IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)

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

CHAPTER 1 **Configuring the Cisco IOS DHCP Server** 1

- Finding Feature Information 1
- Prerequisites for Configuring the DHCP Server 1
- Information About the Cisco IOS DHCP Server 2
  - Overview of the DHCP Server 2
  - DHCP Attribute Inheritance 2
  - DHCP Server Address Allocation Using Option 82 2
- How to Configure the Cisco IOS DHCP Server 4
  - Configuring a DHCP Database Agent or Disabling Conflict Logging 4
  - Excluding IP Addresses 6
  - Configuring DHCP Address Pools 7
    - Configuring a DHCP Address Pool 7
    - Configuring a DHCP Address Pool with Secondary Subnets 11
    - Troubleshooting Tips 16
    - Verifying the DHCP Address Pool Configuration 16
  - Configuring Manual Bindings 18
    - Troubleshooting Tips 20
  - Configuring DHCP Static Mapping 21
    - Configuring the DHCP Server to Read a Static Mapping Text File 22
  - Customizing DHCP Server Operation 25
  - Configuring a Remote Device to Import DHCP Server Options from a Central DHCP Server 26
    - Configuring the Central DHCP Server to Update DHCP Options 26
    - Configuring the Remote Device to Import DHCP Options 28
  - Configuring DHCP Address Allocation Using Option 82 29
    - Enabling Option 82 for DHCP Address Allocation 29
    - Troubleshooting Tips 30
    - Defining the DHCP Class and Relay Agent Information Patterns 30

Troubleshooting Tips 32
Defining the DHCP Address Pool 32
Configuring a Static Route with the Next-Hop Dynamically Obtained Through DHCP 33
Clearing DHCP Server Variables 35
Configuration Examples for the Cisco IOS DHCP Server 36
Example: Configuring the DHCP Database Agent 36
Example: Excluding IP Addresses 36
Example: Configuring DHCP Address Pools 37
Example: Configuring a DHCP Address Pool with Multiple Disjoint Subnets 38
Example: Configuring Manual Bindings 39
Example: Configuring Static Mapping 40
Example: Configuring the Option to Ignore all BOOTP Requests 40
Example: Importing DHCP Options 41
Example: Configuring DHCP Address Allocation Using Option 82 42
Example: Configuring a Static Route with the Next-Hop Dynamically Obtained Through DHCP 43
Additional References for Cisco IOS DHCP Server 43
Feature Information for the Cisco IOS DHCP Server 44

CHAPTER 2 **IPv6 Access Services: DHCPv6 Prefix Delegation 47**
Finding Feature Information 47
Information About IPv6 Access Services: DHCPv6 Prefix Delegation 47
DHCPv6 Prefix Delegation 47
Node Configuration Without Prefix Delegation 48
Client and Server Identification 48
Rapid Commit 48
DHCPv6 Client, Server, and Relay Functions 48
Client Function 49
Server Function 49
How to Configure IPv6 Access Services: DHCPv6 Prefix Delegation 53
Configuring the DHCPv6 Server Function 53
Configuring the DHCPv6 Configuration Pool 53
Configuring a Binding Database Agent for the Server Function 55
Configuring the DHCPv6 Client Function 55
Deleting Automatic Client Bindings from the DHCPv6 Binding Table 57

Configuration Examples for IPv6 Access Services: DHCPv6 Prefix Delegation 57
Examples: Configuring the DHCPv6 Server Function 57
Example: Configuring the DHCPv6 Configuration Pool 59
Example: Configuring the DHCPv6 Client Function 59
Example: Configuring a Database Agent for the Server Function 60
Example: Displaying DHCP Server and Client Information on the Interface 60
Additional References 61
Feature Information for IPv6 Access Services: DHCPv6 Prefix Delegation 62

CHAPTER 3 IPv6 Access Services: DHCPv6 Relay Agent 63
Finding Feature Information 63
Information About IPv6 Access Services: DHCPv6 Relay Agent 63
DHCPv6 Relay Agent 63
DHCPv6 Relay Agent Notification for Prefix Delegation 65
DHCPv6 Relay SSO and ISSU 65
DHCPv6 Relay Options: Remote ID for Ethernet Interfaces 66
DHCPv6 Relay Options: Reload Persistent Interface ID Option 66
How to Configure IPv6 Access Services: DHCPv6 Relay Agent 67
Configuring the DHCPv6 Relay Agent 67
Configuration Examples for IPv6 Access Services: DHCPv6 Relay Agent 68
Example: Configuring the DHCPv6 Relay Agent 68
Additional References 68
Feature Information for IPv6 Access Services: DHCPv6 Relay Agent 69

CHAPTER 4 DHCP Client 71
Finding Feature Information 71
Restrictions for the DHCP Client 71
Information About the DHCP Client 72
DHCP Client Operation 72
DHCP Client Overview 72
How to Configure the DHCP Client 73
Configuring the DHCP Client 73
Configuration Examples for the DHCP Client 75
Example: Configuring the DHCP Client 75
Additional References 75

Feature Information for the DHCP Client 76

CHAPTER 5 DHCPv6 Server Stateless Autoconfiguration 77

Finding Feature Information 77

Information About DHCPv6 Server Stateless Autoconfiguration 77

DHCPv6 Server Stateless Autoconfiguration 77

How to Configure DHCPv6 Server Stateless Autoconfiguration 79

Configuring the Stateless DHCPv6 Server 79

Configuring the Stateless DHCPv6 Client 81

Enabling Processing of Packets with Source Routing Header Options 82

Configuration Examples for DHCPv6 Server Stateless Autoconfiguration 83

Example: Configuring the Stateless DHCPv6 Function 83

Additional References for DHCP Overview 83

Feature Information for DHCPv6 Server Stateless Autoconfiguration 84

CHAPTER 6 DHCPv6 Server Timer Options 87

Finding Feature Information 87

Information About DHCPv6 Server Timer Options 87

Information Refresh Server Option 87

NIS- and NIS+-Related Server Options 88

SNTP Server Option 88

How to Configure DHCPv6 Server Timer Options 88

Configuring the Information Server Refresh Option 88

Importing the Information Server Refresh Option 89

Configuring NIS- and NISP-Related Server Options 90

Importing NIS- and NIS+-Related Server Options 92

Configuring the SNTP Server Option 93

Importing the SNTP Server Option 94

Configuration Examples for DHCPv6 Server Timer Options 95

Example: Configuring DHCPv6 Server Timer Options 95

Additional References 95

Feature Information for DHCPv6 Server Timer Options 96

CHAPTER 7 DHCPv6 Individual Address Assignment 99

Finding Feature Information 99

Prerequisites for Configuring DHCPv6 Address Assignment 99
Information About DHCPv6 Individual Address Assignment 100
DHCPv6 Address Assignment 100
How to Configure DHCPv6 Individual Address Assignment 100
Enabling the DHCPv6 Server Function on an Interface 100
Enabling the DHCPv6 Client Function on an Interface 103
Configuration Examples for DHCPv6 Individual Address Assignment 105
Examples: Configuring the DHCPv6 Server Function 105
Example: Configuring the DHCPv6 Client Function 106
Additional References 106
Feature Information for DHCPv6 Individual Address Assignment 107

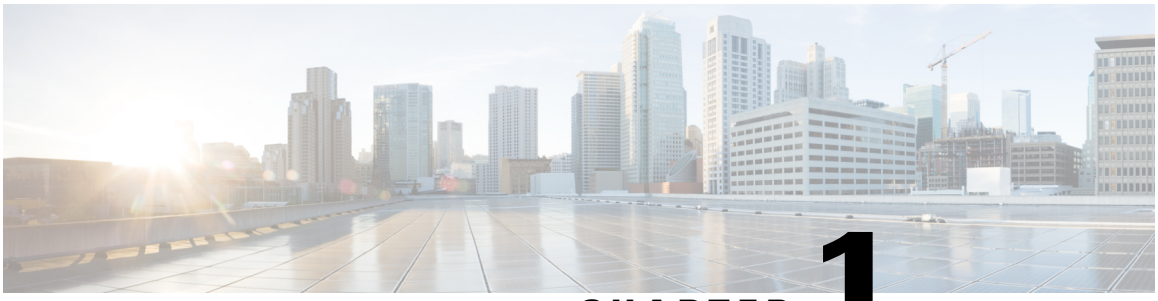
CHAPTER 8 DHCPv6 Ethernet Remote ID Option 109
Finding Feature Information 109
Information About DHCPv6 Ethernet Remote ID Option 109
DHCPv6 Ethernet Remote ID Option Overview 109
Restrictions for DHCPv6 Ethernet Remote ID Option 110
Additional References for DHCPv6 Ethernet Remote ID Option 110
Feature Information for DHCPv6 Ethernet Remote ID Option 111

