name* **Example:** `Router(dhcp-config)# vrf vrf1`	Associates the on-demand address pool with a VRF instance name (or tag). • The **vrf**command and *vrf-name* argument are used to specify the VPN for the VRF pool. The *vrf-name*argument must match the VRF name (or tag) that is configured for the client.
Step 5	**network** *network-number* [*mask* | */ prefix-length*] **Example:** `Router(dhcp-config)# network 10.1.1.0 /24`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server. • The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length* argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length*argument.
Step 6	**subnet prefix-length** *prefix-length* **Example:** `Router(dhcp-config)# subnet prefix-length 16`	Configures the subnet prefix length. • The range of the *prefix-length*argument is from 1 to 31. • This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation format.

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

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

• VRF Pools and VPN IDs, page 92

VRF Pools and VPN IDs

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 vrf** *vrf-name* **Example:** `Router(config)# ip vrf vrf1`	Creates a VRF routing table and specifies the VRF name (or tag). • The *vrf-name* argument must match the VRF name that is configured for the client and VRF pool in Step 9.

	Command or Action	Purpose
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 100:1`	Creates routing and forwarding tables for a VRF instance created in Step 3. • There are two formats for configuring the route distinguisher argument. It can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn).
Step 5	**route-target both** *route-target-number* **Example:** `Router(config-vrf)# route-target both 100:1`	Creates a route-target extended community for the VRF instance that was created in Step 3. • The **both**keyword is used to specify which routes should be imported and exported to the target VPN extended community (or the ODAP manager in this configuration). • The *route-target-number*argument follows the same format as the *route-distinguisher*argument in Step 4. These two arguments must match.
Step 6	**vpn id** *vpn-id* **Example:** `Router(config-vrf)# vpn id 1234:123456`	Configures the VPN ID. • This command is used only if the client (ODAP manager) is also configured with or assigned a VPN ID.
Step 7	**exit** **Example:** `Router(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 8	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool VPN-POOL`	Enters DHCP pool configuration mode and specifies the subnet pool name. • The **vrf**keyword and *vrf-name*argument are used to specify the VPN for the VRF pool. The *vrf-name*argument must match the VRF name (or tag) that is configured for the client.
Step 9	**vrf** *vrf-name* **Example:** `Router(dhcp-config)#vrf RED`	Associates the on-demand address pool with a VRF instance name. • The *vrf-name* argument must match the *vrf-name*argument that was configured in Step 3.

	Command or Action	Purpose
Step 10	**network** *network-number* [*mask*|/*prefix-length*] **Example:** `Router(dhcp-config)# network 192.168.0.0 /24`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server. • The subnet mask or the prefix length can be configured in this step. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation. The forward slash character must be used when configuring the *prefix-length*argument.
Step 11	**subnet prefix-length** *prefix-length* **Example:** `Router(dhcp-config)# subnet prefix-length 16`	Configures the subnet prefix length. • The range of the *prefix-length* argument is from 1 to 31. • This command configures the number of IP addresses that each subnet is configured to allocate from the subnet pool. The values that can be configured for the *prefix-length*argument follow CIDR bit count notation format.

Verifying Subnet Allocation and DHCP Bindings

Perform this task to verify subnet allocation and DHCP bindings. The **show**commands need not be entered in any specific order.

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**show running-config** | **begin dhcp** **Example:** `Router# show running-config | begin dhcp`	Displays the local configuration of the router. • The configuration of the **subnet prefix-length** command will be displayed under the DHCP pools, for which subnet lease allocation has been configured. The subnet allocation size will be shown, following this command, in CIDR bit count notation. • The sample output is filtered with the **begin** keyword to start displaying output at the DHCP section of the running configuration.
Step 3	**show ip dhcp pool** [*pool-name*] **Example:** `Router# show ip dhcp pool`	Displays information about DHCP pools. • This command can be used to verify subnet allocation pool configuration on both the subnet allocation server and the ODAP manager. • The output of this command displays specific address pool information, including the name of the pool, utilization of address space, subnet size, number of total addresses, number of leased address, and pending events.
Step 4	**show ip dhcp binding** [*ip-address*] **Example:** `Router# show ip dhcp binding`	Displays information about DHCP bindings. • This command can be used to display subnet allocation to DHCP binding mapping information. • The output from this command displays binding information for individual IP address assignment and allocated subnets. The output that is generated for DHCP IP address assignment and subnet allocation is almost identical, except that subnet leases display an IP address followed by the subnet mask (which shows the size of the allocated subnet). Bindings for individual IP address display only an IP address and are not followed by a subnet mask.

Troubleshooting the DHCP ODAP Subnet Allocation Server

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuration Examples for DHCP Server On-Demand Address Pool Manager

Specifying DHCP ODAPs as the Global Default Mechanism Example

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

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

Defining DHCP ODAPs on an Interface Example

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

```
interface Virtual-Template 1
 ip vrf forwarding green
 ip unnumbered loopback1
 ppp authentication chap
 peer default ip address dhcp-pool
!
```

Configuring the DHCP Pool as an ODAP Example

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

```
Router# show running-config
Building configuration...
Current configuration : 3943 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
no logging console
enable password password
!
username vpn_green_net1 password 0 lab
username vpn_red_net1 password 0 lab
ip subnet-zero
!
ip dhcp pool green_pool
   vrf Green
   utilization mark high 60
   utilization mark low 40
   origin dhcp subnet size initial /24 autogrow /24
!
ip dhcp pool red_pool
   vrf Red
   origin dhcp
!
ip vrf Green
 rd 200:1
 route-target export 200:1
 route-target import 200:1
!
ip vrf Red
 rd 300:1
 route-target export 300:1
 route-target import 300:1
ip cef
ip address-pool dhcp-pool
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface Loopback0
 ip address 192.0.2.1 255.255.255.255
!
interface Loopback1
 ip vrf forwarding Green
 ip address 192.0.2.2 255.255.255.255
!
```

```
interface Loopback2
 ip vrf forwarding Red
 ip address 192.0.2.3 255.255.255.255
!
interface ATM2/0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface ATM3/0
 no ip address
 no atm ilmi-keepalive
!
interface Ethernet4/0
 ip address 192.0.2.4 255.255.255.224
 duplex half
!
interface Ethernet4/1
 ip address 192.0.2.5 255.255.255.0
 duplex half
!
interface Ethernet4/2
 ip address 192.0.2.6 255.255.255.0
 duplex half
 tag-switching ip
!
interface Virtual-Template1
 ip vrf forwarding Green
 ip unnumbered Loopback1
 ppp authentication chap
!
interface Virtual-Template2
 ip vrf forwarding Green
 ip unnumbered Loopback1
 ppp authentication chap
!
interface Virtual-Template3
 ip vrf forwarding Green
 ip unnumbered Loopback1
 ppp authentication chap
!
interface Virtual-Template4
 ip vrf forwarding Red
 ip unnumbered Loopback2
 ppp authentication chap
!
interface Virtual-Template5
 ip vrf forwarding Red
 ip unnumbered Loopback2
 ppp authentication chap
!
interface Virtual-Template6
 ip vrf forwarding Red
 ip unnumbered Loopback2
 ppp authentication chap
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 209.165.200.225 255.255.255.224 area 0
 network 209.165.200.226 255.255.255.224 area 0
 network 209.165.200.227 255.255.255.224 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.0.2.1 remote-as 100
 neighbor 192.0.2.2 update-source Loopback0
 !
 address-family ipv4 vrf Red
 redistribute connected
 redistribute static
 no auto-summary
```

```
 no synchronization
 network 110.0.0.0
 exit-address-family
 !
 address-family ipv4 vrf Green
 redistribute connected
 redistribute static
 no auto-summary
 no synchronization
 network 100.0.0.0
 exit-address-family
 !
 address-family vpnv4
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
 exit-address-family
!
ip classless
ip route 172.19.0.0 255.255.0.0 10.0.105.1
no ip http server
ip pim bidir-enable
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password password
 login
!
end
```

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

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

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

IPCP Subnet Mask Delivery Example

The following example shows a Cisco 827 router configured to use IPCP subnet masks:

```
Router# show running-config
 Building configuration...

 Current configuration :1479 bytes
 !
 version 12.2
 no service single-slot-reload-enable
 no service pad
 service timestamps debug datetime msec
 service timestamps log uptime
 no service password-encryption
 !
 hostname Router
 !
 no logging buffered
 logging rate-limit console 10 except errors
 !
 username 6400-nrp2 password 0 lab
 ip subnet-zero
 ip dhcp smart-relay
 !
 ip dhcp pool IPPOOLTEST
    import all
    origin ipcp
 !
 no ip dhcp-client network-discovery
 !
 interface Ethernet0
  ip address pool IPPOOLTEST
  ip verify unicast reverse-path
  hold-queue 32 in
 !
 interface ATM0
  no ip address
  atm ilmi-keepalive
  bundle-enable
  dsl operating-mode auto
  hold-queue 224 in
 !
 interface ATM0.1 point-to-point
  pvc 1/40
   no ilmi manage
   encapsulation aal5mux ppp dialer
   dialer pool-member 1
  !
 !
 interface Dialer0
  ip unnumbered Ethernet0
  ip verify unicast reverse-path
  encapsulation ppp
  dialer pool 1
  dialer-group 1
  no cdp enable
  ppp authentication chap callin
  ppp chap hostname Router
  ppp chap password 7 12150415
  ppp ipcp accept-address
  ppp ipcp dns request
  ppp ipcp wins request
  ppp ipcp mask request
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 Dialer0
 no ip http server
 !
 dialer-list 1 protocol ip permit
```

```
 line con 0
  exec-timeout 0 0
  transport input none
  stopbits 1
 line vty 0 4
  login
 !
 scheduler max-task-time 5000
 end
```

Configuring AAA and RADIUS Example

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

```
!
aaa new-model
!
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa session-id common
!
ip subnet-zero
!
ip dhcp ping packets 0
!
ip dhcp pool Green
   vrf Green
   utilization mark high 50
   utilization mark low 30
   origin aaa subnet size initial /28 autogrow /28
!
ip vrf Green
 rd 300:1
 route-target export 300:1
 route-target import 300:1
!
interface Ethernet1/1
 ip address 172.16.1.12 255.255.255.0
 duplex half
!
interface Virtual-Template1
 ip vrf forwarding Green
 no ip address
!
ip radius source-interface Ethernet1/1
!
!IP address of the RADIUS server host
radius-server host 172.16.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 32 include-in-access-req
radius-server attribute 44 include-in-access-req
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuring a Global Pool on a Subnet Allocation Server Example

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

```
ip dhcp pool GLOBAL-POOL
 network 10.0.0.0 255.255.255.0
```

```
 subnet prefix-length 24
!
```

Configuring a VRF Pool on a Subnet Allocation Server Example

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

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

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

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

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

Verifying Local Configuration on a Subnet Allocation Server Example

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

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

Verifying Address Pool Allocation Information Example

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

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

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

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

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

Verifying Subnet Allocation and DHCP Bindings Example

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

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.0/26         0063.6973.636f.2d64.    Mar 29 2003 04:36 AM    Automatic
                    656d.6574.6572.2d47.
                    4c4f.4241.4c
```

Additional References

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

Related Documents

Related Topic	Document Title
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP conceptual information	"DHCP Overview" module
DHCP server configuration	"Configuring the Cisco IOS DHCP Server" module
DHCP client configuration	"Configuring the Cisco IOS DHCP Client" 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 configuration	"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.	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 951	*Bootstrap Protocol (BOOTP)*
RFC 1542	*Clarifications and Extensions for the Bootstrap Protocol*
RFC 2131	*Dynamic Host Configuration Protocol*

RFCs	Title
RFC 2685	*Virtual Private Networks Identifier*
RFC 3046	*DHCP Relay Information Option*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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 Server On-Demand Address Pool Manager

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

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

Table 17 Feature Information for the DHCP On-Demand Address Pool Manager

Feature Name	Releases	Feature Configuration Information
DHCP Server On-Demand Address Pool Manager for Non-MPLS VPNs	12.2(15)T 12.2(28)SB 12.2(33)SRC	This feature was enhanced to provide ODAP support for non-MPLS VPNs. The following command was modified by this feature: **peer default ip address**.

Feature Name	Releases	Feature Configuration Information
DHCP ODAP Server Support	12.2(15)T 12.2(28)SB 12.2(33)SRC	This feature introduces the capability to configure a DHCP server (or router) as a subnet allocation server. This capability allows the Cisco IOS DHCP server to be configured with a pool of subnets for lease to ODAP clients. The following commands were introduced or modified by this feature: **show ip dhcp binding**, **subnet prefix-length**.
DHCP Server On-Demand Address Pool Manager	12.2(8)T 12.28(SB) 12.2(33)SRC	The ODAP manager is used to centralize the management of large pools of addresses and simplify the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses. When a Cisco IOS router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level. The following commands were introduced or modified: **aaa session-id**, **clear ip dhcp binding**, **clear ip dhcp conflict**, **clear ip dhcp subnet**, **ip address-pool**, **ip address pool**, **ip dhcp aaa default username**, **origin**, **peer default ip address**, **show ip dhcp pool**, **utilization mark high**, **utilization mark low**, **vrf**.

Glossary

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

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

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

DHCP --Dynamic Host Configuration Protocol.

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

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

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

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

ODAP --on-demand address pool.

PE router --provider edge router.

PPP --Point-to-Point Protocol.

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

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

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

server --DHCP or BOOTP server.

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

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

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

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

DHCP Server RADIUS Proxy

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

Finding Feature Information

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

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

Prerequisites for DHCP Server RADIUS Proxy

Before you can configure the DHCP Server RADIUS Proxy feature, you must be running DHCPv4 or a later version. For information about release and platform support, see the Feature Information for DHCP Server RADIUS Proxy, page 128.

Restrictions for DHCP Server RADIUS Proxy

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

Information About DHCP Server RADIUS Proxy

DHCP Server RADIUS Proxy Overview

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

The process of authorizing the client using the RADIUS server is as follows:

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

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

DHCP Server RADIUS Proxy Enhancement

The DHCP Server RADIUS Proxy Enhancement feature is an enhancement to the DHCP Server RADIUS Proxy feature introduced in Cisco IOS Release 15.0(1)S. This feature supports DHCP options 60 and 121.

The process of authorizing the client using the RADIUS server is as follows:

1. The DHCP server passes client information to a RADIUS server.
2. The RADIUS server returns classname information and other optional information (Session-Timeout and Session-Duration) to the DHCP server as RADIUS attributes.
3. The DHCP server assigns the IP address from the specified class, if it is available, and translates any other optional attributes received from the RADIUS server into DHCP options. The information is sent to the DHCP client as a DHCP OFFER message.
4. DHCP binding is synchronized after the RADIUS server authorizes the client session.

DHCP Server RADIUS Proxy Architecture

The allocation of addresses in a DHCP and RADIUS proxy architecture occurs in the following sequence:

1. The client accesses the network from a residential gateway and sends a DHCP DISCOVER broadcast message to the relay agent. The DHCP DISCOVER message contains the client IP address, hostname, vendor class identifier, and client identifier.
2. The relay agent sends a DHCP DISCOVER unicast message with the following information to the router:

- Relay agent information (option 82) with the remote ID suboption containing the inner and outer VLAN IDs.
- Client information in the DHCP DISCOVER packet.

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

1. RADIUS receives an access-request message to translate the DHCP options to RADIUS attributes.
2. RADIUS responds with an access-accept message, and delivers the following attributes to the DHCP server:
   - Framed-IP-Address
   - Framed-IP-Netmask
   - Session-Timeout
   - Session-Duration
3. The DHCP server sends an OFFER unicast message with the following translations from the RADIUS server access-accept message to the client:
   - Framed-IP-Address inserted into the DHCP header.
   - Framed-IP-Netmask inserted into DHCP option 1 (subnet mask).
   - Session-Timeout inserted into DHCP option 51 (IP address lease time).
   - Framed-Route that is translated from the standard Cisco Framed-Route format into DHCP option 121 or the DHCP default gateway option (if the network and netmask are appropriate for a default route).
   - A copy of relay agent information (option 82). Before the DHCP client receives the packet, the relay removes option 82.
   - T1 time set to the Session-Timeout and T2 time set to the Session-Duration.
4. The client returns a formal request for the offered IP address to the DHCP server in a DHCP REQUEST broadcast message.
5. The DHCP confirms that the IP address is allocated to the client by returning a DHCP ACK unicast message containing the lease information and the DHCP options to the client.
6. A RADIUS server accounting request starts, followed by a RADIUS server accounting response that is used by the authentication, authorization, and accounting (AAA) subsystem.