CHAPTER 9 DHCPv6 Relay—Reload Persistent Interface ID Option 113
Finding Feature Information 113
Information About DHCPv6 Relay—Reload Persistent Interface ID Option 114
DHCPv6 Relay—Reload Persistent Interface ID Option Overview 114
Additional References for DHCPv6 Relay—Reload Persistent Interface ID Option 114
Feature Information for DHCPv6 Relay—Reload Persistent Interface ID Option 115

CHAPTER 10 DHCP Server Port-Based Address Allocation 117
Finding Feature Information 117
Restrictions for DHCP Server Port-Based Address Allocation 117
Information About DHCP Server Port-Based Address Allocation 118
DHCP Server Port-Based Address Allocation Feature Design 118
How to Configure DHCP Server Port-Based Address Allocation 119
Automatically Generating a Subscriber Identifier for a DHCP Message Received on a Port 119
Troubleshooting Tips 120

Preassigning IP Addresses and Associating Them to a Client 120
Preassigning IP Addresses and Associating Them to a Client 122
Configuration Examples for DHCP Server Port-Based Address Allocation 123
DHCP Server Port-Based Address Allocation Example 123
Additional References 124
Feature Information for DHCP Server Port-Based Address Allocation 125

CHAPTER 11 DHCPv6 Repackaging 127
Finding Feature Information 127
Information About DHCPv6 Repackaging 128
DHCPv6 Prefix Delegation 128
Node Configuration Without Prefix Delegation 128
DHCPv6 Address Assignment 128
How to Configure DHCPv6 Repackaging 129
Configuring DHCPv6 Address Assignment 129
Prerequisites for Configuring DHCPv6 Address Assignment 129
Enabling the DHCPv6 Server Function on an Interface 129
Enabling the DHCPv6 Client Function on an Interface 132
Configuring the Stateless DHCPv6 Function 133
Configuring the Stateless DHCPv6 Server 134
Configuring the Stateless DHCPv6 Client 135
Enabling Processing of Packets with Source Routing Header Options 136
Configuration Examples for DHCPv6 Repackaging 137
Examples: Configuring the DHCPv6 Server Function 137
Example: Configuring the DHCPv6 Client Function 139
Example: Configuring the Stateless DHCPv6 Function 139
Additional References 140
Feature Information for DHCPv6 Repackaging 140



CHAPTER 1

Configuring the Cisco IOS DHCP Server

Cisco devices running Cisco software include Dynamic Host Configuration Protocol (DHCP) server and the 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 device 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 device.

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

- Finding Feature Information, page 1
- Prerequisites for Configuring the DHCP Server, page 1
- Information About the Cisco IOS DHCP Server, page 2
- How to Configure the Cisco IOS DHCP Server, page 4
- Configuration Examples for the Cisco IOS DHCP Server, page 36
- Additional References for Cisco IOS DHCP Server, page 43
- Feature Information for the Cisco IOS DHCP Server, page 44

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 a Cisco Dynamic Host Control Protocol (DHCP) server, you must understand the concepts documented in the Overview of the DHCP Server section.

- The Cisco DHCP server and the relay agent services are enabled by default. Use the **no service dhcp** command to disable the Cisco DHCP server and the relay agent and the **service dhcp** command to reenable the functionality.
- Port 67 (the DHCP server port) is closed in the Cisco DHCP/BOOTP default configuration. There are two logical parts to the **service dhcp** command: service enabled and service running. The DHCP service is enabled by default, but port 67 does not open until the DHCP service is running. If the DHCP service is running, the **show ip sockets details** or the **show sockets detail** command displays port 67 as open.
- The Cisco DHCP relay agent is enabled on an interface only when you configure the **ip helper-address** command. This command enables a DHCP broadcast to be forwarded to the configured DHCP server.

Information About the Cisco IOS DHCP Server

Overview of the DHCP Server

The Cisco DHCP server accepts address assignment requests and renewals from the client and assigns the addresses from predefined groups of addresses 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 Domain Name System (DNS) server, the default device, and other configuration parameters. The Cisco 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) sent by the relay agent.

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 are also called options. Option 82 is organized as a single DHCP option that contains information known by the relay agent.

Automatic DHCP address allocation is based on an IP address. This IP address can either be the gateway address (giaddr field of the DHCP packet) or the IP address of an incoming interface. 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 DHCP relay agent can 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 to provide additional information to properly allocate IP addresses to DHCP clients. The information sent via option 82 is used to identify the port where the DHCP request arrives. Automatic DHCP address allocation does not parse out the individual suboptions contained in option 82. Rather, the address allocation is done by matching a configured pattern byte by byte.

This 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.

For example, DHCP clients are connected to two ports of a single switch. Each port can be configured to be a part of two VLANs: VLAN1 and VLAN2. DHCP clients belong to either VLAN1 or VLAN2 and 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) have the giaddr field set to the same value indicating the subnet of the VLAN.

Problems can occur while allocating IP addresses to DHCP clients that are connected to different ports of the same VLAN. These IP addresses must be part of the same subnet but the range of IP addresses must be different. In the preceding example, when a DHCP client that is connected to a port of VLAN1 must be allocated an IP address from a range of IP addresses within the VLAN's subnet, whereas a DHCP client connecting to port 2 of VLAN1 must be allocated an IP address from another range of IP addresses. The two range of IP addresses are part of the same subnet (and have the same subnet mask). Generally, during DHCP address allocation, the DHCP server refers only to the giaddr field and is unable 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 inspects both the giaddr field and the inserted option 82 during the address selection process.

When you enable option 82 on a device, the following sequence of events occurs:

1. The host (DHCP client) generates a DHCP request and broadcasts it on the network.
2. When the device receives the DHCP request, it adds the option 82 information in the packet. The option 82 information contains the device MAC address (the remote ID suboption) and the port identifier, vlan-mod-port, from which the packet is received (the circuit ID suboption).
3. The device adds the IP address of the relay agent to the DHCP packet.
4. The device forwards the DHCP request that includes the option 82 field to the DHCP server.
5. The DHCP server receives the packet. If the server is option 82 capable, it uses the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. The DHCP server echoes the option 82 field in the DHCP reply.
6. The DHCP server unicasts the reply to the device if the request is relayed to the server by the device. The device verifies that it originally inserted the option 82 data by inspecting remote ID and possibly circuit ID fields. The device removes the option 82 field and forwards the packet to the interface that connects to the DHCP client that sent the DHCP request.

The Cisco software refers to a pool of IP addresses (giaddr or incoming interface IP address) and matches 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 is configured with one or more DHCP classes, the pool becomes a restricted access pool, which means that no addresses are allocated from the pool unless one or more classes in the pool matches. This design allows DHCP classes to be used either for access control (no default class is configured on the pool) or to provide further address range partitions within 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 new relay agent information configuration mode.
- Support for bit-masking the raw relay information hexadecimal value.
- Support for a wildcard at the end of a 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** command. This configuration prevents the server from dropping the DHCP message.

How to Configure the Cisco IOS DHCP Server

Configuring a DHCP Database Agent or Disabling Conflict Logging

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

Automatic bindings are IP addresses that are 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 in 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 by using ping and gratuitous Address Resolution Protocol (ARP). If a conflict is detected, the address is removed from the pool. The address is not assigned until the administrator resolves the conflict.

Note We strongly recommend using database agents. However, the Cisco DHCP server can run without database agents. 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 a conflict logging but no database agent is configured, bindings during a switchover are lost when a device reboots. Possible false conflicts can occur causing the address to be removed from the address pool.

SUMMARY STEPS

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

DETAILED STEPS

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

Step 3	Do one of the following:
	• **ip dhcp database** *url* [**timeout** *seconds* | **write-delay** *seconds*]
	• **no ip dhcp conflict logging**
	
	Example:
	`Device(config)# ip dhcp database ftp://user:password@172.16.1.1/router-dhcp timeout 80`
	
	Example:
	`Device(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.

Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Excluding IP Addresses

The IP address configured on a device 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 must exclude addresses from the pool if the DHCP server does not allocate those IP addresses to DHCP clients. Consider a scenario where two DHCP servers are set up for the same network segment (subnet) for redundancy. If DHCP servers do not coordinate their services with each other using a protocol such as DHCP failover, each DHCP server must be configured to allocate addresses from a nonoverlapping set of addresses in the shared subnet. See the Example: Configuring Manual Bindings section for a configuration example.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp excluded-address** *low-address* [*high-address*] **Example:** `Device(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.103`	Specifies IP addresses that the DHCP server should not assign to DHCP clients.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring DHCP Address Pools

Configuring 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 string (such as “engineering”) or an integer (such as 0). Configuring a DHCP address pool also puts the device 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 device 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 the DHCP address pool to use for a client request is described in the Configuring Manual Bindings section.

The DHCP server identifies and uses DHCP address pools for a client request, in the following manner:

- If the client is not directly connected to the DHCP server (the giaddr field of the DHCPDISCOVER broadcast message is nonzero), the server matches the DHCPDISCOVER with the DHCP pool that has the subnet that contains the IP address in the giaddr field.
- If the client is directly connected to the DHCP server (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, 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 DHCP server software supports advanced capabilities for IP address allocation. See the Configuring DHCP Address Allocation Using Option 82 section for more information.

Before You Begin

Before you configure the DHCP address pool, you must:

- Identify DHCP options for devices where necessary, including the following:
  - Default boot image name
  - Default devices
  - Domain Name System (DNS) servers
  - Network Basic Input/Output System (NetBIOS) name server
  - Primary subnet
  - Secondary subnets and subnet-specific default device 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 the Configuring Manual Bindings section.

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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Device(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:** `Device(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:** `Device(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:** `Device(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:** `Device(dhcp-config)# domain-name cisco.com`	Specifies the domain name for the client.
Step 8	**dns-server** *address* [*address2 ... address8*] **Example:** `Device(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. • Servers should be listed in order of preference.
Step 9	**bootfile** *filename* **Example:** `Device(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 that the client uses to load.
Step 10	**next-server** *address* [*address2 ... address8*] **Example:** `Device(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. • One address is required; however, you can specify up to eight addresses in one command line.

	Command or Action	Purpose
		• If multiple servers are specified, DHCP assigns them to clients in a 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:** `Device(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:** `Device(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:** `Device(dhcp-config)# default-router 172.16.1.100 172.16.1.101`	(Optional) Specifies the IP address of the default device 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 devices are listed in order of preference; that is, *address* is the most preferred device, *address2* is the next most preferred device, and so on. • When a DHCP client requests an IP address, the device—acting as a DHCP server—accesses the default device list to select another device that the DHCP client will use as the first hop for forwarding messages. After a DHCP client has booted, the client begins sending packets to its default device.
Step 14	**option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*} **Example:** `Device(dhcp-config)# option 19 hex 01`	(Optional) Configures DHCP server options.
Step 15	**lease** {*days* [*hours* [*minutes*]] | **infinite**} **Example:** `Device(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.

	Command or Action	Purpose
Step 16	**end** **Example:** `Device(dhcp-config)# end`	Returns to privileged EXEC mode.

Configuring 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 device uses to allocate an IP address to a DHCP client. The DHCP server multiple subnet functionality enables a Cisco 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 device in DHCP pool secondary subnet configuration mode—identified by the (config-dhcp-subnet-secondary)# prompt—where 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 an available IP address in the primary subnet.
- When the primary subnet is exhausted, the DHCP server automatically looks for an available IP address in any of the 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 of subnets that were added to the pool.
- If the giaddr matches a secondary subnet in the pool, the DHCP server allocates an IP address from that particular secondary subnet (even if IP addresses are available in the primary subnet and irrespective of the order of secondary subnets that were 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* | */prefix-length*] [**secondary**]
17. **override default-router** *address* [*address2 ... address8*]
18. **override utilization high** *percentage-number*
19. **override utilization low** *percentage-number*
20. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Device(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:** `Device(dhcp-config)# utilization mark high 80 log`	(Optional) Configures the high utilization mark of the current address pool size. • The **log** keyword enables logging of a system message. A system message is generated for a DHCP pool when the pool utilization exceeds the configured high utilization threshold.
Step 5	**utilization mark low** *percentage-number* [**log**] **Example:** `Device(dhcp-config)# utilization mark low 70 log`	(Optional) Configures the low utilization mark of the current address pool size. • The **log** keyword enables logging of a system message. A system message is 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:** `Device(dhcp-config)# network 172.16.0.0 /16`	Specifies the subnet network number and mask of the primary DHCP address pool.
Step 7	**domain-name** *domain* **Example:** `Device(dhcp-config)# domain-name cisco.com`	Specifies the domain name for the client.
Step 8	**dns-server** *address* [*address2 ... address8*] **Example:** `Device(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. • Servers should be listed in the order of preference.
Step 9	**bootfile** *filename* **Example:** `Device(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 image that the client loads.
Step 10	**next-server** *address* [*address2 ... address8*] **Example:** `Device(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. • One IP address is required; however, you can specify up to eight IP addresses in one command line.

	Command or Action	Purpose
		• If multiple servers are specified, DHCP assigns the servers to clients in a 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:** `Device(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:** `Device(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:** `Device(dhcp-config)# default-router 172.16.1.100 172.16.1.101`	(Optional) Specifies the IP address of the default device 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 devices are listed in order of preference; that is, *address* is the most preferred device, *address2* is the next most preferred device, and so on. • When a DHCP client requests for an IP address, the device—acting as a DHCP server—accesses the default device list to select another device that the DHCP client uses as the first hop for forwarding messages. After a DHCP client has booted, the client begins sending packets to its default device.
Step 14	**option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*} **Example:** `Device(dhcp-config)# option 19 hex 01`	(Optional) Configures DHCP server options.
Step 15	**lease** {*days* [*hours*] [*minutes*] | **infinite**} **Example:** `Device(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.

	Command or Action	Purpose
Step 16	**network** *network-number* [*mask* | */prefix-length*] [**secondary**] **Example:** `Device(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 a DHCP server address pool. • During execution of this command, the configuration mode changes to DHCP pool secondary subnet configuration mode, which is identified by (config-dhcp-subnet-secondary)# prompt. In this mode, the administrator can configure a default device list that is specific to the subnet. • See Troubleshooting Tips section if you are using secondary IP addresses under a loopback interface with DHCP secondary subnets.
Step 17	**override default-router** *address* [*address2 ... address8*] **Example:** `Device(config-dhcp-subnet-secondary)# override default-router 10.10.0.100 10.10.0.101`	(Optional) Specifies the default device list that is used when an IP address is assigned to a DHCP client from a particular secondary subnet. • If the subnet-specific override value is configured, this override value is used when assigning an IP address from the subnet; the network-wide default device list is used only to set the gateway device for the primary subnet. • If this subnet-specific override value is not configured, the network-wide default device list is used when assigning an IP address from the subnet. • See Example: Configuring a DHCP Address Pool with Multiple Disjoint Subnets section for a sample configuration.
Step 18	**override utilization high** *percentage-number* **Example:** `Device(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** command.
Step 19	**override utilization low** *percentage-number* **Example:** `Device(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** command.
Step 20	**end** **Example:** `Device(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 using 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

The following configuration commands are optional. You can enter the **show** commands in any 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip dhcp pool** [*name*] **Example:** `Device# show ip dhcp pool`	(Optional) Displays information about DHCP address pools.
Step 3	**show ip dhcp binding** [*address*] **Example:** `Device# 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 is not exhausted. If necessary, recreate 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:** `Device# show ip dhcp conflict`	(Optional) Displays a list of all IP address conflicts.
Step 5	**show ip dhcp database** [*url*] **Example:** `Device# 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:** `Device# 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 are manually mapped to MAC addresses of hosts that are found in the DHCP database. Manual bindings are stored in the NVRAM of the DHCP server. Manual bindings are just special address pools. There is no limit to 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 MAC addresses of hosts that are found in the DHCP database. Because the bindings are stored in the volatile memory of the DHCP server, binding information is lost in the event of power failures or on device reloads. To prevent the loss of automatic binding information, a copy of the automatic binding information is stored on a remote host called the DHCP database agent. The bindings are periodically written to the database agent. When the device reloads, the bindings are read from the database agent to the DHCP database in the DHCP server.

Note We strongly recommend that you use database agents. However, Cisco DHCP server can function even 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** command with the hexadecimal values that identify the DHCP client. To configure manual bindings for clients that do not send a client identifier option, you must enter the **hardware-address** DHCP pool configuration command with the hexadecimal hardware address of the client.