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

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

DHCP Server RADIUS Proxy Enhancement Architecture

The allocation of addresses in a DHCP and RADIUS proxy enhancement architecture occurs in the following sequence:

1. The client accesses the network from a residential gateway and sends a DHCP DISCOVER broadcast message to the relay agent. The DHCP DISCOVER message contains the client IP address, hostname, vendor class identifier, and client identifier.

2 The relay agent sends a DHCP DISCOVER unicast message with the following information to the router:

   - Relay agent information (option 82) with the remote ID suboption containing the inner and outer VLAN IDs.
   - Client information in the DHCP DISCOVER packet.

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

1 The RADIUS server receives an access-request message to translate the DHCP options to RADIUS attributes.
2 The RADIUS server responds with an access-accept message and delivers the following attributes to the DHCP server:

   - Classname
   - Session-Timeout (optional)
   - Session-Duration (optional)

3 The DHCP server identifies the addresses configured under the specified classname and assigns an address to the client.
4 The DHCP server sends an OFFER unicast message containing the following translations from the RADIUS server access-accept message to the client:

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

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

Note If the classname attribute is not present in the access-accept message received, the DHCP server assumes a default classname and tries to assign the IP address from a default class. The IP address is assigned to the client only if the IP address is available for a default class.

- If the Framed-IP-Address, Framed-IP-Netmask, Session-Timeout, and Session-Duration attributes are present in the access-accept message, then the classname attribute is ignored and the DHCP server assigns the IP address received in the Framed-IP-Address attribute to the client.

DHCP Server and RADIUS Translations

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

Table 18 DCHP DISCOVER to RADIUS Access-Request Translations

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

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

Table 19 RADIUS Access-Accept to DHCP OFFER Translations

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

RADIUS Profiles for the DHCP Server RADIUS Proxy

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

- The Session-Timeout attribute must contain a value, in seconds. If this attribute is not present, the DHCP OFFER is not sent to the client.

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

RADIUS Profiles for the DHCP Server RADIUS Proxy Enhancement

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

- The Session-Timeout attribute (if present) must contain a value, in seconds.
- A RADIUS user profile may contain the following attributes:
  - Classname (default classname is considered, if this attribute is not present)
  - Framed-Route
  - Session-Timeout
  - Session-Duration--Session-Duration is the Cisco AV pair session-duration = seconds, where “seconds” is the maximum time for the duration of a lease including all renewals. The value for Session-Duration should be greater than or equal to the Session-Timeout attribute value, and it cannot be zero.
- Additional RADIUS server attributes are allowed but are not required. The DHCP server ignores additional attributes that it does not understand.

How to Configure DHCP Server RADIUS Proxy

Configuring AAA-Related Commands for DHCP Server RADIUS Proxy

Perform this task to configure AAA-related commands required to configure the DHCP Server RADIUS Proxy and DHCP Server RADIUS Proxy Enhancement features.

SUMMARY STEPS

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

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	**service dhcp** **Example:** `Router(config)# service dhcp`	Enables DHCP server and relay agent features on the router. • By default, these features are enabled on the router.

	Command or Action	Purpose
Step 4	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control system.
Step 5	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius group1`	Specifies the name of the server host list to group RADIUS server hosts, and enters server-group configuration mode. • *group-name* --Character string to name the server group. The following words cannot be used as the group name: ◦ auth-guest ◦ enable ◦ guest ◦ if-authenticated ◦ if-needed ◦ krb5 ◦ krb-instance ◦ krb-telnet ◦ line ◦ local ◦ none ◦ radius ◦ rcmd ◦ tacacs ◦ tacacsplus
Step 6	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config-sg-radius)# server 10.1.1.1 auth-port 1700 acct-port 1701`	Specifies the IP address of the RADIUS server host for the defined server group. • Repeat this command for each RADIUS server host to associate with the server group. ◦ *ip-address*- —IP address of the RADIUS server host. ◦ **auth-port** *port-number*- —(Optional) Specifies the UDP destination port for authentication requests. Default value is 1645. ◦ **acct-port** *port-number* —(Optional) Specifies the UDP destination port for accounting requests. Default value is 1646.
Step 7	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server-group configuration mode.

	Command or Action	Purpose
Step 8	**aaa authorization network** *method-list-name* **group** *group-name* **Example:** `Router(config)# aaa authorization network auth1 group group1`	Specifies the methods list and server group for DHCP authorization. • *method-list-name* --Character string to name the authorization methods list. • **group** --Specifies a server group. • *group-name* --Name of the server group to apply to DHCP authorization.
Step 9	**aaa accounting network** *method-list-name* **start-stop group** *group-name* **Example:** `Router(config)# aaa accounting network acct1 start-stop group group1`	Specifies that AAA accounting runs for all network service requests. • *method-list-name* --Character string to name the accounting methods list. • **start-stop** --Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice is received by the accounting server. • **group** --Specifies a server group. • *group-name* --Name of the server group to apply to DHCP accounting.
Step 10	**interface** *type slot* / *subslot* / *port* [**.** *subinterface*] **Example:** `Router(config)# interface ethernet 1/10/0.0`	Configures an interface or subinterface that allows the DHCP client to obtain an IP address from the DHCP server, and enters subinterface configuration mode.
Step 11	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* [**,** *vlan-id* [**-** *vlan-id*]]} **Example:** `Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`	(Optional) Enables IEEE 802.1Q encapsulation of traffic on a subinterface in a VLAN. • *vlan-id* --VLAN ID, integer in the range 1 to 4094. To separate the starting and ending VLAN ID values that are used to define a range of VLAN IDs, enter a hyphen. (Optional) To separate each VLAN ID range from the next range, enter a comma. • **second-dot1q** --Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature to configure an inner VLAN ID. • **any** --Any second tag in the range 1 to 4094.
Step 12	**ip address** *address mask* **Example:** `Router(config-subif)# ip address 192.168.1.1 255.255.255.0`	Specifies an IP address for an interface or subinterface. • *address* is the IP address of the interface or subinterface. • *mask* is the subnet address for the IP address.

	Command or Action	Purpose
Step 13	**no shutdown** **Example:** `Router(config-subif)# no shutdown`	Enables the interface or subinterface.
Step 14	**exit** **Example:** `Router(config-subif)#` **exit**	Exits subinterface configuration mode and enters global configuration mode.
Step 15	**radius-server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config)# radius-server host 10.1.1.1`	Specifies a RADIUS server host. • *ip-address* is the IP address of the RADIUS server host. • **auth-port** *port-number*-- (Optional) Specifies the UDP destination port for authentication requests. Default value is 1645. • **acct-port** *port-number*-- (Optional) Specifies the UDP destination port for accounting requests. Default value is 1646.
Step 16	**radius-server key** {**0** *string* | **7** *string* | *string*} **Example:** `Router(config)#` **radius-server key string1**	Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon. • **0** *string*-- Specifies an unencrypted (cleartext) shared key • **7** *string* -- Specifies a hidden shared key. **Note** Any key you enter must match the key on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 17	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring the DHCP Server for RADIUS Proxy Authorization

Perform this task to configure the DHCP Server for RADIUS Proxy feature.

Configure the AAA configuration before configuring the DHCP Server for RADIUS Proxy feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp use class** [**aaa**]
4. **ip dhcp pool** *name*
5. **accounting** *method-list-name*
6. **authorization method** *method-list-name*
7. **authorization shared-password** *password*
8. **authorization username** *string*
9. **exit**

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** [**aaa**] **Example:** `Router(config)# ip dhcp use class aaa`	Configures the DHCP server to use the AAA server to get the class name.
Step 4	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool pool1`	Specifies a name for the DHCP server address pool, and enters DHCP pool configuration mode. • *name* --Name of the pool.
Step 5	**accounting** *method-list-name* **Example:** `Router(dhcp-config)# accounting acct1`	Enables DHCP accounting. • *method-list-name* --Name of the accounting methods list.

	Command or Action	Purpose
Step 6	**authorization method** *method-list-name* **Example:** `Router(dhcp-config)# authorization method auth1`	Enables DHCP authorization. • *method-list-name* --Name of the authorization methods list.
Step 7	**authorization shared-password** *password* **Example:** `Router(dhcp-config)#` **authorization shared-password password1**	Specifies the password that is configured in the RADIUS user profile.

	Command or Action	Purpose
Step 8	**authorization username** *string* **Example:** `Router(dhcp-config)#` **authorization username %c-user1**	Specifies the parameters that RADIUS sends to a DHCP server when downloading configuration information for a DHCP client. • The *string* argument contains the following formatting characters to insert DHCP client information: ◦ **%%**--Transmits the percent sign (%) character in the string sent to the RADIUS server ◦ **%c**--Ethernet address of the DHCP client (chaddr field) in ASCII format ◦ **%C**--Ethernet address of the DHCP client in hexadecimal format ◦ **%g**--Gateway address of the DHCP relay agent (giaddr field) ◦ **%i**--Inner VLAN ID from the DHCP relay information (option 82) in ASCII format ◦ **%I**--Inner VLAN ID from the DHCP relay information in hexadecimal format ◦ **%o**--Outer VLAN ID from the DHCP relay information (option 82) in ASCII format ◦ **%O**--Outer VLAN ID from the DHCP relay information (option 82) in hexadecimal format ◦ **%p**--Port number from the DHCP relay information (option 82) in ASCII format ◦ **%P**--Port number from the DHCP relay information (option 82) in hexadecimal format ◦ **%u**--Circuit ID from the DHCP relay information in ASCII format ◦ **%U**--Circuit ID from the DHCP relay information in hexadecimal format ◦ **%r**--Remote ID from the DHCP relay information in ASCII format ◦ **%R**--Remote ID from the DHCP relay information in hexadecimal format **Note** The percent (%) sign is a marker to insert the DHCP client information associated with the specified character. The % is not sent to the RADIUS server unless you specify the %% characters.
Step 9	**exit** **Example:** `Router(dhcp-config)# exit`	Exits DHCP pool configuration mode.

Configuring the DHCP Server Proxy Enhancement

Perform this task to configure the DHCP Server Proxy Enhancement feature.

Configure the AAA configuration before configuring the DHCP Server for RADIUS Proxy feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp use class aaa**
4. **ip dhcp pool** *name*
5. **accounting** *server-group-name*
6. **authorization method** *method-list-name*
7. **authorization shared-password** *password*
8. **authorization username** *username*
9. **exit**
10. **ip dhcp pool** *name*
11. **network** *network-number* [*mask* [**secondary**] | **/** *prefix-length* [**secondary**]]
12. **class** *class-name*
13. **address range** *start-ip end-ip*

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 aaa** **Example:** `Router(config)# ip dhcp use class aaa`	Specifies to use the AAA server to get class name.
Step 4	**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.

	Command or Action	Purpose
Step 5	**accounting** *server-group-name* **Example:** `Router(dhcp-config)# accounting list1`	Enables DHCP accounting on a server group.
Step 6	**authorization method** *method-list-name* **Example:** `Router(dhcp-config)# authorization method list1`	Specifies a method list to be used for address allocation using RADIUS for DHCP.
Step 7	**authorization shared-password** *password* **Example:** `Router(dhcp-config)# authorization shared-password password1`	Specifies the password that RADIUS sends to a DHCP or RADIUS server when downloading configuration information for a DHCP client.
Step 8	**authorization username** *username* **Example:** `Router(dhcp-config)# authorization username user1`	Specifies the parameters that RADIUS sends to a DHCP server when downloading configuration information for a DHCP client.
Step 9	**exit** **Example:** `Router(dhcp-config)# exit`	Exits DHCP pool configuration mode and returns to global configuration mode.
Step 10	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool name2`	Configures a DHCP address pool on a DHCP server and enters DHCP pool configuration mode.
Step 11	**network** *network-number* [*mask* [**secondary**] | / *prefix-length* [**secondary**]] **Example:** `Router(config)# network 10.0.0.1 255.255.255.0`	Configures the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco IOS DHCP server.

	Command or Action	Purpose
Step 12	**class** *class-name* **Example:** `Router(config)# class name1`	Associates a class with a DHCP address pool and enters DHCP pool class configuration mode.
Step 13	**address range** *start-ip end-ip* **Example:** `Router(config-dhcp-pool-class)# address range 10.0.0.1 10.0.0.5`	Sets an address range for a DHCP class in a DHCP server address pool.

Monitoring and Maintaining the DHCP Server

Perform this task to verify and monitor DHCP server information. Once the router is in privileged EXEC mode, you can enter the commands in any order.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip dhcp server packet** **Example:** `Router# debug ip dhcp server packet`	(Optional) Enables DHCP server debugging.

	Command or Action	Purpose
Step 3	**debug ip dhcp server events** **Example:** `Router#` **debug ip dhcp server events**	(Optional) Reports DHCP server events, such as address assignments and database updates.
Step 4	**show ip dhcp binding** [*address*] **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 5	**show ip dhcp server statistics** **Example:** `Router# show ip dhcp server statistics`	(Optional) Displays count information about server statistics and messages sent and received.
Step 6	**show ip dhcp pool** [*name*] **Example:** `Router#` **show ip dhcp pool**	(Optional) Displays the routes added to the routing table by the DHCP server and relay agent.
Step 7	**show ip route dhcp** [*address*] **Example:** `Router#` **show ip route dhcp [address]**	(Optional) Displays information about DHCP address pools.

Configuration Examples for DHCP Server Radius Proxy

Example Configuring the DHCP Server for RADIUS Proxy

The following example shows how to configure a DHCP server for RADIUS-based authorization of DHCP leases. In this example, DHCP clients can attach to Ethernet interface 4/0/1 and Ethernet subinterface

4/0/3.10. The username string (%c-user1) specifies that the RADIUS server sends the Ethernet address of DHCP client named user1 to the DHCP server.

```
Router> enable
Router# configure terminal
Router(config)# service dhcp
Router(config)# aaa new-model
Router(config)# aaa group server radius rad1
Router(config-sg)# server 10.1.1.1
Router(config-sg)# server 10.1.5.10
Router(config-sg)# exit

Router(config)# aaa authorization network auth1 group group1
Router(config)# aaa accounting network acct1 start-stop group group1
Router(config)# aaa session-id common
Router(config)# ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100 timeout 5
!
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# accounting acct1
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password cisco
Router(config-dhcp)# authorization username %c-user1
Router(config-dhcp)# exit
!
Router(config)# interface ethernet 4/0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
Router(config-if)# interface ethernet 4/0/3.10

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

Example Configuring RADIUS Profiles for RADIUS Proxy

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

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

Example Configuring the DHCP Server for RADIUS Proxy Enhancement

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

```
Router> enable
Router# configure terminal
Router(config)# service dhcp
Router(config)# aaa new-model
Router(config)# aaa group server radius rad1
Router(config-sg)# server 10.1.1.1
Router(config-sg)# server 10.1.5.10
Router(config-sg)# exit
Router(config)# aaa authorization network auth1 group group1
```

```
Router(config)# aaa accounting network acct1 start-stop group group1
Router(config)# aaa session-id commo
n
Router(config)# ip dhcp database tftp://172.0.2.1/router-dhcp write-delay 100 timeout 5
!
Router(config)# ip dhcp pool pool_common
Router(config-dhcp)# accounting acct1
Router(config-dhcp)# authorization method auth1
Router(config-dhcp)# authorization shared-password password1
Router(config-dhcp)# authorization username %c-user1
Router(config-dhcp)# exit
!
Router(config)# ip dhcp pool pool_subnet
Router(config-dhcp)# network 10.3.4.0 255.255.255.0
Router(config-dhcp)# class class-1
Router(config-dhcp)# address range 10.3.4.1 10.3.4.10
Router(config-dhcp)# exit
!
Router(config)# interface ethernet 4/0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
Router(config-if)# interface ethernet 4/0/3.10
Router(config-if)# encapsulation dot1q 100 second-dot1q 200
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# radius-server host 10.1.3.2
Router(config)# radius-server key cisco
Router(config)# exit
```

Example Configuring RADIUS Profiles for RADIUS Proxy Enhancement

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