Depending on your release, the DHCP server sends infinite lease time to the clients for which manual bindings are configured.

Depending on your release, the DHCP server sends lease time that is configured using the **lease** command to 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*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Device(config)# ip dhcp pool pool1`	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.
Step 4	**host** *address* [*mask*	*/prefix-length*] **Example:** `Device(dhcp-config)# host 172.16.0.1`	Specifies the IP address and subnet mask of the client. • There is no limit to the number of manual bindings you can configure. However, you can configure only one manual binding per host pool.
Step 5	**client-identifier** *unique-identifier* **Example:** `Device(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. You can specify the unique identifier for the client in either of the following ways: • A 7-byte dotted hexadecimal notation. For example, 01b7.0813.8811.66, where 01 represents the Ethernet media type and the remaining bytes represent the MAC address of the DHCP client.

	Command or Action	Purpose
		• A 27-byte dotted hexadecimal notation. For example, 7665.6e64.6f72.2d30.3032.342e.3937.6230.2e33.3734.312d.4661.302f.31. The equivalent ASCII string for this hexadecimal value is vendor-0024.97b0.3741-fa0/1, where vendor represents the vendor, 0024.97b0.3741 represents the MAC address of the source interface, and fa0/1 represents the source interface of the DHCP client. • See the Troubleshooting section for information about how to determine the client identifier of the DHCP client. **Note** The identifier specified here is considered for a DHCP client that sends a client identifier in the packet.
Step 6	**hardware-address** *hardware-address* [*protocol-type* | *hardware-number*] **Example:** `Device(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 a DHCP client that does not send a client identifier in the packet.
Step 7	**client-name** *name* **Example:** `Device(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.
Step 8	**end** **Example:** `Device(dhcp-config)# end`	Returns to privileged EXEC mode.

Troubleshooting Tips

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

```
Device# 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 the 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.

A DHCP database contains the mappings between a client IP address and the hardware address, which is 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 device 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 device 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, manual (or 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 to the number of addresses that can be stored in the file. The file format has the following elements:

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

See the following table 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 1: Static Mapping Text File Field Descriptions

Field	Description
time	Specifies the time the file was created. This field allows DHCP to differentiate between the new and old database versions when multiple agents are configured. The valid format of the time is mm dd yyyy hh:mm AM/PM.
version 2	Specifies the database version number.
IP address	Specifies the static IP address. If the subnet mask is not specified, a mask is automatically assigned depending on the IP address. The IP address and the mask is separated by a space.
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, the type 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," the type refers to a match on the client identifier. For more information about the client identifier, 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. If you are unsure about the client identifier to match with the hardware type, 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

Before You Begin

The administrator must 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 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Device(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 the **service dhcp** command.
Step 4	**origin file** *url* **Example:** `Device(dhcp-config)# origin file tftp://10.1.0.1/static-bindings`	Specifies the URL that the DHCP server can access to locate the text file.
Step 5	**end** **Example:** `Device(dhcp-config)# end`	Returns to privileged EXEC mode.

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

Examples

The following sample output from the **show ip dhcp binding** command displays address bindings that are configured:

```
Device# 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 output displays 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:

```
Device# 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 for 2 seconds before timing out a ping packet.

You can configure the DHCP server to ignore and not reply to any BOOTP requests that the server receives. 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 DHCP server servicing the network segment. The BOOTP server is configured with static bindings for the BOOTP clients and the BOOTP clients must obtain their addresses from the BOOTP server. However, DHCP servers can also respond to BOOTP requests and the DHCP server may offer an address that causes 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 ensures that the BOOTP clients will receive address information from the BOOTP server and will not accept an address from a DHCP server.

Cisco software can forward these ignored BOOTP request packets to another DHCP server if the **ip helper-address** 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**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp ping packets** *number* **Example:** `Device(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.

	Command or Action	Purpose
		• The default is two packets. Setting the *number* argument to a value of 0 disables the DHCP server ping operation.
Step 4	**ip dhcp ping timeout** *milliseconds* **Example:** `Device(config)# ip dhcp ping timeout 850`	(Optional) Specifies the duration the DHCP server waits for a ping reply from an address pool.
Step 5	**ip dhcp bootp ignore** **Example:** `Device(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 device. BOOTP requests cannot be selectively ignored on a per-DHCP pool basis.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring a Remote Device to Import DHCP Server Options from a Central DHCP Server

The Cisco DHCP server can dynamically configure options such as the Domain Name System (DNS) and Windows Internet Name Service (WINS) addresses to respond to DHCP requests from local clients behind the customer premises equipment (CPE). Earlier, network administrators configured the Cisco DHCP server on each device manually. Now, the Cisco DHCP server is 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 centralized servers.

This section contains the following tasks:

Configuring the Central DHCP Server to Update DHCP Options

Perform the following 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*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Device(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:** `Device(dhcp-config)# network 172.16.0.0 /16`	Specifies the subnet number and mask of the DHCP address pool.
Step 5	**dns-server** *address* [*address2 ... address8*] **Example:** `Device(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 the order of preference.
Step 6	**end** **Example:** `Device(dhcp-config)# end`	Returns to privileged EXEC mode.

Configuring the Remote Device to Import DHCP Options

Perform the following task to configure the remote device to import DHCP options:

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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Device(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:** `Device(dhcp-config)# network 172.30.0.0 /16`	Specifies the subnet network number and mask of the DHCP address pool.

	Command or Action	Purpose
Step 5	**import all** **Example:** `Device(dhcp-config)# import all`	Imports DHCP option parameters into the DHCP server database.
Step 6	**exit** **Example:** `Device(dhcp-config)# exit`	Exits DHCP pool configuration mode and enters global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 0/0`	Configures an interface and enters interface configuration mode.
Step 8	**ip address dhcp** **Example:** `Device(config-if)# ip address dhcp`	Specifies that the interface acquires an IP address through DHCP.
Step 9	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 10	**show ip dhcp import** **Example:** `Device# show ip dhcp import`	Displays the options that are imported from the central DHCP server.

Configuring DHCP Address Allocation Using Option 82

Enabling Option 82 for DHCP Address Allocation

By default, the Cisco DHCP server uses information provided by option 82 to allocate IP addresses. If the DHCP address allocation is disabled, perform the task described in this section to reenable this capability.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp use class** **Example:** `Device(config)# ip dhcp use class`	Controls DHCP classes that 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.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Troubleshooting Tips

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

Defining the DHCP Class and Relay Agent Information Patterns

Before You Begin

You must know the hexadecimal value of each byte location in option 82 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.

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

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.
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp class** *class-name* **Example:** `Device(config)# ip dhcp class CLASS1`	Defines a DHCP class and enters DHCP class configuration mode.
Step 4	**relay agent information** **Example:** `Device(dhcp-class)# relay agent information`	Enters relay agent information option configuration mode. • If you omit this step, the DHCP class matches any relay agent information option, whether the relay agent information option value is available or not.
Step 5	**relay-information hex** *pattern* [*] [**bitmask** *mask*] **Example:** `Device(dhcp-class-relayinfo)# relay-information hex 01030a0b0c02050000000123`	(Optional) Specifies a hexadecimal value for full relay information option. • The *pattern* argument creates a pattern that is used to match 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 available in the DHCP packet.

	Command or Action	Purpose
		• 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.	
Step 7	**end** **Example:** `Device(dhcp-class-relayinfo)# end`	Returns to privileged EXEC mode.

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 with the DHCP pool.
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *name* **Example:** `Device# 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:** `Device(dhcp-config)# network 10.0.20.0`	Configures the subnet and mask for a DHCP address pool on a Cisco IOS DHCP server.
Step 5	**class** *class-name* **Example:** `Device(dhcp-config)# class CLASS1`	Associates a class with a pool and enters DHCP pool class configuration mode. • This command also creates a DHCP class if the DHCP class is not yet defined.
Step 6	**address range** *start-ip end-ip* **Example:** `Device(dhcp-pool-class)# address range 10.0.20.1 10.0.20.100`	(Optional) Sets an address range for the 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. Each class in the DHCP pool is examined for a match in the order configured.
Step 7	Repeat Steps 5 and 6 for each DHCP class you need to associate with the DHCP pool.	
Step 8	**end** **Example:** `Device(dhcp-pool-class)# end`	Returns to privileged EXEC mode.

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

This task enables static routes to be assigned using a DHCP default gateway as the next-hop device. 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. You cannot configure a static route with the CLI without knowing that DHCP-supplied address.

The static routes are updated 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 and then the routes are removed.

When a DHCP client releases an address, the corresponding static route (the route configured using 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 after the renewal.

This feature is particularly useful for VPN deployments such as Dynamic Multipoint VPNs (DMVPNs). This feature is useful when a nonphysical interface, such as a multipoint generic routing encapsulation (mGRE) tunnel, is configured on a device and certain traffic must be excluded from entering the tunnel interface.

Before You Begin

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

Note

- If the DHCP client is not able to obtain an IP address or the default device 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} **dhcp** [*distance*] **Example:** `Device(config)# ip route 192.168.1.1 255.255.255.255 192.168.2.2 dhcp`	Assigns a static route for the default next-hop device when the DHCP server is accessed for an IP address. • If more than one interface 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 a default device.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show ip route** **Example:** `Device# show ip route`	(Optional) Displays the current state of the routing table.

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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip dhcp binding** {*address* | ***}	Deletes an automatic address binding from the DHCP database.

	Command or Action	Purpose
	Example: `Device# clear ip dhcp binding *`	• 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:** `Device# 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:** `Device# clear ip dhcp server statistics`	Resets all DHCP server counters to 0.

Configuration Examples for the Cisco IOS DHCP Server

Example: Configuring the DHCP Database Agent

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

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

Example: Excluding IP Addresses

In the following example, server A and server B service the subnet 10.0.20.0/24. If the subnet is split 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
```

Example: Configuring DHCP Address Pools

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, Domain Name System (DNS) server, (Network Basic Input/Output System) NetBIOS name server, and NetBIOS node type—are inherited in subnetworks 172.16.1.0 and 172.16.2.0. In each pool, clients are granted 30-day leases and all addresses in each subnetwork, except the excluded addresses, are available to the DHCP server for assigning to clients. The table below lists the IP addresses for the devices in three DHCP address pools.

Table 2: DHCP Address Pool Configuration

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 devices	—	Default devices	172.16.1.100 172.16.1.101	Default devices	172.16.2.100 172.16.2.101
DNS server	172.16.1.102 172.16.2.102	—	—	—	—
NetBIOS name server	172.16.1.103 172.16.2.103	—	—	—	—
NetBIOS node type	h-node	—	—	—	—

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

Example: Configuring a DHCP Address Pool with Multiple Disjoint Subnets

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. 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 the other secondary subnet is 172.16.2.0/24.

- When 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 device list that consists of IP addresses 172.16.1.100 and 172.16.1.101. However, when the DHCP server allocates an IP address from the subnet 172.16.2.0/24, 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 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 3: DHCP Address Pool Configuration with Multiple Disjoint Subnets

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 devices	172.16.0.100 172.16.0.101 172.16.0.102 172.16.0.103	Default devices	172.16.1.100 172.16.1.101	Default devices	172.16.0.100 172.16.0.101 172.16.0.102 172.16.0.103
DNS server	172.16.1.102 172.16.2.102	—	—	—	—
NetBIOS name server	172.16.1.103 172.16.2.103	—	—	—	—

Primary Subnet (172.16.0.0/16)	First Secondary Subnet (172.16.1.0/24)	Second Secondary Subnet (172.16.2.0/24)			
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
```

Example: Configuring Manual Bindings

The following example shows how to create a manual binding for a client named example1.abc.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.abc.com that does 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 abc.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
```

Example: Configuring Static Mapping

The following example shows how to restart the DHCP server, configure the pool, and specify the URL where 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 device and served by the TFTP process of the device. In this case, the IP address in the original file line must be an address owned by the device and one additional line of configuration is required on the device:**tftp-server flash** *static-filename*.

Example: Configuring the Option to Ignore all BOOTP Requests

The following example shows two DHCP pools that are configured on the device and that the device'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 device (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.

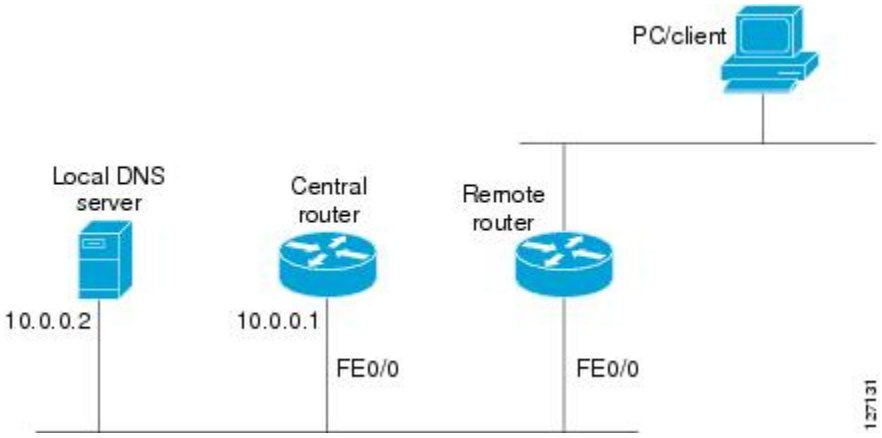
```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
ip subnet-zero
!
ip dhcp bootp ignore
!
ip dhcp pool ABC
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.3
   lease 2
!
ip dhcp pool DEF
   network 10.0.18.0 255.255.255.0
!
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
```

Example: Importing DHCP Options

The following example shows how to configure a remote and central server 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 1: DHCP Example Network Topology



Central Device

```
!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 Device

```
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
```

Example: Configuring DHCP Address Allocation Using Option 82

This example shows how to configure 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.

The subnet of pool ABC has been divided into three ranges without further subnetting 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.

Therefore, 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 10.0.20.1 to 10.0.20.254.

Multiple pools can be configured with the same class, eliminating the need to configure the same patterns in multiple pools. For example, there may be a need to specify that one or more pools must 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
```

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

The following example shows how to configure two Ethernet interfaces to obtain the next-hop device 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 for Cisco IOS DHCP Server

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command 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 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

Related Topic	Document Title
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

RFCs

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

Technical Assistance

Description	Link
The Cisco Support 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

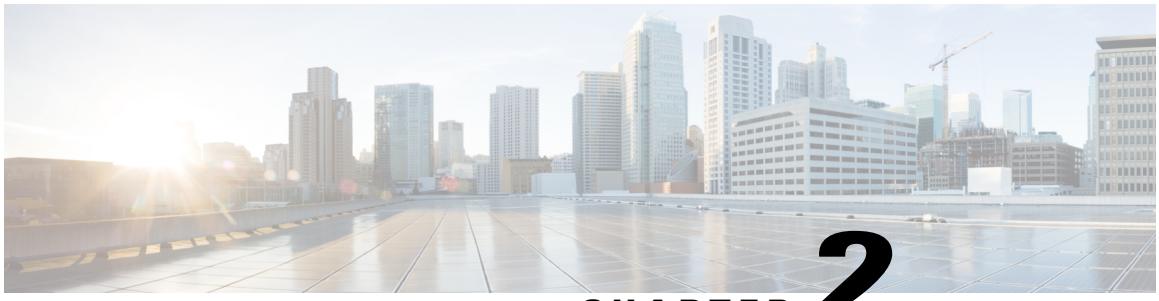
Feature Information for the Cisco IOS DHCP Server

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 . An account on Cisco.com is not required.

Table 4: Feature Information for the Cisco IOS DHCP Server

Feature Name	Releases	Feature Configuration Information
DHCP Server Import All Enhancement	Cisco IOS XE Release 3.2SE	The DHCP Server Import All Enhancement feature is an enhancement to the **import all** command. Prior to this feature, 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	Cisco IOS XE Release 3.2SE	The DHCP Server Multiple Subnet 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	Cisco IOS XE Release 3.2SE	The DHCP Server Option to Ignore all BOOTP Requests 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**.



CHAPTER 2

IPv6 Access Services: DHCPv6 Prefix Delegation

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

- Finding Feature Information, page 47
- Information About IPv6 Access Services: DHCPv6 Prefix Delegation, page 47
- How to Configure IPv6 Access Services: DHCPv6 Prefix Delegation, page 53
- Configuration Examples for IPv6 Access Services: DHCPv6 Prefix Delegation, page 57
- Additional References, page 61
- Feature Information for IPv6 Access Services: DHCPv6 Prefix Delegation, page 62

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About IPv6 Access Services: DHCPv6 Prefix Delegation

DHCPv6 Prefix Delegation

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

- Stateful prefix delegation—Address assignment is centrally managed and clients must obtain configuration information such as address autoconfiguration and neighbor discovery that is not available through protocols.
- Stateless prefix delegation—Stateless configuration parameters do not require a server to maintain any dynamic state for individual clients, such as Domain Name System (DNS) server addresses and domain search list options.