```
DHCP-00059A3C7800 Password = “password”
Service-Type = Framed,
Classname = "class-1"
Framed-Route = "0.0.0.0 0.0.0.0 10.3.4.1",
Session-Timeout = 3600,
Cisco:Cisco-Avpair = "session-duration=7200”
```

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

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 RADIUS Proxy

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

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

Table 20 Feature Information for Cisco IOS DHCP Server Radius Proxy

Feature Name	Releases	Feature Information
DHCP Server RADIUS Proxy	12.2(31)ZV1 12.2(34)SB 12.2(33)XNE 15.0(1)S	The DHCP Server RADIUS Proxy feature enables a server to authorize remote clients and allocate addresses based on replies from the server. The following commands were modified by this feature: **authorization method** (DHCP), **authorization shared-password , authorization username** (DHCP).
DHCP Radius Proxy Enhancement	15.0(1)S	The DHCP Radius Proxy Enhancement feature provides an option to configure the DHCP server to accept either the class name or an IP address to assign to the client. The following commands were introduced or modified: **accounting** (DHCP), **address range**, **authorization method** (DHCP), **authorization shared-password**, **authorization username** (DHCP), **class** (DHCP), **network** (DHCP).

Glossary

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

DHCP --Dynamic Host Configuration Protocol.

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

MPLS --Multiprotocol Label Switching.

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

server --DHCP or BOOTP server.

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

VRF --VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that

defines a customer VPN site that is attached to a PE router. Each VPN instantiated on the PE router has its own VRF.

Configuring the Cisco IOS DHCP Relay Agent

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

Finding Feature Information

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

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

Prerequisites for Configuring the 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 if they have been disabled by checking your configuration file. If they have been disabled, the **no service dhcp** command will appear in the configuration file. Use the **service dhcp** command to reenable the functionality if necessary.

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

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

How to Configure the DHCP Relay Agent

Specifying the Packet Forwarding Address

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

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 normally forwarded because most routers are configured to not forward broadcast traffic. Also, when the DHCP client broadcasts a

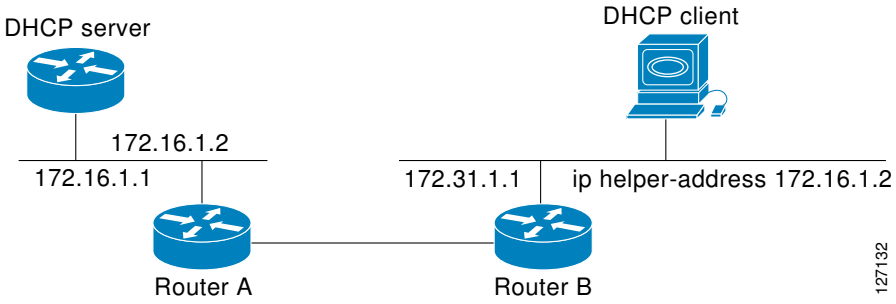
DHCPDISCOVER message, the relay agent sends the broadcast messages toward the client. The Address Resolution Protocol (ARP) entries are created due to an unnecessary ARP check performed by the client after receiving the ACK message. If there are two entries in the ARP table, one gets timed out after 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 is acting as a DHCP relay agent. The Cisco router implementation of the DHCP relay agent is provided via the **ip helper-address** interface configuration command.

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

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



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**

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 FastEthernet0/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip helper-address** *address* **Example:** `Router(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. Using the network address enables other servers to respond to DHCP requests. • If you have multiple servers, you can configure one helper address for each server.
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and enters global configuration mode.
Step 6	**ip dhcp relay prefer known-good-server** **Example:** `Router(config)# ip dhcp relay prefer known-good-server`	(Optional) Reduces the frequency with which the DHCP clients change their address and forwards client requests to the server that handled the previous request. • The DHCP relay deletes the ARP entries for addresses offered to the DHCP client on the unnumbered interfaces.

Configuring Relay Agent Information Option Support

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

Automatic DHCP address allocation is typically based on an IP address, whether it be the gateway IP address (giaddr field of the DHCP packet) or the incoming interface IP address. In some networks, it is

necessary to use additional information to further determine which IP addresses to allocate. By using the relay agent information option (option 82), the Cisco IOS relay agent can include additional information about itself when forwarding client-originated DHCP packets to a DHCP server.

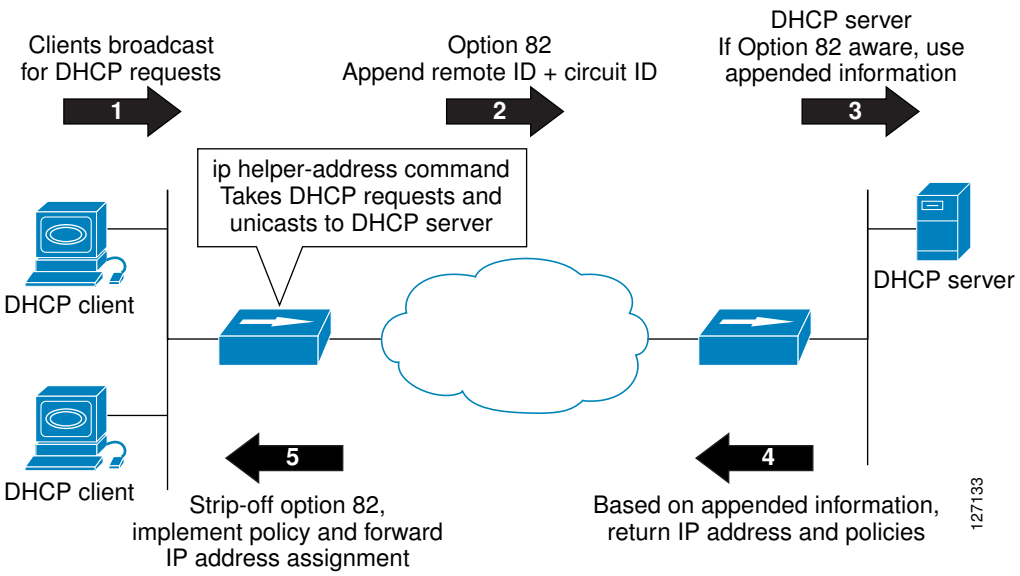
Cisco IOS supports this functionality by using the **ip dhcp relay information option** command. The relay agent will automatically add the circuit identifier suboption and the remote ID suboption to the relay agent information option and forward them to the DHCP server.

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

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

Figure 6 Relay Agent Information Option Operation



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

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

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:** `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 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 **ip dhcp relay information check** **Example:** `Router(config)# ip dhcp relay information check`	(Optional) Configures DHCP to check that the relay agent information option in forwarded BOOTREPLY messages is valid. • By default, DHCP checks that the option-82 field in DHCP reply packets it receives from the DHCP server is valid. If an invalid message is received, the relay agent drops it. If a valid message is received, the relay agent removes the option-82 field and forwards the packet. Use the **ip dhcp relay information check** command to reenable this functionality if it has been disabled.
Step 5 **ip dhcp relay information policy** {**drop**| **keep**| **replace**} **Example:** `Router(config)# ip dhcp relay information policy replace`	(Optional) Configures the reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information).
Step 6 **ip dhcp relay information trust-all** **Example:** `Router(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 in between the client and the relay agent that may insert option 82. Use this command to ensure that these packets do not get dropped. • 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:** `Router(config)# end`	Returns to privileged EXEC mode.

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

Configuring Relay Agent Information Option Support per Interface

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

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

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.

>

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:** `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 FastEthernet0/0`	Configures an interface and enters interface configuration mode.
Step 4	**ip dhcp relay information option-insert** [**none**] **Example:** `Router(config-if)# ip dhcp relay information option-insert`	Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server. • This function is disabled by default. However, if support for the relay agent information option is configured in global configuration mode, but not in interface configuration mode, the interface inherits the global configuration. • 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:** `Router(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 checks that the option-82 field in DHCP reply packets it receives from the DHCP server is valid. If an invalid message is received, the relay agent drops it. If a valid message is received, the relay agent removes the option-82 field and forwards the packet. Use the **ip dhcp relay information check-reply** command to reenable this functionality if it has been disabled. • 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:** `Router(config-if)# ip dhcp relay information policy-action replace`	Configures the information reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains relay information).
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 8	Repeat Steps 3 through 7 to configure relay agent information settings on different interfaces.	(Optional)

Configuring the Subscriber Identifier Suboption of the Relay Agent Information Option

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

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

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

You should configure the unique identifier for each subscriber.

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

The server should be able to recognize the new suboption.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 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:** `Router(config)# interface atm4/0.1`	Configures an interface and enters interface configuration mode.
Step 5	**ip dhcp relay information option subscriber-id** *string* **Example:** `Router(config-if)# ip dhcp relay information option subscriber-id newsubscriber123`	Specifies that a DHCP relay agent add a subscriber identifier suboption to the relay information option. • The *string* argument can be up to a maximum of 50 characters and can be alphanumeric. **Note** If more than 50 characters are configured, the string is truncated. **Note** The **ip dhcp relay information option subscriber-id**command is disabled by default to ensure backward capability.

Configuring DHCP Relay Class Support for Client Identification

Perform this task to configure DHCP relay class support for client identification.

DHCP relay class support for client identification allows the Cisco IOS 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 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 the 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 (H323 and 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 H323 devices must be forwarded to the H323 server and requests from the 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 that 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, then 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 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 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 SIP`	Defines a DHCP class and enters DHCP class configuration mode.
Step 4	**option** *code* **hex** *hex-pattern* [*****][**mask** *bit-mask-pattern*] **Example:** `Router(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:** `Router(dhcp-class)# exit`	Exits DHCP class configuration mode.
Step 6	Repeat Steps 3 through 5 for each DHCP class you need to configure.	--
Step 7	**ip dhcp pool** *name* **Example:** `Router(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:** `Router(dhcp-config)# relay source 10.2.0.0 255.0.0.0`	Configures the relay source. The *ip-address* and *subnet-mask* arguments are the IP address and subnet mask for 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 matches the relay source configuration.
Step 9	**class** *class-name* **Example:** `Router(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:** `Router(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:** `Router(dhcp-class)# exit`	Exits DHCP pool class configuration mode.
Step 12	Repeat Steps 9 through 11 for each DHCP class you need to configure.	--

Configuring DHCP Relay Agent Support for MPLS VPNs

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

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

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

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

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

- VPN identifier
- Subnet selection
- Server identifier override

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

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

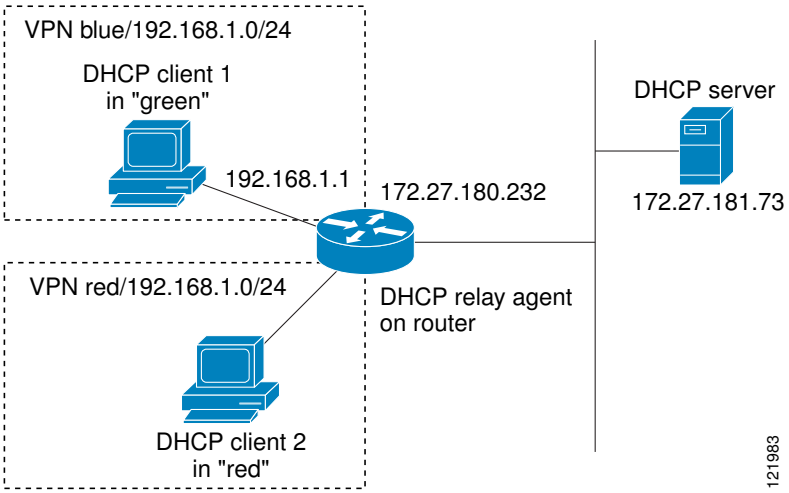
The server identifier override suboption value is copied in the reply packet from the DHCP server instead of the normal server ID address. The server identifier override suboption contains the incoming interface IP address, which is the IP address on the relay agent that is accessible from the client.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

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

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

identifier override suboptions of the relay agent information option to distinguish the correct VPN of the client.

Figure 7 Virtual Private Network DHCP Configuration



Before configuring DHCP relay support for 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**interfaceconfigurationcommand 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 configurationcommand 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 configurationcommand is not configured and the **ip dhcp relay information option vpn-id**interface configurationcommand is configured, only the interface with the configuration option applied is affected. All other interfaces are not impacted by the configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **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**]

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 relay information option vpn** **Example:** `Router(config)# ip dhcp relay information option vpn`	Enables the system to insert VPN suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server and sets the gateway address to the outgoing interface toward the DHCP server. • The VPN suboptions are also added to the BOOTP broadcast packets when the command is configured.
Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernet0/0`	Configures an interface and enters interface configuration mode.
Step 5	**ip helper-address vrf** *name* [**global**] *address* **Example:** `Router(config-if)# ip helper-address vrf blue 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, then the **vrf** *name* or **global** options allow you to specify the name of the VRF or global space in which the DHCP server resides.

	Command or Action	Purpose
Step 6	**ip dhcp relay information option vpn-id** [**none**] **Example:** `Router(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.

Configuring Relay Agent Information Option Encapsulation Support

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

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

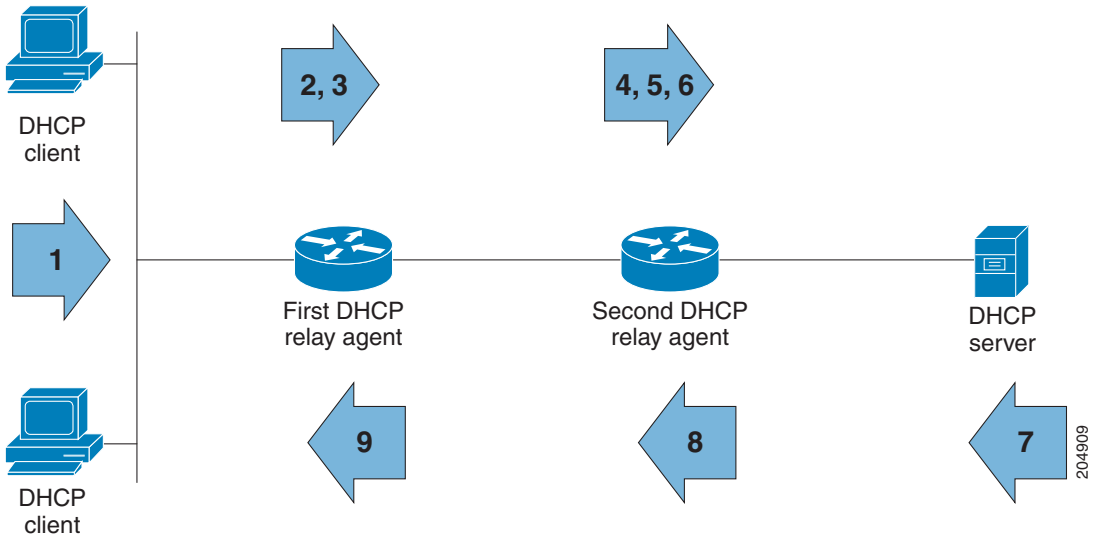
The DHCP Relay Option 82 Encapsulation feature allows the second relay agent to encapsulate option 82 information in a received message from the first relay agent if it is also configured to add its own option 82 information. This configuration allows the DHCP server to use option 82 information from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

The diagram 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, along with the option 82 information from the first relay agent, to assign IP addresses and other configuration parameters and forwards the packet back to the second relay agent.
8 When the second relay agent receives the reply message from the server, it restores the encapsulated option 82 and prior giaddr from the first relay agent. The reply message is then sent to the prior giaddr.
9 The option 82 is stripped off of the packet by the first relay agent before forwarding to the client.

Figure 8 DHCP Relay Agent Information Option Encapsulation Support Processing



SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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	**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	**ip dhcp relay information option vpn** **Example:** `Router(config)# ip dhcp relay information option vpn`	(Optional) Enables the system to insert VPN suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server and sets the gateway address to the outgoing interface toward the DHCP server. • 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:** `Router(config)# ip dhcp relay information policy encapsulate`	Enables the system to encapsulate the DHCP relay agent information option (option-82 field) received from a prior relay agent in forwarded BOOTREQUEST messages to a DHCP server. • Option 82 information from both relay agents will be forwarded to the DHCP server.
Step 6	**interface** *type number* **Example:** `Router(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 a different configuration to apply on specific interfaces.
Step 7	**ip dhcp relay information policy-action encapsulate** **Example:** `Router(config-if)# ip dhcp relay information policy-action encapsulate`	(Optional) Enables the system to encapsulate the DHCP relay agent information option (option-82 field) received on an interface from a prior relay agent in forwarded BOOTREQUEST messages to a DHCP server on an interface. • This function is disabled by default. This command has precedence over any global configuration. However, if support for the relay agent information option encapsulation support is configured in global configuration mode, but not in interface configuration mode, the interface inherits the global configuration.

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

Perform this task to configure smart relay agent forwarding.

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 smart-relay** **Example:** `Router(config)# ip dhcp smart-relay`	Allows the DHCP relay agent to switch the gateway address (giaddr field of a DHCP packet) to secondary addresses when there is no DHCPOFFER message from a DHCP server.

Configuring Private and Standard Suboption Numbers Support

Some features that are not standardized will be using the private Cisco relay agent suboption numbers. Once the features are standardized, the relay agent suboptions are assigned the Internet Assigned Numbers Authority (IANA) numbers. Cisco IOS supports both the 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:** `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 compatibility suboption link-selection** {**cisco** | **standard**} **Example:** `Router(config)# ip dhcp compatibility suboption link-selection standard`	Configures the DHCP client to use the private or IANA standard relay agent suboption numbers.
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode.

Troubleshooting the DHCP Relay Agent

Perform this task to troubleshoot the DHCP relay agent.

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

SUMMARY STEPS

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

DETAILED STEPS

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

Configuration Examples for the Cisco IOS DHCP Relay Agent

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

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

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

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

The following example shows that for subscribers being serviced by the same aggregation router, the relay agent information option needs to be processed differently for ATM subscribers than 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 to the client. For Ethernet subscribers, the connected device provides the relay agent information option, and it is configured to remain in the packet and be forwarded to the client.

```
ip dhcp relay information trust-all
interface Loopback0
 ip address 10.16.0.1 255.255.255.0
!
interface 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
 encap dot1q 123
 ip unnumbered loopback1
 ip helper-address 10.18.1.2
 ip dhcp relay information policy-action keep
```

Example Configuring the Subscriber Identifier Suboption

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

```
ip dhcp relay information option
!
interface Loopback0
 ip address 10.1.1.129 255.255.255.192
!
interface 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 192.169.2.1
!
 class SIP
  relay target 192.170.2.1
```

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 DHCP Relay Agent Information Option Encapsulation Support

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 relay agents and 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 Configuring DHCP 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), inserting 192.168.100.1 in the giaddr field of the DHCP packet. If the DHCP server has a scope or pool configured for the 192.168.100.0/24 network, it will respond; otherwise it will not respond.

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

```
ip dhcp smart-relay
!
interface 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	Cisco IOS IP Addressing Services Command Reference

Related Topic	Document Title
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)*

RFCs	Title
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 21 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

Feature Name	Releases	Feature 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 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 trying to configure its interface (obtain an IP address) using DHCP or BOOTP protocols.

DHCP --Dynamic Host Configuration Protocol.

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

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

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

server --DHCP or BOOTP server.

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

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

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Restrictions for 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.

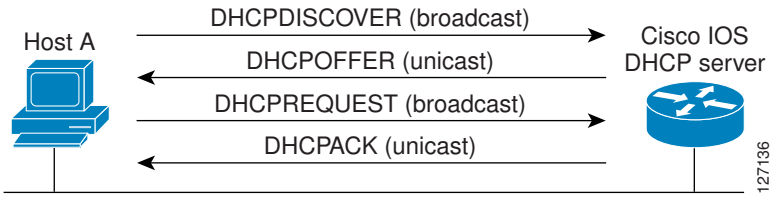
For multipoint interfaces, an IP address can be acquired using other encapsulation types because broadcast packets are used. However, unicast packets to the other end will fail because there is no ATM map entry and thus DHCP renewals and releases also fail.

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 9 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

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*}	(Optional) Specifies the class identifier.
	Example: `Router(config-if)# ip dhcp client class-id my-class-id`	
Step 6	**ip dhcp client lease** *days* [*hours*][*minutes*]	(Optional) Configures the duration of the lease for an IP address that is requested from a DHCP client to a DHCP server.
	Example: `Router(config-if)# ip dhcp client lease 2`	
Step 7	**ip dhcp client hostname** *host-name*	(Optional) Specifies or modifies the hostname sent in the DHCP message.
	Example: `Router(config-if)# ip dhcp client hostname router1`	

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.

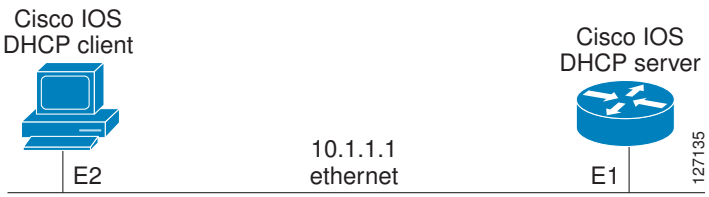
Configuration Examples for the DHCP Client

- Example Renewing a DHCP Lease, page 179

Example Configuring the DHCP Client

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

Figure 10 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

Related Topic	Document Title
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 22 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**.

Feature Name	Releases	Feature Information
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.
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**.

DHCP Option 82 Configurable Circuit ID and Remote ID

The Cisco DHCP Option 82 Configurable Circuit ID and Remote ID provides more naming choices in the Option 82 Remote ID and Option 82 Circuit ID suboptions. For example, you can use a switch-configured hostname or specify an ASCII text string for the remote ID, and you can configure an ASCII text string to override the circuit ID.

Note Refer to the configuration guide for your platform for information about configuring Dynamic Host Configuration Protocol (DHCP). See the “Configuring DHCP Snooping” section of the *Cisco 7600 Series Cisco IOS Software Configuration Guide, Release 12.2SR*, for information about configuring DHCP on Cisco 7600 series routers. See the "Additional References" section for sources of information about configuring DHCP on other Cisco platforms.

Finding Feature Information

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

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

Restrictions for DHCP Option 82 Configurable Circuit ID and Remote ID

When DHCP snooping is configured on a primary VLAN, you cannot configure snooping with different settings on any of its secondary VLANs. You must configure DHCP snooping for all associated VLANs on the primary VLAN. If DHCP snooping is not configured on the primary VLAN and you try to configure it on the secondary VLAN, for example, VLAN 200, this message appears:

```
2w5d:%DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING:DHCP Snooping configuration may not
take effect on secondary vlan 200. DHCP Snooping configuration on secondary vlan is
derived from its primary vlan.
```

You can use the **show ip dhcp snooping** command to display all VLANs, both primary and secondary, that have DHCP snooping enabled.

Information About DHCP Option 82 Configurable Circuit ID and Remote ID

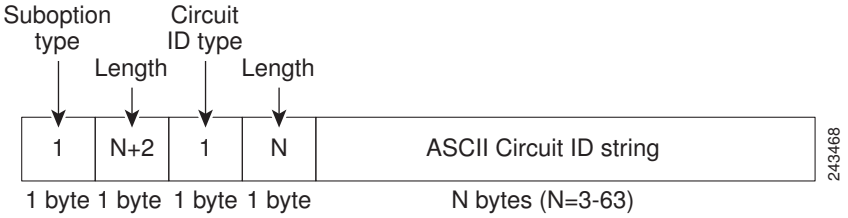
The DHCP Option 82 Configurable Circuit ID and Remote ID feature enhances validation security by allowing you to determine what information is provided in the Option 82 Remote ID and Option 82 Circuit ID suboptions.

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

See the "DHCP Snooping Option-82 Data Insertion" section of the *Cisco 7600 Series Cisco IOS Software Configuration Guide* for information about using DHCP to centrally manage the IP address assignments for a large number of subscribers in residential, metropolitan Ethernet-access environments.

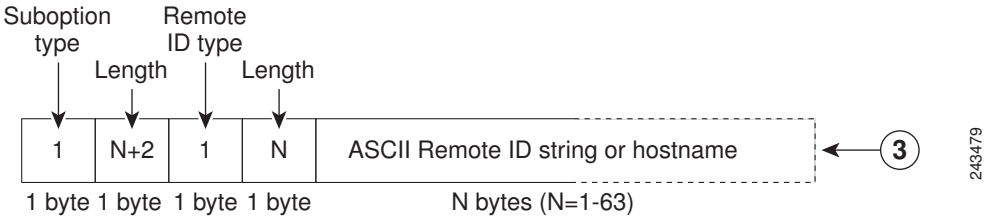
The figure below shows the packet format used when DHCP snooping is globally enabled and the **ip dhcp snooping information option** global configuration command is entered with the Circuit ID suboption.

Figure 11 Suboption Packet Formats, Circuit ID Specified



The figure below shows the packet format used when DHCP snooping is globally enabled and the **ip dhcp snooping information option** global configuration command is entered with the Remote ID suboption.

Figure 12 Suboption Packet Formats, Remote ID Specified



How to Configure DHCP Option 82 Configurable Circuit ID and Remote ID

Configuring DHCP Snooping on Private VLANs

Perform these tasks to configure DHCP snooping on private primary and secondary VLANs:

- Configure a private, primary VLAN.
- Associate with it an isolated VLAN.
- Create an SVI interface for the primary VLAN, and associate it with the appropriate loopback IP and helper address.
- Enable DHCP snooping on the primary VLAN, which also enables it on the associated VLAN.

Note You must also configure a server to assign the IP address, a DHCP pool, and a relay route so that snooping can be effective.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan** *vlan-id*
4. **private-vlan primary**
5. **private-vlan association** *secondary-vlan-list*
6. **configure terminal**
7. **vlan** *vlan_ID*
8. **private-vlan isolated**
9. **configure terminal**
10. **interface vlan** *primary-vlan_id*
11. **ip unnumbered loopback**
12. **private-vlan mapping** [*secondary-vlan-list* | **add** *secondary-vlan-list*| **remove** *secondary-vlan-list*]
13. **configure terminal**
14. **ip dhcp snooping vlan** *primary-vlan_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	**vlan** *vlan-id* **Example:** `Router(config)# vlan 70`	Enters VLAN configuration submode for the named private VLAN.
Step 4	**private-vlan primary** **Example:** `Router(config-vlan)# private-vlan primary`	Designates the VLAN as the primary private VLAN.
Step 5	**private-vlan association** *secondary-vlan-list* **Example:** `Router(config-vlan)# private-vlan association 7`	Configures private VLANs (PVLANs) and the association between a PVLAN and a secondary VLAN.
Step 6	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 7	**vlan** *vlan_ID* **Example:** `Router(config)# vlan 7`	Enters VLAN configuration mode for the named private VLAN. • In this example, the associated secondary VLAN, vlan 7.

	Command or Action	Purpose
Step 8	**private-vlan isolated** **Example:** `Router(config-vlan)# private-vlan isolated`	Designates the VLAN as an isolated private VLAN.
Step 9	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 10	**interface vlan** *primary-vlan_id* **Example:** `Router(config)# interface vlan 70`	Creates a dynamic Switch Virtual Interface (SVI) on the primary VLAN.
Step 11	**ip unnumbered loopback** **Example:** `Router(config)# ip unnumbered loopback1`	Specifies IP unnumbered loopback.
Step 12	**private-vlan mapping** [*secondary-vlan-list* | **add** *secondary-vlan-list*| **remove** *secondary-vlan-list*] **Example:** `Router(config-vlan)# private-vlan mapping 7`	Creates a mapping between the primary and the secondary VLANs so that they share the same primary VLAN SVI.
Step 13	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 14	**ip dhcp snooping vlan** *primary-vlan_id* **Example:** `Router(config)# ip dhcp snooping vlan 70`	Enables DHCP snooping on the primary and associated VLANs.

Configuration Example for DHCP Option 82 Configurable Circuit ID and Remote ID

Mapping Private-VLAN Associations Example

The following interface configuration example shows how to map the private-VLAN associations. The user-configurable circuit ID “aabb11” is inserted on the secondary VLAN, vlan 7.

```
interface GigabitEthernet9/0/1
switchport
switchport private-vlan host-association 70 7
switchport mode private-vlan host
no mls qos trust
spanning-tree portfast
ip dhcp snooping vlan 7 information option format-type circuit-id string aabb11
```

The following example shows how to define a DHCP class “C1” and specify the hex string of the corresponding class at the server by using the hex string that matches the circuit-ID value entered in the interface configuration example. That is, the hex string 00000000000000000000000000000006616162623131 mask ffffffffffffffffffffffffffff0000000000000 matches the circuit ID aabb11.

```
ip dhcp class C1
relay agent information
relay-information hex 00000000000000000000000000000006616162623131 mask
ffffffffffffffffffffffffffff0000000000000
```

Additional References

Related Documents

Related Topic	Document Title
Configuring DHCP on the Cisco 7600 series router	“Configuring DHCP Snooping” section of the *Cisco 7600 Series Cisco IOS Software Configuration Guide*
Configuring DHCP on the Cisco Catalyst 3550 multilayer switch	“Configuring DHCP Features” section of the *Catalyst 3550 Multilayer Switch Software Configuration Guide*
Configuring DHCP on the Cisco Catalyst 2970 switch	“Configuring DHCP Features” section of the *Catalyst 2970 Switch Software Configuration Guide*
Configuring DHCP on the Cisco Catalyst 3560 switch	“Configuring DHCP Features and IP Source Guard” section of the *Catalyst 3560 Switch Software Configuration Guide*

Related Topic	Document Title
Configuring DHCP on the Cisco Catalyst 3750 switch	"Configuring DHCP Features and IP Source Guard" section of the *Catalyst 3750 Switch Software Configuration Guide*
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
•	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

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

Technical Assistance

Description	Link
The Cisco Support 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 Option 82 Configurable Circuit ID and Remote ID

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 23 Feature Information for DHCP Option 82 Configurable Circuit ID and Remote ID

Feature Name	Releases	Feature Information
DHCP Option 82 Configurable Circuit ID and Remote ID	12.2(33)SRD1	Provides naming choices in the Option 82 Remote ID and Option 82 Circuit ID suboptions. The following commands were introduced or modified: **ip dhcp snooping vlan**.

Configuring DHCP Services for Accounting and Security

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

Finding Feature Information

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

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

Prerequisites for Configuring DHCP Services for Accounting and Security

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

Information About DHCP Services for Accounting and Security

DHCP Operation in Public Wireless LANs

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

Security Vulnerabilities in Public Wireless LANs

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

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

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

DHCP Services for Security and Accounting Overview

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

DHCP accounting provides authentication, authorization, and accounting (AAA) and RADIUS support for DHCP. The AAA and RADIUS support improves security by sending secure START and STOP accounting messages. The configuration of DHCP accounting adds a layer of security that allows DHCP lease assignment and termination to be triggered for the appropriate RADIUS START and STOP accounting records so that the session state is properly maintained by upstream devices, such as an SSG. This additional security can help to prevent hackers or unauthorized clients 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 without the system detecting it. 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 allowed to install ARP entries.

The third feature is ARP Auto-logoff, 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 frequently a peer is probed (the interval), and the maximum number of retries (the count).

DHCP Lease Limits

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

How to Configure DHCP Services for Accounting and Security

Configuring AAA and RADIUS for DHCP Accounting

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

RADIUS Accounting Attributes

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

Table 24 RADIUS Accounting Attributes

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model. • DHCP accounting functions only in the access control model. **Note** TACACS and extended TACACS commands are not available after this command is configured and are not supported by DHCP accounting.
Step 4	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius RGROUP-1`	Creates a server group for AAA or TACACS+ services and enters server group RADIUS configuration mode. • The server group is created in this step so that accounting services can be applied.
Step 5	**server** *ip-address* **auth-port** *port-number* **acct-port** *port-number* **Example:** `Router(config-sg-radius)# server 10.0.0.1 auth-port 1645 acct-port 1646`	Specifies the servers that are members of the server group that was created in Step 4. • You must open port numbers for authorization and accounting. 1645 is the default port number for authorization, and 1646 is the default port number for accounting. The range of port numbers that can be specified is from 0 to 65535. • The values entered for the **auth-port** *port-number*and **acct-port** *port-number* keywords and arguments must match the port numbers that will be configured in Step 10.
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server group RADIUS configuration mode and enters global configuration mode.
Step 7	**aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name* **Example:** `Router(config)# aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1`	Configures RADIUS accounting for the specified server group. • The RADIUS accounting server is specified in the first *list-name* argument (RADIUS-GROUP1), and the target server group is specified in the second *group-name*argument (RGROUP-1). • This command enables start and stop accounting for DHCP accounting. The **start-stop** keyword enables the transmission of both START and STOP accounting messages. The **stop-only** keyword will enable the generation and verification of STOP accounting messages only.