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

Node Configuration Without Prefix Delegation

Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6) allows the DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. The use of stateless DHCPv6 is controlled by router advertisement (RA) messages that are multicast by devices. The DHCPv6 client invokes stateless DHCPv6 when it receives an RA. The DHCPv6 server responds to a stateless DHCPv6 request with configuration parameters, such as the Domain Name System (DNS) servers and domain search list options.

Client and Server Identification

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

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

Rapid Commit

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

DHCPv6 Client, Server, and Relay Functions

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

The following sections describe these functions:

Client Function

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

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

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

Server Selection

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

IAPD and IAID

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

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

Server Function

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

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

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

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

Configuration Information Pool

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

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

- Prefix delegation information, which includes:

- A prefix pool name and associated preferred and valid lifetimes
- A list of available prefixes for a particular client and associated preferred and valid lifetimes

- A list of IPv6 addresses of DNS servers
- A domain search list, which is a string containing domain names for the DNS resolution

DHCP for IPv6 Address Assignment

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

Prefix Assignment

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

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

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

An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

Automatic Binding

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

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

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, and the entry is updated when the client renews, rebinds, or confirms the prefix delegation. A binding

table entry is deleted when the client voluntarily releases all the prefixes in the binding, the valid lifetimes of all prefixes have expired, or administrators run the **clear ipv6 dhcp binding** command.

Binding Database

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

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

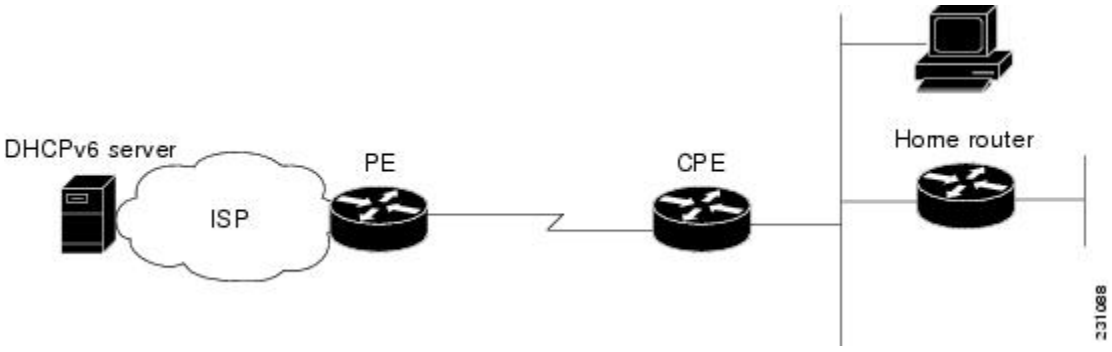
- DHCPv6 pool name from which the configuration was assigned to the client.
- Interface identifier from which the client requests were received.
- The client IPv6 address.
- The client DUID.
- IAID of the IAPD.
- Prefix delegated to the client.
- The prefix length.
- The prefix preferred lifetime in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

DHCPv6 Server Stateless Autoconfiguration

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

The figure below shows a typical broadband deployment.

Figure 2: Broadband Topology



The CPE interface towards the PE can be a stateless or stateful DHCPv6 client. In either case, the ISP-side DHCPv6 server may provide configuration parameters such as DNS server addresses, domain names, and

Simple Network Time Protocol (SNTP) servers to the DHCP client on the CPE. Such information can be specific to ISPs.

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

DHCPv6 supports the following options for IPv6 on the server:

Information Refresh Server Option

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

NIS- and NIS+-Related Server Options

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

SIP Server Options

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

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

SNTP Server Option

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

How to Configure IPv6 Access Services: DHCPv6 Prefix Delegation

Configuring the DHCPv6 Server Function

Configuring the DHCPv6 Configuration Pool

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**domain-name** *domain* **Example:** `Device(config-dhcp)# domain-name example.com`	Configures a domain name for a DHCPv6 client.
Step 5	**dns-server** *ipv6-address* **Example:** `Device(config-dhcp)# dns-server 2001:DB8:3000:3000::42`	Specifies the DNS IPv6 servers available to a DHCPv6 client.
Step 6	**prefix-delegation** *ipv6-prefix* / *prefix-length* *client-duid* [**iaid** *iaid*] [*lifetime*] **Example:** `Device(config-dhcp)# prefix-delegation 2001:DB8:1263::/48 0005000400F1A4D070D03`	Specifies a manually configured numeric prefix to be delegated to a specified client's IAPD.
Step 7	**prefix-delegation pool** *poolname* [**lifetime** *valid-lifetime preferred-lifetime*] **Example:** `Device(config-dhcp)# prefix-delegation pool pool1 lifetime 1800 60`	Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCPv6 clients.
Step 8	**exit** **Example:** `Device(config-dhcp)# exit`	Exits DHCPv6 pool configuration mode, and returns the device to global configuration mode.
Step 9	**interface** *type* *number* **Example:** `Device(config)# interface serial 3`	Specifies an interface type and number, and enters interface configuration mode.
Step 10	**ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**] **Example:** `Device(config-if)# ipv6 dhcp server pool1`	
Step 11	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuring a Binding Database Agent for the Server Function

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp database** *agent* [**write-delay** *seconds*] [**timeout** *seconds*] **Example:** `Device(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding`	Specifies DHCPv6 binding database agent parameters.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring the DHCPv6 Client Function

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 dhcp client pd** {*prefix-name* | **hint** *ipv6-prefix*} [**rapid-commit**] **Example:** `Device(config-if)# ipv6 dhcp client pd dhcp-prefix`	Enables the DHCPv6 client process and enables a request for prefix delegation through a specified interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Deleting Automatic Client Bindings from the DHCPv6 Binding Table

SUMMARY STEPS

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

DETAILED STEPS

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

Configuration Examples for IPv6 Access Services: DHCPv6 Prefix Delegation

Examples: Configuring the DHCPv6 Server Function

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

```
ipv6 dhcp pool dhcp-pool
 prefix-delegation pool client-prefix-pool1 lifetime 1800 600
 dns-server 2001:DB8:3000:3000::42
 domain-name example.com
!
interface Ethernet 0/0
 description downlink to clients
 ipv6 address FEC0:240:104:2001::139/64
 ipv6 dhcp server dhcp-pool
```

```
!
ipv6 local pool client-prefix-pool1 2001:DB8:1200::/40 48
```

The following example from the **show ipv6 dhcp** command shows the DHCP unique identifier (DUID) of the device:

```
Device# show ipv6 dhcp

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

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

```
Device# show ipv6 dhcp binding

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

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

```
Device# show ipv6 dhcp database

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

Example: Configuring the DHCPv6 Configuration Pool

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

```
Device# show ipv6 dhcp pool

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

Example: Configuring the DHCPv6 Client Function

In the following example, this Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client has three interfaces. Ethernet interface 0/0 is the upstream link to a service provider, which has a DHCPv6 server function enabled. The Fast Ethernet interfaces 0/0 and 0/1 are links to local networks.