	Command or Action	Purpose
Step 8	**aaa session-id** {**common** | **unique**} **Example:** `Router(config)# aaa session-id common`	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
Step 9	**ip radius source-interface** *type number* [**vrf** *vrf-name*] **Example:** `Router(config)# ip radius source-interface Ethernet 0`	Forces RADIUS to use the IP address of the specified interface for all outgoing RADIUS packets.
Step 10	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config)# radius-server host 10.1.1.1 auth-port 1645 acct-port 1646`	Specifies the RADIUS server host. • The values entered for the **auth-port** *port-number*and **acct-port** *port-number* keywords and arguments must match the port numbers that were configured in Step 5.
Step 11	**radius-server retransmit** *number-of-retries* **Example:** `Router(config)# radius-server retransmit 3`	Specifies the number of times that Cisco IOS software will look for RADIUS server hosts.

Troubleshooting Tips

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

debug radius accounting

Configuring DHCP Accounting

Perform this task to configure DHCP accounting.

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

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

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

Note The following restrictions apply to DHCP accounting:

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

>

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 WIRELESS-POOL`	Configures a DHCP address pool and enters DHCP pool configuration mode.

	Command or Action	Purpose
Step 4	**accounting** *method-list-name* **Example:** `Router(config-dhcp)# accounting RADIUS-GROUP1`	Enables DHCP accounting if the specified server group is configured to run RADIUS accounting. • The example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will be sent only if RADIUS-GROUP1 is configured as a stop-only group. See Step 7 in the Configuring AAA and RADIUS for DHCP Accounting, page 193 section for more details.

Verifying DHCP Accounting

Perform this task to verify the DHCP accounting configuration.

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Securing ARP Table Entries to DHCP Leases

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 WIRELESS-POOL`	Configures a DHCP address pool and enters DHCP pool configuration mode.
Step 4	**update arp** **Example:** `Router(config-dhcp)# update arp`	Secures insecure ARP table entries to the corresponding DHCP leases. • Existing active DHCP leases will not be secured until they are renewed. Using the **no update arp** command will change secured ARP table entries back to dynamic ARP table entries.
Step 5	**renew deny unknown** **Example:** `Router(config-dhcp)# renew deny unknown`	(Optional) Configures the renewal policy for unknown clients. • See the "Troubleshooting Tips" section for information about when to use this command.

• Troubleshooting Tips, page 200

Troubleshooting Tips

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

To remedy this situation, use the **renew deny unknown** command in DHCP pool configuration mode. This command forces the DHCP server to reject renewal requests from clients if the requested address is present

at the server but is not leased. The DHCP server sends a DHCPNAK denial message to the client, which forces the client back to its initial state. The client can then negotiate for a new lease immediately, instead of waiting for its old lease to expire.

Configuring DHCP Authorized ARP

Perform this task to configure DHCP authorized ARP, which disables dynamic ARP learning on an interface.

DHCP authorized ARP has a limitation in supporting accurate one-minute billing. DHCP authorized ARP probes for authorized users once or twice, 30 seconds apart. In a busy network the possibility of missing reply packets increases, which can cause a premature logoff. If you need a more accurate and finer control for probing of the authorized user, configure the **arp probe interval** command. This command specifies when to start a probe, the interval between unsuccessful probes, and the maximum number of retries before triggering an automatic logoff.

Note If both static and authorized ARP are installing the same ARP entry, static configuration overrides authorized ARP. You can install a static ARP entry by using the **arp** global configuration command. You can only remove a nondynamic ARP entry by the same method in which it was installed.

The ARP timeout period should not be set to less than 30 seconds. The feature is designed to send out an ARP message every 30 seconds, beginning 90 seconds before the ARP timeout period specified by the **arp timeout**command. This behavior allows probing for the client at least three times before giving up on the client. If the ARP timeout is set to 60 seconds, an ARP message is sent twice, and if it is set to 30 seconds, an ARP message is sent once. An ARP timeout period set to less than 30 seconds can yield unpredictable results.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **arp authorized**
6. **arp timeout** *seconds*
7. **arp probe interval** *seconds* **count** *number*
8. **end**
9. **show arp**

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 address** *ip-address mask* **Example:** `Router(config-if)# ip address 209.165.200.224 209.165.200.224`	Sets a primary IP address for an interface.
Step 5	**arp authorized** **Example:** `Router(config-if)# arp authorized`	Disables dynamic ARP learning on an interface. • The IP address to MAC address mapping can be installed only by the authorized subsystem.
Step 6	**arp timeout** *seconds* **Example:** `Router(config-if)# arp timeout 60`	Configures how long an entry remains in the ARP cache.

	Command or Action	Purpose
Step 7	**arp probe interval** *seconds* **count** *number* **Example:** `Router(config-if)# arp probe interval 5 count 30`	(Optional) Specifies an interval, in seconds, and number of probe retries. • *seconds* --Interval, in seconds, after which the next probe will be sent to see if a peer is present. The range is from 1 to 10. • *number* --Number of probe retries. If there is no reply after the count has been reached, the peer has logged off. The range is from 1 to 60. **Note** You must use the **no** form of the command to stop the probing process.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 9	**show arp** **Example:** `Router# show arp`	(Optional) Displays the entries in the ARP table.

Configuring a DHCP Lease Limit to Globally Control the Number of Subscribers

Perform this task to globally control the number of DHCP leases allowed for clients behind an ATM Routed Bridged Encapsulation (RBE) unnumbered interface or serial unnumbered interface.

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

If this feature is enabled on a Cisco IOS DHCP relay agent connected to clients through unnumbered interfaces, the relay agent keeps information about the DHCP leases offered to the clients per subinterface. When a DHCPACK message is forwarded to the client, the relay agent increments the number of leases offered to clients on that subinterface. If a new DHCP client tries to obtain an IP address and the number of leases has already reached the configured lease limit, DHCP messages from the client will be dropped and will not be forwarded to the DHCP server.

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

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

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease log**
4. **ip dhcp limit lease per interface** *lease-limit*
5. **end**
6. **show ip dhcp limit lease** [*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	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp limit lease log** **Example:** `Router(config)# ip dhcp limit lease log`	(Optional) Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded. • If this command is configured, any lease limit violations will display in the output of the **show ip dhcp limit lease** command.
Step 4	**ip dhcp limit lease per interface** *lease-limit* **Example:** `Router(config)# ip dhcp limit lease per interface 2`	Limits the number of leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**show ip dhcp limit lease** [*type number*] **Example:** `Router# show ip dhcp limit lease`	(Optional) Displays the number of times the lease limit threshold has been violated. • You can use the **clear ip dhcp limit lease** privileged EXEC command to manually clear the stored lease violation entries.

• Troubleshooting Tips, page 205

Troubleshooting Tips

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

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

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

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

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

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

>

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **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 limit lease log** **Example:** `Router(config)# ip dhcp limit lease log`	(Optional) Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded. • If this command is configured, any lease limit violations will display in the output of the **show ip dhcp limit lease** command.
Step 4	**interface** *type number* **Example:** `Router(config)# interface Seria l0/0`	Enters interface configuration mode.
Step 5	**ip dhcp limit lease** *lease-limit* **Example:** `Router(config-if)# ip dhcp limit lease 6`	Limits the number of leases offered to DHCP clients per interface. • The interface configuration will override any global setting specified by the **ip dhcp limit lease per interface** global configuration command.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**show ip dhcp limit lease** [*type number*] **Example:** `Router# show ip dhcp limit lease Serial 0/0`	(Optional) Displays the number of times the lease limit threshold has been violated. • You can use the **clear ip dhcp limit lease** privileged EXEC command to manually clear the stored lease violation entries.
Step 8	**show ip dhcp server statistics** [*type number*] **Example:** `Router# show ip dhcp server statistics Serial0/0`	(Optional) Displays DHCP server statistics. • This command was modified in Cisco IOS Release 12.2(33)SRC to display interface-level DHCP statistics.

- Troubleshooting Tips, page 207

Troubleshooting Tips

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

Configuration Examples for DHCP Services for Accounting and Security

Example Configuring AAA and RADIUS for DHCP Accounting

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

```
aaa new-model
aaa group server radius RGROUP-1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 exit
```

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

Example Configuring DHCP Accounting

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

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

Example Verifying DHCP Accounting

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

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

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

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

```
00:45:50:DHCPD:DHCPDISCOVER received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 on
interface Ethernet0.
00:45:52:DHCPD:assigned IP address 10.10.10.16 to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.
00:45:52:DHCPD:Sending DHCPOFFER to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31(10.10.10.16)
00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.
00:45:52:DHCPD:DHCPREQUEST received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.
00:45:52:DHCPD:Sending DHCPACK to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31
(10.10.10.16).
00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.
00:45:52:DHCPD:triggered Acct Start for 0001.42c9.ec75 (10.10.10.16).
```

The following is sample output from the **debug ip dhcp server events**command. The output was generated on a DHCP server and shows the receipt of an explicit release message from the DHCP client. The DHCP

server triggers an accounting STOP message and then returns the IP address to the DHCP pool. Information about the accounting STOP message is shown in the third line of the following output:

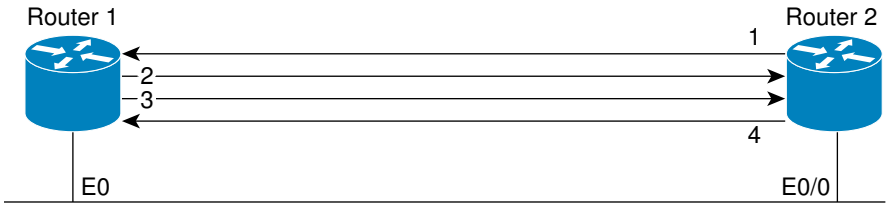
```
00:46:26:DHCPD:DHCPRELEASE message received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 (10.10.10.16)
00:46:26:DHCPD:triggered Acct Stop for (10.10.10.16).
00:46:26:DHCPD:returned 10.10.10.16 to address pool WIRELESS-POOL.
```

Example Configuring DHCP Authorized ARP

Router 1 is the DHCP server that assigns IP addresses to the routers that are seeking IP addresses, and Router 2 is the DHCP client configured to obtain its IP address through the DHCP server. Because the **update arp** DHCP pool configuration command is configured on Router 1, the router will install a secure ARP entry in its ARP table. The **arp authorized** command stops any dynamic ARP on that interface. Router 1 sends periodic ARPs to Router 2 to make sure that the client is still active. Router 2 responds with an ARP reply. Unauthorized clients cannot respond to these periodic ARPs. The unauthorized ARP responses are blocked at the DHCP server. The timer for the entry is refreshed on Router 1 upon receiving the response from the authorized client.

See the figure below for a sample topology.

Figure 13 Sample Topology for DHCP Authorized ARP



1. Send request for IP address.
2. Assign IP address and install secure ARP entry for it in Router 1.
3. Send periodic ARPs to make sure Router 2 is still active.
4. Reply to periodic ARPs.

103063

Router 1 (DHCP Server)

```
ip dhcp pool name1
 network 10.0.0.0 255.255.255.0
 lease 0 0 20
 update arp
!
interface Ethernet 0
 ip address 10.0.0.1 255.255.255.0
 half-duplex
 arp authorized
 arp timeout 60
! optional command to adjust the periodic ARP probes sent to the peer
 arp probe interval 5 count 15
```

Router 2 (DHCP Client)

```
interface Ethernet 0/0
 ip address dhcp
 half-duplex
```

Example Verifying DHCP Authorized ARP

The following is sample output from the **show arp** command on Router 1 (see the figure above):

```
Router1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.3               0   0004.dd0c.ffcb  ARPA   Ethernet01
Internet  10.0.0.1               -   0004.dd0c.ff86  ARPA   Ethernet0
```

The following is sample output from the **show arp** command on Router 2 (see the figure above):

```
Router2# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.3               -   0004.dd0c.ffcb  ARPA   Ethernet0/02
Internet  10.0.0.1               0   0004.dd0c.ff86  ARPA   Ethernet0/0
```

Example Configuring a DHCP Lease Limit

In the following example, if more than three clients try to obtain an IP address from ATM interface 4/0.1, the DHCPDISCOVER packets will not be forwarded to the DHCP server. If the DHCP server resides on the same router, DHCP will not reply to more than three clients.

```
ip dhcp limit lease per interface 3
!
interface loopback 0
 ip address 10.1.1.129 255.255.255.192
!
interface ATM 4/0.1
 no ip address
!
interface ATM 4/0.1 point-to-point
 ip helper-address 172.16.1.2
 ip unnumbered loopback 0
 atm route-bridged ip
  pvc 88/800
  encapsulation aal5snap
```

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

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

Additional References

Related Documents

Related Topic	Document Title
ARP commands: complete command syntax, command modes, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP commands: complete command syntax, command modes, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP conceptual information	"DHCP Overview" module 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 ODAP configuration	"Configuring the DHCP Server On-Demand Address Pool Manager" 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 relay agent configuration	"Configuring the Cisco IOS DHCP Relay Agent" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP enhancements for edge-session management	"Configuring DHCP Enhancements for Edge-Session Management" module in the *Cisco IOS IP Addressing Configuration Guide*
AAA and RADIUS configuration tasks	*Cisco IOS Security Configuration Guide*
AAA and RADIUS commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*

Standards

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

MIBs

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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support 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 Services for Accounting and Security

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

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

Table 25 Feature Information for DHCP Services for Accounting and Security

Feature Name	Releases	Feature Information
DHCP per Interface Lease Limit and Statistics	12.2(33)SRC	This feature limits the number of DHCP leases offered to DHCP clients on an interface. DHCP server statistics reporting was enhanced to display interface-level statistics. The following commands were introduced or modified by this feature: **clear ip dhcp limit lease**, **ip dhcp limit lease**, **ip dhcp limit lease log**, **show ip dhcp limit lease**, **show ip dhcp server statistics**.
DHCP Lease Limit per ATM RBE Unnumbered Interface	12.2(28)SB 12.3(2)T 15.1(1)S	This feature limits the number of DHCP leases per subinterface offered to DHCP clients connected from an ATM RBE unnumbered interface or serial unnumbered interface of the DHCP server or DHCP relay agent. The following command was introduced by this feature: **ip dhcp limit lease per interface**.
ARP Auto-logoff	12.3(14)T	The ARP Auto-logoff feature enhances DHCP authorized ARP by providing finer control and probing of authorized clients to detect a logoff. The following command was introduced by this feature: **arp probe interval**.

Feature Name	Releases	Feature Information
DHCP Authorized ARP	12.2(33)SRC 12.3(4)T	DHCP authorized ARP enhances the DHCP and ARP components of the Cisco IOS software to limit the leasing of IP addresses to mobile users to authorized users. This feature enhances security in PWLANs by blocking ARP responses from unauthorized users at the DHCP server. The following command was introduced by this feature: **arp authorized**.
DHCP Accounting	12.2(15)T 12.2(28)SB 12.2(33)SRB	DHCP accounting introduces AAA and RADIUS support for DHCP configuration. The following command was introduced by this feature: **accounting**.
DHCP Secured IP Address Assignment	12.2(15)T 12.2(28)SB 12.2(33)SRC	DHCP secure IP address assignment provides the capability to secure ARP table entries to DHCP leases in the DHCP database. This feature secures and synchronizes the MAC address of the client to the DHCP binding, preventing hackers or unauthorized clients from spoofing the DHCP server and taking over a DHCP lease of an authorized client. The following commands were introduced or modified by this feature: **show ip dhcp server statistics**, **update arp**.

Configuring DHCP Enhancements for Edge-Session Management

The DHCP Enhancements for Edge-Session Management feature provides the capability of simultaneous service by multiple Internet Service Providers (ISPs) to customers using one network infrastructure. The end-user customer may change ISPs at any time.

The DHCP enhancements evolved out of the Service Gateways (SGs) requirement to receive information from the DHCP server about when client DISCOVER packets (session initiation) are received, when an address has been allocated to a client, and when a client has released a DHCP lease or the lease has expired (session termination).