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

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

```
interface Ethernet 0/0
 description uplink to provider DHCP IPv6 server
 ipv6 dhcp client pd prefix-from-provider
!
```

```
interface FastEthernet 0/0
 description local network 0
 ipv6 address prefix-from-provider ::5:0:0:0:100/64
!
interface FastEthernet 0/1
 description local network 1
 ipv6 address prefix-from-provider ::6:0:0:0:100/64
```

Example: Configuring a Database Agent for the Server Function

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

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

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

```
ipv6 dhcp database bootflash
```

Example: Displaying DHCP Server and Client Information on the Interface

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

```
Device1# show ipv6 dhcp interface

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

Device2# show ipv6 dhcp interface

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

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

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

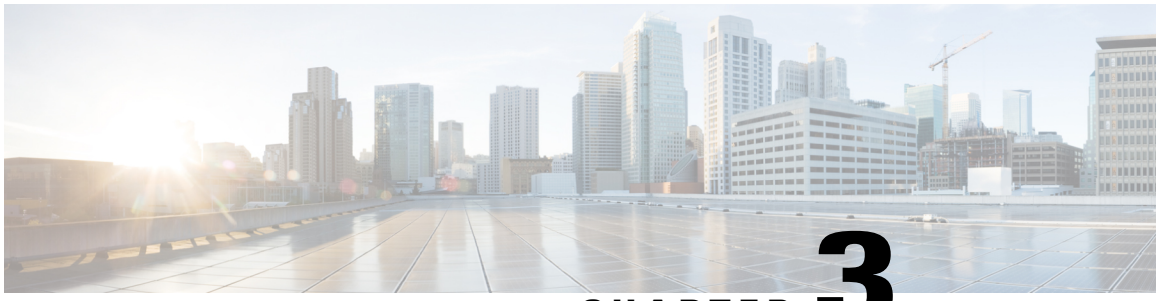
Technical Assistance

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

Feature Information for IPv6 Access Services: DHCPv6 Prefix Delegation

Table 5: Feature Information for IPv6 Access Services: DHCPv6 Prefix Delegation

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCPv6 Prefix Delegation	Cisco IOS XE Release 3.2SE	The DHCPv6 Prefix Delegation feature can be used to manage link, subnet, and site addressing changes. DHCPv6 can be used in environments to deliver stateful and stateless information. The following commands were introduced or modified: **clear ipv6 dhcp binding**, **dns-server**, **domain-name**, **ipv6 dhcp client pd**, **ipv6 dhcp database**, **ipv6 dhcp pool**, **ipv6 dhcp server**, **prefix-delegation**, **prefix-delegation pool**, **show ipv6 dhcp**, **show ipv6 dhcp binding**, **show ipv6 dhcp interface**, **show ipv6 dhcp pool**.



CHAPTER 3

IPv6 Access Services: DHCPv6 Relay Agent

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

- Finding Feature Information, page 63
- Information About IPv6 Access Services: DHCPv6 Relay Agent, page 63
- How to Configure IPv6 Access Services: DHCPv6 Relay Agent, page 67
- Configuration Examples for IPv6 Access Services: DHCPv6 Relay Agent, page 68
- Additional References, page 68
- Feature Information for IPv6 Access Services: DHCPv6 Relay Agent, page 69

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About IPv6 Access Services: DHCPv6 Relay Agent

DHCPv6 Relay Agent

A DHCPv6 relay agent, which may reside on the client's link, is used to relay messages between the client and the server. The DHCPv6 relay agent operation is transparent to the client. A DHCPv6 client locates a DHCPv6 server using a reserved, link-scoped multicast address. For direct communication between the DHCPv6 client and the DHCPv6 server, both of them must be attached to the same link. However, in some

situations where ease of management, economy, or scalability is a concern, it is desirable to allow a DHCPv6 client to send a message to a DHCPv6 server that is not connected to the same link.

DHCPv6 Relay Agent Notification for Prefix Delegation

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

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

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

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

DHCPv6 Relay Options: Remote-ID for Gigabit Ethernet and Fast Ethernet Interfaces

The DHCPv6 Ethernet Remote ID Option feature adds the remote identification (remote-ID) option to relayed (RELAY-FORWARD) DHCPv6 packets.

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

The addition of the remote-ID option to the RELAY-FORWARD packet occurs automatically and no user configuration is necessary.

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

If the remote-ID option is included in the RELAY-REPLY packet, the option is removed from the packet before it is relayed to the client.

DHCPv6 Relay Options: Reload Persistent Interface ID

The DHCPv6 Relay—Reload Persistent Interface ID Option feature makes the interface ID option persistent. The interface ID is used by relay agents to decide which interface should be used to forward a RELAY-REPLY packet. A persistent interface-ID option will not change if the device acting as a relay agent goes offline during a reload or a power outage. When the device acting as a relay agent returns online, it is possible that changes to the internal interface index of the relay agent may have occurred in certain scenarios (such as, when the relay agent reboots and the number of interfaces in the interface index changes, or when the relay agents boot

up and has more virtual interfaces than it did before the reboot). This feature prevents such scenarios from causing any problems.

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

DHCPv6 Relay Chaining

DHCPv6 messages can be relayed through multiple relay agents. This configuration is called *relay chaining*. A relay chaining configuration can be supported only when each relay agent adds information to DHCPv6 messages before relaying them. The information helps in relaying the DHCPv6 reply back to the DHCPv6 client through the same path.

The delegated IPv6 prefix must be routable in order to be useful. The actual DHCPv6 Prefix Delegation (PD) client may not be permitted to inject routes into the delegating network. In service provider (SP) networks, for example, an edge device typically acts as a DHCPv6 relay agent, and this edge device often has the responsibility to maintain routes within the SP network for clients' PD bindings. In the event that DHCPv6 requests and responses are relayed through a chain of DHCPv6 relays, there may be a need to introduce appropriate routes (particularly with DHCPv6 PD) in the Forwarding Information Base (FIB) so that routing is handled transparently.

DHCPv6 Relay Agent Notification for Prefix Delegation

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

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

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

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

DHCPv6 Relay SSO and ISSU

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

state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

The Cisco in-service software upgrade (ISSU) process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows the Cisco software to be modified while packet forwarding continues. This increases network availability and reduces downtime caused by planned software upgrades.

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

DHCPv6 Relay Options: Remote ID for Ethernet Interfaces

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

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

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

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

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

DHCPv6 Relay Options: Reload Persistent Interface ID Option

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

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

How to Configure IPv6 Access Services: DHCPv6 Relay Agent

Configuring the DHCPv6 Relay Agent

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 4/2/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*] **Example:** `Device(config-if) ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 gigabitethernet 4/3/0`	Specifies a destination address to which client packets are forwarded and enables the DHCPv6 relay service on the interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for IPv6 Access Services: DHCPv6 Relay Agent

Example: Configuring the DHCPv6 Relay Agent

```
Device# show ipv6 dhcp interface

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

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

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

Technical Assistance

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

Feature Information for IPv6 Access Services: DHCPv6 Relay Agent

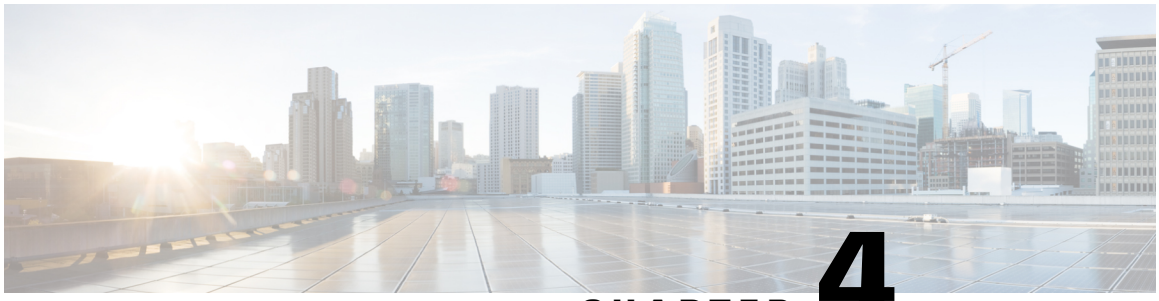
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

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

Table 6: Feature Information for IPv6 Access Services: DHCPv6 Relay Agent

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCPv6 Relay Agent	Cisco IOS XE Release 3.2SE	A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and server. The following commands were introduced or modified: **ipv6 dhcp relay destination**, **show ipv6 dhcp interface**.

Feature Name	Releases	Feature Information
DHCPv6 Relay Agent Notification for Prefix Delegation	Cisco IOS XE Release 3.2SE	DHCPv6 relay agent notification for prefix delegation allows the device working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 packet that is being relayed by the relay agent to the client.
DHCPv6 Relay: Reload Persistent Interface ID Option	Cisco IOS XE Release 3.2SE	This feature makes the interface-ID option, which is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet, persistent.



CHAPTER 4

DHCP Client

The Cisco Dynamic Host Configuration Protocol (DHCP) Client feature allows a Cisco device to act as a host requesting configuration parameters, such as an IP address, from a DHCP server.