Finding Feature Information

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

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

Information About DHCP Enhancements for Edge-Session Management

DHCP Servers and Relay Agents

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

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

For more information, refer to the DHCP modules in the *Cisco IOS IP Addressing Services Configuration Guide* , Release 12.4.

On-Demand Address Pool Management

An On-Demand Address Pool (ODAP) is used to centralize the management of large pools of addresses and simplifies the configuration of large networks. ODAP provides a central management point for the allocation and assignment of IP addresses.

When a Cisco router is configured as an ODAP manager, pools of IP addresses are dynamically increased or reduced in size depending on the address utilization level. The ODAP manager is supported by centralized Remote Authentication Dial-In User Service (RADIUS) or DHCP servers and is configured to request an initial pool of addresses from either the RADIUS or DHCP server.

The ODAP manager controls IP address assignment and will allocate additional IP addresses as necessary. This method of address allocation and assignment optimizes the use of available address space and simplifies the configuration of medium and large-sized networks.

For more information, see the “Configuring the DHCP Server On-Demand Address Pool Manager” module.

Design of the DHCP Enhancements for Edge-Session Management Feature

With the DHCP Enhancements for Edge-Session Management feature, a DHCP server and relay agent are separate, but closely coupled. The basic design of the feature encompasses two types of configuration at the edge of an ISP network as follows:

- DHCP server and an SG that are co-resident (in the same device)
- DHCP relay agent and an SG that are co-resident

- DHCP Server Co-Resident with the SG, page 218
- DHCP Relay Agent Co-Resident with the SG, page 219

DHCP Server Co-Resident with the SG

With this configuration, the DHCP server is in the same device as the SG and allocates addresses from locally configured address pools or acquires a subnet of addresses to allocate from some other system in the network. There are no changes to the server address allocation function to support the configuration.

This configuration enables the DHCP server to notify the SG that it has received a broadcast sent by the end-user DHCP client. The SG passes the MAC address and other information to the DHCP server. The SG

also passes a class name (for example, the name of the ISP), which is used by the DHCP server to match a pool-class definition.

Lease-state notifications are always made by the DHCP server to the SG, because the information is already present.

Note The local configuration may also be performed by an ODAP that acquires subnets for the address pools from another DHCP server or a RADIUS server.

DHCP Relay Agent Co-Resident with the SG

With this configuration, the relay agent is in the same device as the SG and intercedes in DHCP sessions to appear as the DHCP server to the DHCP client. As the server, the relay agent may obtain enough information about the DHCP session to notify the SG of all events (for example, lease termination).

Appearing to be the DHCP server is performed by using the DHCP functionality that is currently in use on unnumbered interfaces. This functionality enables the relay agent to substitute its own IP address for the server.

The packet is passed by the relay agent to the DHCP server and the SG is notified of the receipt. Following the notification, an inquiry is made by the relay agent to the SG about which DHCP class name to use. Then, the packet is passed by the relay agent to the selected DHCP server.

The end-user DHCP client MAC address and other pertinent information is passed to the SG. The SG returns the DHCP class name to use when matching a DHCP pool if the SG is configured to do so. If the DHCP relay agent is not acting as a server, it relays the packet to the DHCP server.

Note An address pool may have one DHCP class defined to specify one central DHCP server to which the relay agent passes the packet, or it may have multiple DHCP classes defined to specify a different DHCP server for each client.

Benefits of the DHCP Enhancements for Edge-Session Management

The benefits of the DHCP Enhancements for Edge-Session Management feature are as follows:

- Allows the full DHCP server system to be located farther inside the network, while only running a relatively simple DHCP relay agent at the edge.
- Simplifies the DHCP configuration at the edge.
- Allows all DHCP server administration to occur closer to the middle of the network on one centralized DHCP server, or on separate DHCP servers (one for each ISP).
- Allows each ISP full control over all DHCP options and lease times.
- Allows both the DHCP server and client configurations to be used on the same edge system simultaneously.

How to Configure DHCP Enhancements for Edge-Session Management

Configuring the DHCP Address Pool and a Class Name

Perform this task to configure a DHCP server that assigns addresses from an address pool for a specific class name that has been assigned by an SG that is co-resident with the DHCP server at the edge.

If a DHCP server is resident in the same device as an SG and both are at the edge, a class name and address pool should be configured. In this case, the DHCP server notifies an SG of a DISCOVER broadcast received from a client and the SG returns a class name. The returned class name designates an address range of an address pool. The DHCP server sends the MAC address and IP address of the incoming interface or the specified relay-agent address to the SG.

Note If the DHCP server has its address pools defined locally or retrieves the subnets from ISP DHCP servers or AAA servers using ODAP, additional DHCP server configuration on behalf of the SG is not required.

If dynamic allocation of the address pool is required using ODAP, the **origin** command is specified.

The specification of the class name is required in the DHCP address-pool configuration and in the SG system itself to designate each DHCP client class name. A default class name should be configured if a user does not have one.

Each address pool should be associated with one or more DHCP classes (address-provider ISPs). When the DHCP client selects an ISP, the selection becomes the class name designated by the SG.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **origin** {**dhcp** | **file** *url*}
5. **network** *network-number* [*mask* | *prefix-length*]
6. **class** *class-name*
7. **address range** *start-ip end-ip*
8. Repeat Steps 3, 5, and 6.
9. **exit**

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 abc-pool`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode. The *name* argument is the name of the pool and may either be a symbolic string (such as engineering) or an integer (such as 0).
Step 4	**origin** {**dhcp** | **file** *url*} **Example:** `Router(dhcp-config)# origin dhcp`	(Optional) Configures an address pool as an On-Demand Address Pool (ODAP) or static mapping pool. The argument and keywords are as follows:
Step 5	**network** *network-number* [*mask* | *prefix-length*] **Example:** `Router(dhcp-config)# network 10.10.0.0 255.255.0.0`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server. The arguments are as follows: • *network-number* --The IP address of the DHCP address pool. Use this argument if ODAP is not the IP address assignment method. • *mask* --(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host. • *prefix-length* --(Optional) The number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 6	**class** *class-name* **Example:** `Router(dhcp-config)# class abc-pool`	Associates a class with a DHCP address pool and enters DHCP pool-class configuration mode. The *class-name* argument is the name of the class. It should match the DHCP address pool name. Repeat this step to specify a default class name if required by the SG.

	Command or Action	Purpose
Step 7	**address range** *start-ip end-ip* **Example:** `Router(config-dhcp-pool-class)# address range 10.10.5.0 10.99.99.99`	(Optional) Configures an IP address range from which the DHCP server would allocate the IP addresses. If an SG returned an IP address that is not configured, no action is taken. This step enables the allocation of an address from a range for the class name specified in the previous step. **Note** The **address range** command cannot be used with a relay pool that is configured with the **relay destination** command. Further, if no address range is assigned to a class name, the address is specified with the **network** command.
Step 8	Repeat Steps 3, 5, and 6.	If there is an interface configured with multiple subnets and different ISPs, repeat this step to match the number of subnets. See the "Multiple DHCP Pools and Different ISPs" Configuration Example.
Step 9	**exit** **Example:** `Router(config-dhcp-pool-class)# exit`	Exits to DHCP pool configuration mode.

Configuring a Relay Pool with a Relay Source and Destination

Perform this task to configure a relay pool when the DHCP relay and SG are resident in the same device at the edge, and all end users will obtain addresses from one pool. This task replaces the IP helper-address interface configuration.

If the SG notifies the relay agent that DHCP session notifications are required for a particular DHCP client, the relay agent will retain enough information about the DHCP session to notify the SG of all events (for example, lease termination). The relay intercedes DHCP sessions and assumes the role of the DHCP server. The IP address configuration becomes a dynamically changing value depending on the DHCP client information and the SG device policy information.

Note If a relay agent is interceding in DHCP sessions and assuming the role of the DHCP server, the use of DHCP authentication is not possible.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **update arp**
5. **relay source** *ip-address subnet-mask*
6. **relay destination** [**vrf** *vrf-name* | **global**] *ip-address*
7. **accounting** *method-list-name*
8. **exit**

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 abc-pool`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode. The *name* argument is the name of the pool and may either be a symbolic string (such as engineering) or an integer (such as 0). More than one name may be configured.
Step 4	**update arp** **Example:** `Router(dhcp-config)# update arp`	(Optional) Configures secure and dynamic Address Resolution Protocol (ARP) entries in the ARP table to their corresponding DHCP bindings. **Note** If the system is allocating an address from an address pool, it will add secure ARP. If the system is relaying a packet using an address pool, it will also add secure ARP.
Step 5	**relay source** *ip-address subnet-mask* **Example:** `Router(dhcp-config)# relay source 10.0.0.0 255.0.0.0`	Configures the relay source. The *ip-address*and *subnet-mask* arguments are the IP address and subnet mask for the relay source. **Note** 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 matches the relay source configuration.

	Command or Action	Purpose
Step 6	**relay destination** [**vrf** *vrf-name* | **global**] *ip-address* **Example:** `Router(dhcp-config)# relay destination 10.5.5.0`	Configures the IPv4 address of a remote DHCP server to which DHCP client packets are sent. The arguments and keywords are as follows: • **vrf** --(Optional) Virtual routing and forwarding (VRF). The *vrf-name* argument is the name of the VRF associated with the relay destination IP address. • **global** --(Optional) Global IP address. Use the this keyword when the relay agent is in the global address space and the relay source is in a VRF. • *ip-address* --IP address of the relay destination. **Note** When using the **relay destination** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay destination IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.
Step 7	**accounting** *method-list-name* **Example:** `Router(dhcp-config)# accounting RADIUS-GROUP1`	(Optional) Enables DHCP accounting if the specified server group is configured to run RADIUS accounting. • AAA and RADIUS must be enabled before DHCP accounting will operate. • The example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group. See "Configuring DHCP Services for Accounting and Security" module for more information on DHCP accounting.
Step 8	**exit** **Example:** `Router(dhcp-config)# exit`	Exits to global configuration mode.

Configuring a Relay Pool for a Remote DHCP Server

Perform this task to use an SG-supplied class name when selecting the remote DHCP server in a configured relay pool, which is used to specify how DHCP client packets should be relayed. Multiple configurations of relay targets may appear in a pool-class definition in which case all addresses are used for relay purposes.

Note The **relay source** command cannot be used with the **network** command or **origin** command since those commands implicitly designate the incoming interface and are used to define a different type of pool. It associates the relay only with an interface in the same way that the **ip helper-address** command does by its presence as an interface configuration command.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **relay source** *ip-address subnet-mask*
5. **relay destination** [**vrf** *vrf-name* | **global**] *ip-address*
6. **accounting method-list-name**
7. **class** *class-name*
8. **relay target** [**vrf** *vrf-name* | **global**] *ip-address*
9. **exit**

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 abc-pool`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode. The *name* argument is the name of the pool and may either be a symbolic string (such as engineering) or an integer (such as 0). You may specify more than one DHCP address pool.
Step 4	**relay source** *ip-address subnet-mask* **Example:** `Router(dhcp-config)# relay source 10.0.0.0 255.0.0.0`	Configures the relay source. The *ip-address*and *subnet-mask* arguments are the IP address and subnet mask for the relay source. **Note** 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 matches the relay source configuration.

Command or Action	Purpose
Step 5 **relay destination** [**vrf** *vrf-name* | **global**] *ip-address* **Example:** `Router(dhcp-config)# relay destination 10.5.5.0`	Configures the IPv4 address of a remote DHCP server to which DHCP client packets are sent. The arguments and keywords are as follows: • **vrf** --(Optional) Virtual routing and forwarding (VRF). The *vrf-name* argument is the name of the VRF associated with the relay destination IP address. • **global** --(Optional) Global IP address. Use the this keyword when the relay agent is in the global address space and the relay source is in a VRF. • *ip-address* --IP address of the relay destination. **Note** When using the **relay destination** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay destination IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.
Step 6 **accounting method-list-name** **Example:** `Router(dhcp-config)# accounting RADIUS-GROUP1`	(Optional) Enables DHCP accounting if the specified server group is configured to run RADIUS accounting. • AAA and RADIUS must be enabled before DHCP accounting will operate. • The example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group. See "Configuring DHCP Services for Accounting and Security" module for more information on DHCP accounting.
Step 7 **class** *class-name* **Example:** `Router(dhcp-config)# class abc-pool`	Associates a class with a DHCP address pool and enters DHCP pool-class configuration mode. The *class-name* argument is the name of the class. You may configure more than one class name.
Step 8 **relay target** [**vrf** *vrf-name* | **global**] *ip-address* **Example:** `Router(config-dhcp-pool-class)# relay target 10.0.0.0`	Configures the relay target IP address. The arguments and keywords are as follows: • **vrf** --(Optional) Virtual routing and forwarding (VRF). The *vrf-name* argument is the name of VRF associated with the relay target IP address and more than one target may be specified. • **global** --(Optional) Global IP address space. • *ip-address* --IP address of the relay target. More than one target IP address may be specified. **Note** This command specifies the destination for the relay function in the same manner as the **ip helper-address** command. **Note** When using the **relay target** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay target IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config-dhcp-pool-class)# exit`	Exits to DHCP pool configuration mode.

Configuring Other Types of Relay Pools

Configuring Relay Information for an Address Pool

Perform this task to configure relay information for an address pool. In this configuration, the SG sends one class name that results in the DISCOVER packet being relayed to a server at the IP address configured using the **relay target**command. If the SG sends a class name that is not configured as being associated with the address pool, then no action is taken.

Note Specifying the **address range** command and **relay target** command in a pool-class definition is not possible, because this would allocate an address and relay for the same packet.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *name*
4. **network** *network-number* [*mask* | *prefix-length*]
5. **class** *class-name*
6. **relay target** [**vrf** *vrf-name* | **global**] *ip-address*
7. **exit**
8. Repeat Steps 5 through 7 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 pool** *name* **Example:** `Router(config)# ip dhcp pool abc-pool`	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode. The *name* argument is the name of the pool and may either be a symbolic string (such as engineering) or an integer (such as 0).
Step 4	**network** *network-number* [*mask* | *prefix-length*] **Example:** `Router(dhcp-config)# network 10.0.0.0 255.0.0.0`	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server. The arguments are as follows: • *network-number* --The IP address of the DHCP address pool. • *mask* --(Optional) The bit combination that renders which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host. • *prefix-length* --(Optional) The number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 5	**class** *class-name* **Example:** `Router(dhcp-config)# class abc-pool`	Associates a class with a DHCP address pool and enters DHCP pool-class configuration mode. The *class-name* argument is the name of the class. More than one class name may be configured. **Note** If no relay target or address range is configured for a DHCP pool class name, the DHCP pool configuration is used as the class by default.

	Command or Action	Purpose
Step 6	**relay target** [**vrf** *vrf-name* | **global**] *ip-address* **Example:** `Router(config-dhcp-pool-class)# relay target 10.0.0.0`	Configures the relay target IP address. The arguments and keywords for the **relay target** command are as follows: • **vrf** --(Optional) Virtual routing and forwarding (VRF). The *vrf-name* argument is the name of VRF associated with the relay target IP address and more than one target may be specified. • **global** --(Optional) Global IP address space. • *ip-address* --IP address of the relay target. More than one target IP address may be specified. **Note** When using the **relay target** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay target IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.
Step 7	**exit** **Example:** `Router(config-dhcp-pool-class)# exit`	Exits to DHCP pool configuration mode.
Step 8	Repeat Steps 5 through 7 for each DHCP class you need to configure.	--

Configuring Multiple Relay Sources for a Relay Pool

Perform this task to configure multiple relay sources for a relay pool. The configuration is similar to configuring an IP helper address on multiple interfaces. Pools are matched to the IP addresses on an incoming interface in the order in which the interfaces display when the **show running-config**command is used. Once a relay is found or an address allocation is found, the search stops.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **exit**
6. **ip dhcp pool** *name*
7. **relay source** *ip-address subnet-mask*
8. **relay destination** [**vrf** *vrf-name* | **global**] *ip-address*
9. **accounting** *method-list-name*
10. Repeat Steps 6 and 7 for each configured DHCP pool.
11. **exit**

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 ethernet1`	Configures an interface and enters interface configuration mode. The arguments are as follows:
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.0.0.0 255.0.0.0`	Sets a primary or secondary IP address for an interface.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits to global configuration mode.
Step 6	**ip dhcp pool** *name* **Example:** `Router(config)# ip dhcp pool abc-pool1`	Configures a DHCP address pool on a DHCP server and enters DHCP pool configuration mode. The *name* argument is the name of the pool and may either be a symbolic string (such as engineering) or an integer (such as 0). More than one pool may be assigned.

	Command or Action	Purpose
Step 7	**relay source** *ip-address subnet-mask* **Example:** `Router(dhcp-config)# relay source 10.0.0.0 255.0.0.0`	Configures the relay source. The *ip-address*and *subnet-mask* arguments are the IP address and subnet mask for the relay source. **Note** 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 matches the relay source configuration.
Step 8	**relay destination** [**vrf** *vrf-name* | **global**] *ip-address* **Example:** `Router(dhcp-config)# relay destination 10.5.5.0`	Configures the IPv4 address of a remote DHCP server to which DHCP client packets are sent. The arguments and keywords are as follows: • **vrf** --(Optional) Virtual routing and forwarding (VRF). The *vrf-name* argument is the name of the VRF associated with the relay destination IP address. • **global** --(Optional) Global IP address. Use the this keyword when the relay agent is in the global address space and the relay source is in a VRF. • *ip-address* --IP address of the relay destination. **Note** When using the **relay destination** command, the *ip-address* argument is assumed to be in the same VRF as the address pool under which the command was configured. If the relay destination IP address is in a different VRF, or in the global address space, then the **vrf** *vrf-name* or **global** keywords need to be specified.
Step 9	**accounting** *method-list-name* **Example:** `Router(dhcp-config)# accounting RADIUS-GROUP1`	(Optional) Enables DHCP accounting if the specified server group is configured to run RADIUS accounting. • AAA and RADIUS must be enabled before DHCP accounting will operate. • The example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group. See “Configuring DHCP Services for Accounting and Security” module for more information on DHCP accounting.
Step 10	Repeat Steps 6 and 7 for each configured DHCP pool.	--
Step 11	**exit** **Example:** `Router(dhcp-config)# exit`	Exits to global configuration mode.

Configuration Examples for DHCP Enhancements for Edge Session Management

DHCP Address Range and Class Name Configuration Example

The following example shows how to configure an address range for a particular network and class name for a DHCP pool.

```
ip dhcp pool abc-pool
 network 10.10.0.0 255.255.0.0
 class abc-pool
  address range 10.10.5.0 10.10.5.99
```

DHCP Server Co-Resident with SG Configuration Example

In the following example, the ISPs are ABC and DEF companies. The ABC company has its addresses assigned from an address pool that is dynamically allocated using ODAP. The DEF company has its customer addresses assigned from the address pool 10.100.0.0/16. Customers not associated with any ISP will have an address allocated from the address pool 10.1.0.0/16 and the lease time is set to 10 minutes.

```
!Interface configuration
interface ethernet1
 ip address 10.20.0.1. 255.255.0.0
 ip address 10.1.0.1 255.255.0.0 secondary
 ip address 10.100.0.1 255.255.0.0 secondary
!Address pool for ABC customers
ip dhcp pool abc-pool
 network 20.1.0.0 255.255.0.0
 class abc
!
!Address pool for DEF customers
ip dhcp pool def-pool
 network 10.100.0.0 255.255.0.0
 class def
!Address pool for customers without an ISP
ip dhcp pool temp
 network 10.1.0.0 255.255.0.0
 lease 0 0 10
 class default
```

DHCP Relay Agent Co-Resident with SG Configuration Example

In the following example, there are two ISPs: abcpool and defpool. The abcpool ISP and its customers are allowed to have addresses in the ranges 10.1.0.0/16 and 30.1.0.0/16 and are relayed to the DHCP server at 10.55.10.1. The defpool ISP and its customers are allowed to have addresses in the ranges 20.1.0.0/16 and 40.4.0.0/16 and are relayed to the DHCP server at 12.10.2.1.

```
!Address ranges:
interface ethernet1
 ip address 10.1.0.0 255.255.0.0
 ip address 10.2.0.0 255.255.0.0 secondary
interface ethernet2
 ip address 10.3.0.0 255.255.0.0
 ip address 10.4.0.0 255.255.0.0 secondary
```

```
!Address pools for abcpool1 and abcpool2:
ip dhcp pool abcpool1
 relay source 10.1.0.0 255.255.0.0
 class abcpool
  relay target 10.5.10.1
!Address pool for abcpool2:
ip dhcp pool abcpool2
 relay source 10.1.0.0 255.255.0.0
 class abcpool
  relay target 10.55.10.1
!Address pools for defpool1 and defpool2:
ip dhcp pool defpool1
 relay source 10.1.0.0 255.255.0.0
 class defpool
  relay target 10.10.2.1
ip dhcp pool defpool2
 relay source 10.4.0.0 255.255.0.0
 class defpool
  relay target 10.10.2.1
```

Multiple DHCP Pools and Different ISPs Configuration Example

The following example shows how to configure one interface and multiple DHCP pools that have different ISPs by using the **network** command.

```
interface ethernet1
 ip address 10.0.0.1 255.0.0.0
 ip address 10.1.0.1 255.0.0.0
!
ip dhcp pool x
 network 10.0.0.0 255.0.0.0
 class ISP1
!
ip dhcp pool y
 network 10.1.0.0 255.0.0.0
 class ISP2
```

Multiple Relay Sources and Destinations Configuration Example

In the following example, multiple relay sources and destinations may be configured for a relay pool. This is similar the ip helper-address configuration on multiple interfaces. Pools are matched to the (possibly multiple) IP addresses on an incoming interface in the order in which they appear when using the **show running-config** command to display information about that interface. Once either a relay is found or an address allocation is found, the search stops. For example, given the following configuration:

```
interface ethernet1
 ip address 10.0.0.1 255.0.0.0
 ip address 10.0.0.5 255.0.0.0 secondary
ip dhcp pool x
 relay source 10.0.0.0 255.0.0.0
 relay destination 10.0.0.1
ip dhcp pool y
 relay source 10.0.0.0 255.0.0.0
 relay destination 10.0.0.1
```

In the following example, the DHCP client packet would be relayed to 10.0.0.1, if the SG specified ISP1 as the class name, and would be relayed to 10.0.0.5, if the SG specified ISP2 as the class name.

```
interface ethernet1
 ip address 10.0.0.1 255.0.0.0
 ip address 10.0.0.5 255.0.0.0 secondary
ip dhcp pool x
 relay source 10.0.0.0 255.0.0.0
 relay destination 10.2.0.0 255.0.0.0
 class ISP1
```

```
 relay target 10.0.0.1
class ISP2
 relay target 10.0.0.5
```

SG-Supplied Class Name Configuration Example

In the following example, an SG-supplied class name is to be used in selecting the remote DHCP server to which packets should be relayed.

```
ip dhcp pool abc-pool-1
 relay source 10.1.0.0 255.255.0.0
 relay destination 10.1.0.0
 class classname1
  relay target 10.20.10.1
 class classname2
  relay target 10.0.10.1
 class classname3
```

In the example above, an SG-supplied class name, called classname1, would relay the DHCP DISCOVER packet to the server at the relay target IP address 10.20.10.1, while SG classname2 would relay the DHCP DISCOVER packet to the server at the relay target IP address 10.0.10.1. This configuration relays the packet to destination IP address 10.0.0.1, because the pool matches the first configured address on the interface. If the SG returns a classname3, then the default pool is the default address specified as the relay destination. If the SG returns any class name other than classname1, classname2, or classname3, then no relay action is taken.

Additional References

The following sections provide references related to configuring DHCP Enhancements for Edge-Session Management.

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 client configuration	“Configuring the Cisco IOS DHCP Client” module
DHCP relay agent configuration	“Configuring the Cisco IOS DHCP Relay Agent” module
DHCP server on-demand address pool manager configuration	“Configuring the DHCP Server On-Demand Address Pool Manager” module
DHCP advanced features	“Configuring DHCP Services for Accounting and Security” module

Related Topic	Document Title
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.	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*

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/techsupport

Feature Information for DHCP Enhancements for Edge-Session Management

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 26 Feature Information for DHCP Enhancements for Edge-Session Management

Feature Name	Releases	Feature Configuration Information
DHCP Relay Accounting	12.4(6)T	The DHCP Relay Accounting feature allows a Cisco IOS DHCP relay agent to send a RADIUS accounting start packet when an address is assigned to a client and a RADIUS accounting stop packet when the address is released. This feature is enabled by using the **accounting** command with relay pools that use the **relay destination** command in DHCP pool configuration mode. No new commands were introduced by this feature.

Feature Name	Releases	Feature Configuration Information
DHCP Enhancements for Edge-Session Management	12.3(14)T 12.2(28)SB 12.2(33)SRC	The DHCP Enhancements for Edge-Session Management feature provides the capability of simultaneous service by multiple ISPs to customers using one network infrastructure. The end-user customer may change ISPs at any time. The following commands were introduced by this feature: **relay destination**, **relay source**,and **relay target**.

ISSU and SSO--DHCP High Availability Features

Cisco IOS Release 12.2(31)SB2 introduces the following series of Dynamic Host Configuration Protocol (DHCP) High Availability features that support the Broadband Access Server (BRAS):

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

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

Finding Feature Information

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

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

Prerequisites for DHCP High Availability

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

Restrictions for DHCP High Availability

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

Information About DHCP High Availability

ISSU

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

SSO

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

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

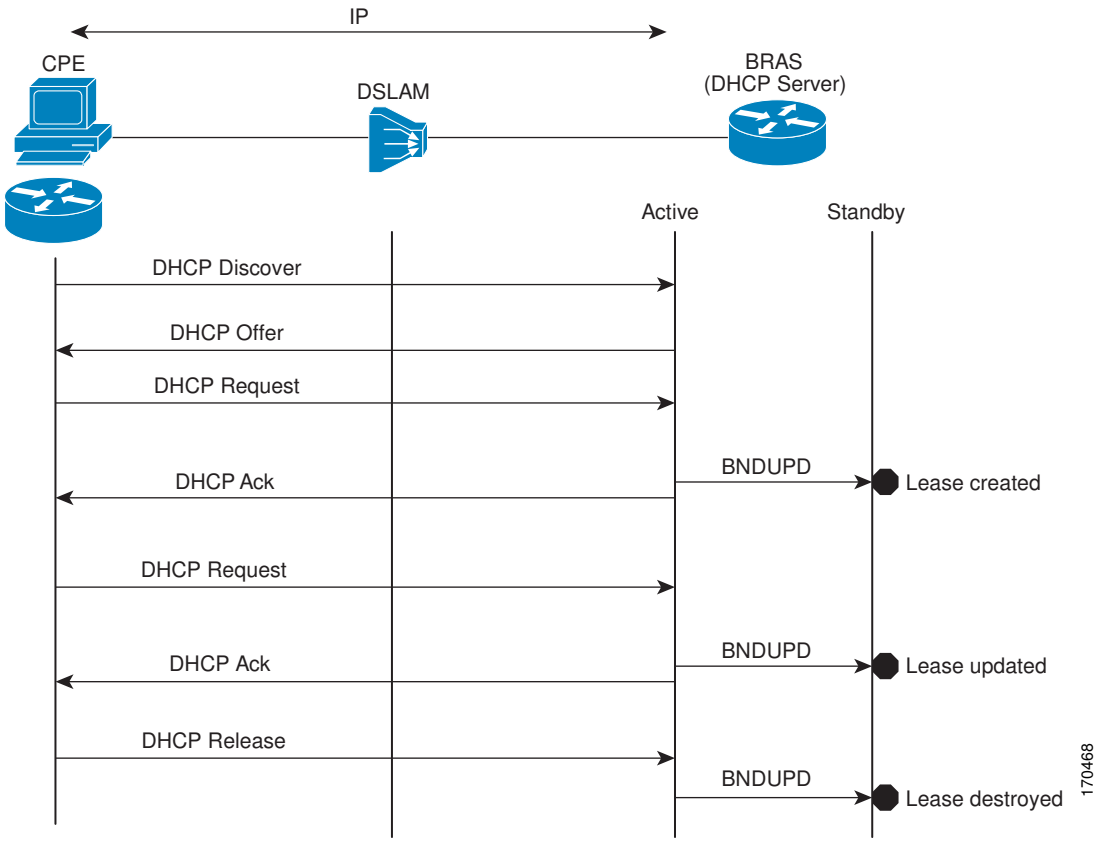
A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

ISSU and SSO--DHCP Server

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

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

Figure 14 DHCP Server Maintaining States Between the Active and Standby Route Processor



ISSU and SSO--DHCP Relay on Unnumbered Interface

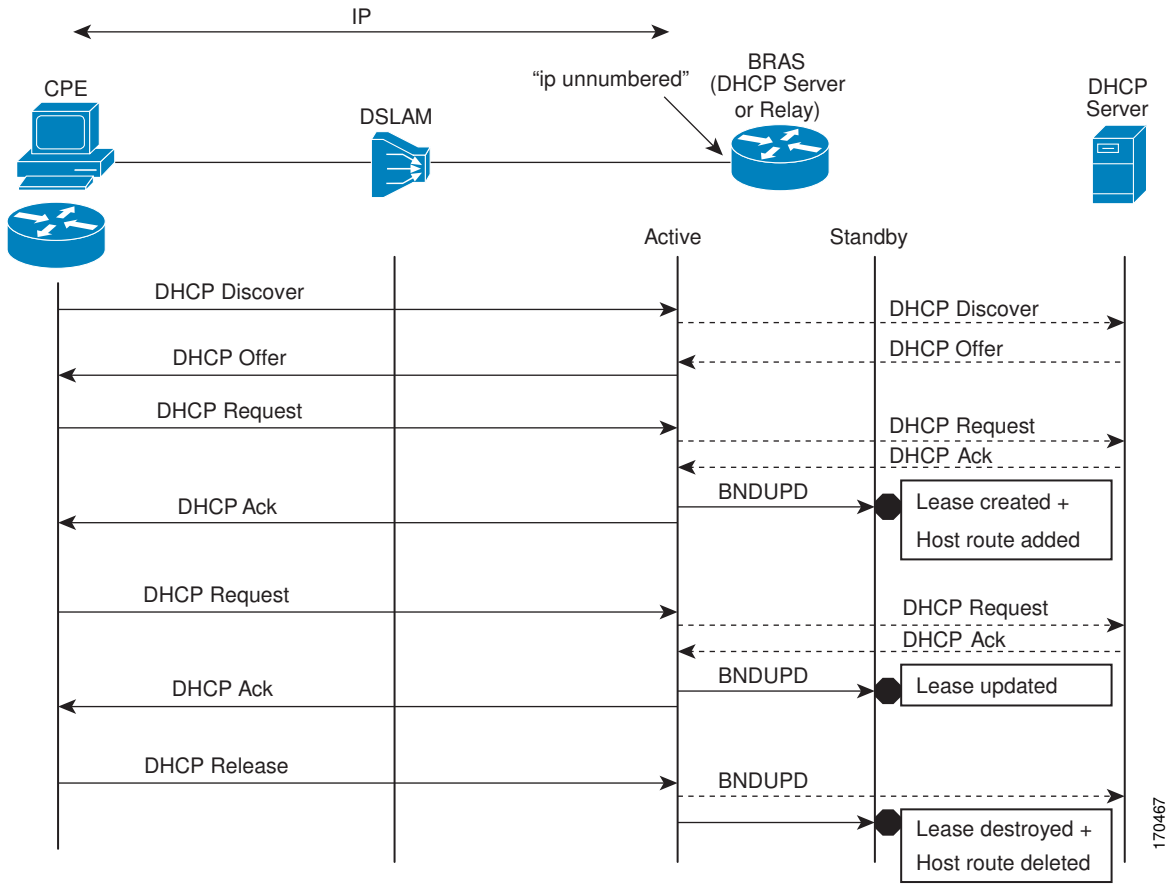
The DHCP relay agent supports the use of unnumbered interfaces. For DHCP clients connected through the unnumbered interfaces, the DHCP relay agent automatically adds a static host route once the DHCP client obtains an address, specifying the unnumbered interface as the outbound interface. The route is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

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

The ISSU and SSO DHCP relay on unnumbered interface functionality adds high availability support for host routes to clients connected through unnumbered interfaces. The DHCP relay agent can now detect

when a router is failing over to the standby RP and keep the states related to unnumbered interfaces. The figure below illustrates the process.

Figure 15 DHCP Maintaining States with an IP Unnumbered Interface

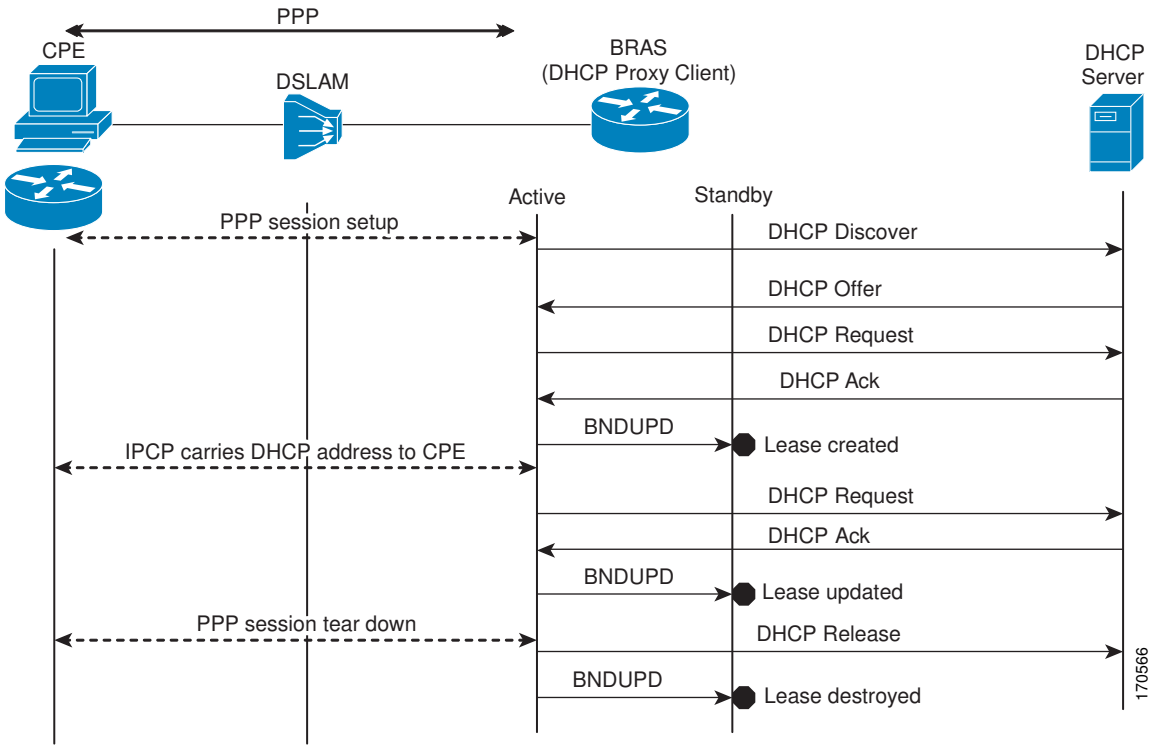


ISSU and SSO--DHCP Proxy Client

The DHCP proxy client enables the router to obtain a lease for configuration parameters from a DHCP server for a remote Point-to-Point Protocol (PPP) client. The DHCP proxy client that is ISSU and SSO

aware is able to request a lease from the DHCP server and the state of the lease is synchronized between the active and standby RP. The figure below illustrates the process.

Figure 16 DHCP Proxy Client Lease Synchronization

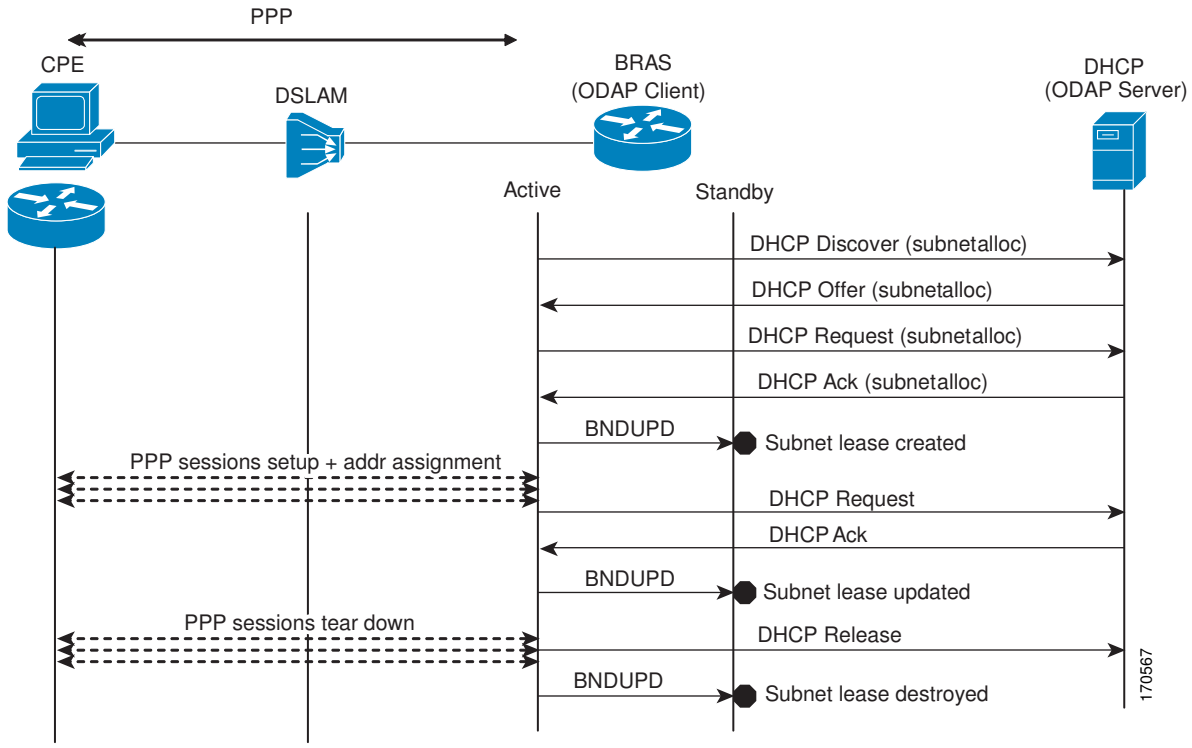


ISSU and SSO--DHCP ODAP Client and Server

The DHCP on-demand address pool (ODAP) client that is ISSU and SSO aware can request a lease for a subnet from the DHCP ODAP server. After the DHCP ODAP server allocates the subnet to the client, the state of the lease is synchronized between the active and standby RP through binding updates. Following a

switchover event, the DHCP ODAP client can continue to allocate IP addresses from the same subnets and also continue to renew the subnets from the DHCP ODAP server. The figure below illustrates the process.

Figure 17 ODAP Subnet Lease Synchronization



How to Configure DHCP High Availability

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

Configuration Examples for DHCP High Availability

There are no configuration examples for DHCP high availability features.

Additional References

Related Documents

Related Topic	Document Title
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP conceptual and configuration information	*Cisco IOS IP Addressing Services Configuration Guide, Release 12.2SR*
In-Service Software Upgrade process conceptual and configuration information	" Cisco IOS In Service Software Upgrade Process" module
Nonstop Forwarding conceptual and configuration information	"Cisco Nonstop Forwarding" module
Stateful switchover conceptual and configuration information	"Stateful Switchover" module

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS 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 High Availability Features

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

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

Table 27 Feature Information for DHCP High Availability Features

Feature Name	Releases	Feature Information
ISSU--DHCP Server	12.2(31)SB2 12.2(33)SRC Cisco IOS XE Release 2.1	The DHCP server has been enhanced to support ISSU.
SSO--DHCP Server	12.2(31)SB2 12.2(33)SRB Cisco IOS XE Release 2.1	The DHCP server has been enhanced to support SSO.
ISSU--DHCP Relay on Unnumbered Interface	12.2(31)SB2 12.2(33)SRC	The DHCP relay on unnumbered interface has been enhanced to support ISSU.
SSO--DHCP Relay on Unnumbered Interface	12.2(31)SB2 12.2(33)SRB	The DHCP relay on unnumbered interface has been enhanced to support SSO.
ISSU--DHCP Proxy Client	12.2(31)SB2 12.2(33)SRC	The DHCP proxy client has been enhanced to support ISSU.
SSO--DHCP Proxy Client	12.2(31)SB2 12.2(33)SRC	The DHCP proxy client has been enhanced to support SSO.

Feature Name	Releases	Feature Information
ISSU--DHCP ODAP Client and Server	12.2(31)SB2 12.2(33)SRC	The DHCP ODAP client and server have been enhanced to support ISSU.
SSO--DHCP ODAP Client and Server	12.2(31)SB2 12.2(33)SRC	The DHCP ODAP client and server have been enhanced to support SSO.

Glossary

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

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

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

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

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

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

Note See Internetworking Terms and Acronyms for terms not included in this glossary.

DHCP Option 82 Support for Routed Bridge Encapsulation

The DHCP Option 82 Support for Routed Bridge Encapsulation feature allows service providers to create a policy on a DHCP server to determine the number of IP addresses (number of bridging users) to be assigned to a particular ATM virtual path identifier/virtual channel identifier (VPI/VCI) port.

Finding Feature Information

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

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

Prerequisites for DHCP Option 82 Support for Routed Bridge Encapsulation

Configure the DHCP Option 82 Support feature on the DHCP relay agent using the **ip dhcp relay information option** command before configuring the DHCP Option 82 Support for Routed Bridge Encapsulation feature.

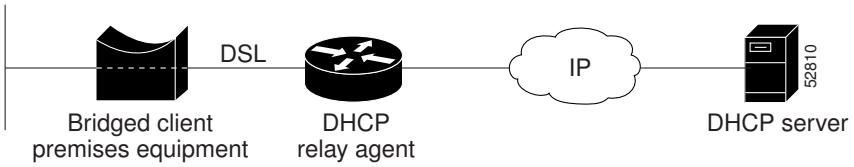
Information About DHCP Option 82 Support for Routed Bridge Encapsulation

DHCP Option 82 for Routed Bridge Encapsulation--Overview

The DHCP relay agent information option (option 82) enables a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.

The DHCP Option 82 Support for Routed Bridge Encapsulation feature provides support for the DHCP relay agent information option when ATM routed bridge encapsulation (RBE) is used. The figure below shows a typical network topology in which ATM RBE and DHCP are used. The aggregation router that is using ATM RBE is also serving as the DHCP relay agent.

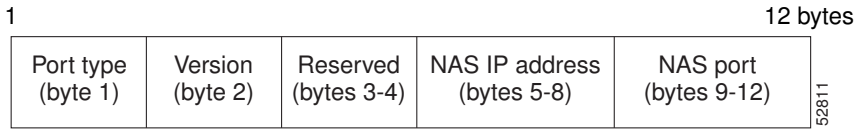
Figure 18 Network Topology Using ATM RBE and DHCP



The DHCP Option 82 Support for Routed Bridge Encapsulation feature communicates information to the DHCP server using a suboption of the DHCP relay agent information option called agent remote ID. The information sent in the agent remote ID includes an IP address identifying the relay agent and information about the ATM interface and the permanent virtual circuit (PVC) over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

The figure below shows the format of the agent remote ID suboption.

Figure 19 Format of the Agent Remote ID Suboption



The table below describes the agent remote ID suboption fields displayed in the figure above.

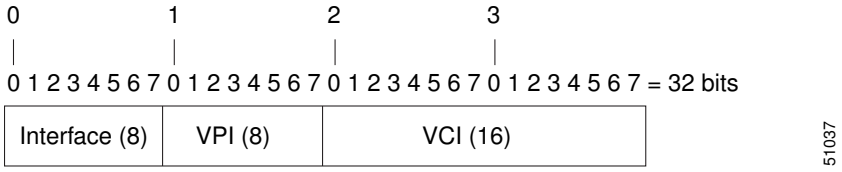
Table 28 Agent Remote ID Suboption Field Descriptions

Field	Description
Port type	Port type. The value 0x01 indicates RBE (1 byte).
Version	Option 82 version. The value 0x01 specifies the RBE version of option 82 (1 byte).

Field	Description
Reserved	Reserved (2 bytes).
NAS IP address	IP address of one of the interfaces on the DHCP relay agent. The **rbe nasip** command can be used to specify which IP address will be used (4 bytes).
NAS port	RBE-enabled virtual circuit on which the DHCP request has come in. See the figure below for the format of this field (4 bytes).

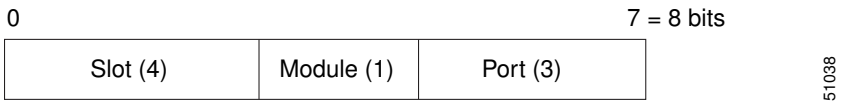
The figure below shows the format of the network access server (NAS) port field in the agent remote ID suboption.

Figure 20 Format of the NAS Port Field



The figure below shows the format of the interface field. If there is no module, the value of the module bit is 0.

Figure 21 Format of the Interface Field



- Benefits, page 251

Benefits

The DHCP Option 82 Support for Routed Bridge Encapsulation feature enables the service providers to use DHCP to assign IP addresses and DHCP option 82 to implement security and IP address assignment policies.

How to Configure DHCP Option 82 Support for Routed Bridge Encapsulation

- Configuring the DHCP Option 82 Support for Routed Bridge Encapsulation Feature, page 252

Configuring the DHCP Option 82 Support for Routed Bridge Encapsulation Feature

Perform this task to configure the DHCP Option 82 Support for Routed Bridge Encapsulation feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp relay information option**
4. **rbe nasip** *interface-type number*
5. **exit**
6. **more system:running-config**

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 relay information option** **Example:** `Router(config)# ip dhcp relay information option`	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.
Step 4	**rbe nasip** *interface-type number* **Example:** `Router(config)# rbe nasip GigabitEthernet 1/1`	Specifies the IP address of an interface on the DHCP relay agent that will be sent to the DHCP server via the agent remote ID suboption.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**more system:running-config** **Example:** `Router# more system:running-config`	(Optional) Displays the running configuration.

Configuration Examples for DHCP Option 82 Support for Routed Bridge Encapsulation

Example DHCP Option 82 Support for Routed Bridge Encapsulation

The following example shows how to enable DHCP option 82 support on the DHCP relay agent using the **ip dhcp relay information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server.

```
ip dhcp-server 172.16.1.2
!
ip dhcp relay information option
!
interface Loopback0
 ip address 10.1.1.129 255.255.255.192
!
interface ATM 4/0
 no ip address
!
interface ATM 4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 172.16.1.2
 atm route-bridged ip
 pvc 88/800
  encapsulation aal5snap
!
!
interface Ethernet 5/1
 ip address 172.16.1.1 255.255.0.0
!
router eigrp 100
 network 10.1.0.0
 network 172.16.0.0
!
rbe nasip Loopback 0
```

For this configuration example, the value (in hexadecimal) of the agent remote ID suboption is 010100000B01018140580320. The table below shows the value of each field within the agent remote ID suboption.

Table 29 Agent Remote ID Suboption Field Values

Agent Remote ID Suboption Field	Value
Port type	0x01
Version	0x01
Reserved	Undefined
NAS IP address	0x0B010181 (hexadecimal value of 11.1.1.129)
NAS port • Interface (slot/module/port) • VPI • VCI	• 0x40 (The slot/module/port values are 01 00/0/000.) • 0x58 (hexadecimal value of 88) • 0x320 (hexadecimal value of 800)

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
DHCP Commands	*Cisco IOS IP Addressing Services Command Reference*
DHCP Configuration	*Cisco IOS IP Addressing Services Configuration Guide*
Cisco IOS Wide-Area Networking Commands	*Cisco IOS Wide-Area Networking Command Reference*
Cisco IOS Wide-Area Networking Configuration	*Cisco IOS Wide-Area Networking Configuration Guide*

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 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

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

Technical Assistance

Description	Link
The Cisco Support 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 Option 82 Support for Routed Bridge Encapsulation

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 30 Feature Information for DHCP Option 82 Support for Routed Bridge Encapsulation

Feature Name	Releases	Feature Information
DHCP Option 82 Support for Routed Bridge Encapsulation	15.1(1)S 12.2(28)SB 12.2(2)T	The DHCP Option 82 Support for Routed Bridge Encapsulation feature allows service providers to create a policy on a DHCP server to determine the number of IP addresses (number of bridging users) to be assigned to a particular ATM VPI/VCI port. The following command was introduced or modified: **rbe nasip**.