- Finding Feature Information, page 71
- Restrictions for the DHCP Client, page 71
- Information About the DHCP Client, page 72
- DHCP Client Overview, page 72
- How to Configure the DHCP Client, page 73
- Configuration Examples for the DHCP Client, page 75
- Additional References, page 75
- Feature Information for the DHCP Client, page 76

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 the DHCP Client

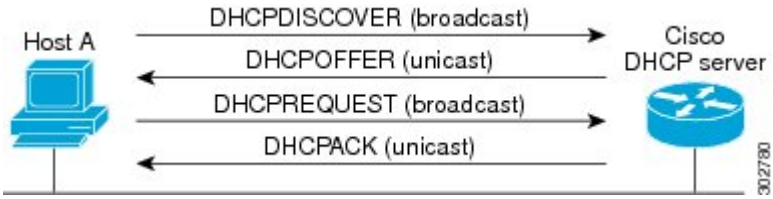
The DHCP client can be configured on Ethernet interfaces.

Information About the DHCP Client

DHCP Client Operation

The Dynamic Host Configuration Protocol (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 3: 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. 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 dynamic host configuration protocol client functionality allows a DHCP client to use a user-specified client identifier, class identifier, or suggested lease time when requesting an address from a DHCP server.

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

- Option 12—This option specifies the name of the client. The name may or may not be qualified with the local domain.
- Option 51—This option is used in a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for the IP address.
- Option 55—This option allows the DHCP client to request certain options from the DHCP server. The **ip dhcp client request** command allows the system administrator to turn off some of the requested options, thus removing them from the request list.

- Option 60—This option allows the user to configure the vendor class identifier string to use in the DHCP interaction.
- Option 61—This option is used by DHCP clients to specify their unique identifier. DHCP servers use this value to index their database of address bindings. This value is expected to be unique for all clients in an administrative domain.
- 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; that is, each routing table entry includes a subnet mask. Upto ten classless static routes are supported using option 121 on the DHCP client.

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.

How to Configure the DHCP Client

Configuring the DHCP Client

Cisco devices running Cisco software include the Dynamic Host Configuration Protocol (DHCP) server and relay agent software, which are enabled by default. Your device can act as both the DHCP client and the DHCP server. Use the **ip address dhcp** command to obtain IP address information for the configured interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address dhcp**
5. **end**
6. **debug dhcp detail**
7. **debug ip dhcp server packets**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

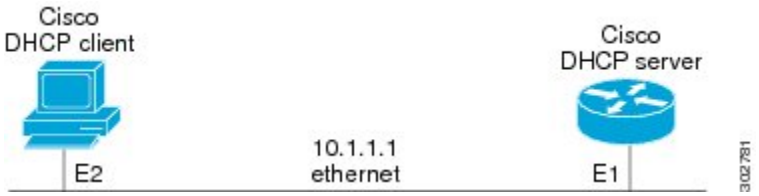
	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address dhcp** **Example:** `Device(config-if)# ip address dhcp`	Acquires an IP address on an interface from DHCP.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**debug dhcp detail** **Example:** `Device# debug dhcp detail`	Displays the DHCP packets that were sent and received.
Step 7	**debug ip dhcp server packets** **Example:** `Device# debug ip dhcp server packets`	Displays the server side of the DHCP interaction.

Configuration Examples for the DHCP Client

Example: Configuring the DHCP Client

The figure below shows a simple network diagram of a Dynamic Host Configuration Protocol (DHCP) client on an Ethernet LAN.

Figure 4: Topology Showing a DHCP Client with a Gigabit 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 GigabitEthernet 0/0/0
 ip address dhcp
```

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

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
DHCP commands	Cisco IOS IP Addressing Services Command Reference
DHCP conceptual information	"DHCP Overview" module in the *IP Addressing: DHCP Configuration Guide*

RFCs

RFCs	Title
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

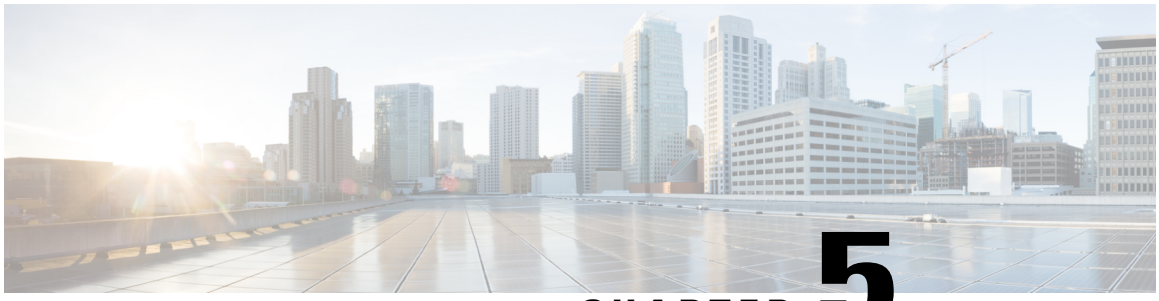
Feature Information for the DHCP Client

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 . An account on Cisco.com is not required.

Table 7: Feature Information for the DHCP Client

Feature Name	Releases	Feature Information
DHCP Client	Cisco IOS XE Release 3.2SE	The DHCP client is defined as an Internet host using DHCP to obtain configuration parameters such as an IP address.



CHAPTER 5

DHCPv6 Server Stateless Autoconfiguration

Hierarchical Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for stateless configuration parameters allows a stateless or stateful DHCPv6 client to export configuration parameters (DHCPv6 options) to a local DHCPv6 server pool. The local DHCPv6 server can then provide the imported configuration parameters to other DHCPv6 clients.

- Finding Feature Information, page 77
- Information About DHCPv6 Server Stateless Autoconfiguration, page 77
- How to Configure DHCPv6 Server Stateless Autoconfiguration, page 79
- Configuration Examples for DHCPv6 Server Stateless Autoconfiguration, page 83
- Additional References for DHCP Overview, page 83
- Feature Information for DHCPv6 Server Stateless Autoconfiguration, page 84

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 DHCPv6 Server Stateless Autoconfiguration

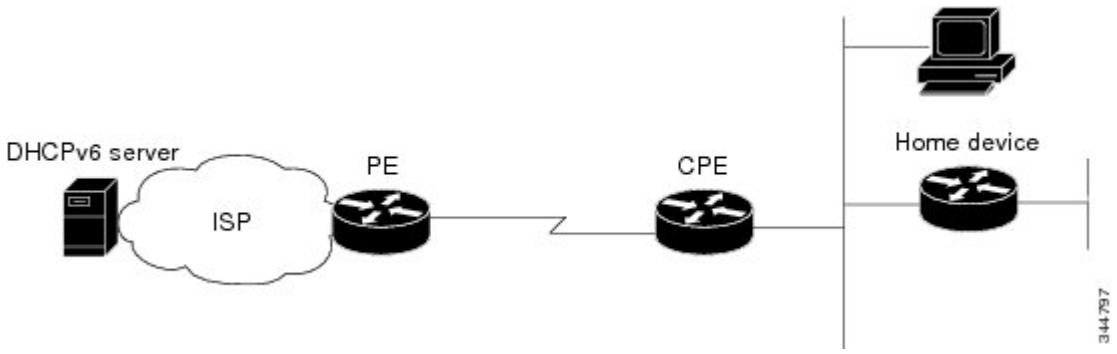
DHCPv6 Server Stateless Autoconfiguration

Hierarchical Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for stateless configuration parameters allows a stateless or stateful DHCPv6 client to export configuration parameters (DHCPv6 options) to a local

DHCPv6 server pool. The local DHCPv6 server can then provide the imported configuration parameters to other DHCPv6 clients.

The figure below shows a typical broadband deployment.

Figure 5: Broadband Topology



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

In addition to being a DHCPv6 client (for example, toward the ISP), the CPE can act as a DHCPv6 server to the home network. For example, neighbor discovery followed by a stateless or stateful DHCPv6 client can occur on the link between the CPE and the home devices. In some cases, the information to be provided to the home network is the same as that obtained from the ISP-side DHCPv6 server. Because this information can be dynamically changed, it cannot be hard-configured in the CPE's configuration. Therefore, the DHCPv6 component on the CPE allows automatic importing of configuration parameters from the DHCPv6 client to the DHCPv6 server pool.

DHCPv6 supports the options for IPv6 on the server described in the following sections.

Information Refresh Server Option

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

NIS- and NIS+-Related Server Options

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

SIP Server Options

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

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

SNTP Server Option

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

How to Configure DHCPv6 Server Stateless Autoconfiguration

Configuring the Stateless DHCPv6 Server

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool dhcp-pool`	Configures a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) configuration information pool and enters DHCPv6 pool configuration mode.

	Command or Action	Purpose
Step 4	**dns-server** *ipv6-address* **Example:** `Device(config-dhcp)# dns-server 2001:DB8:3000:3000::42`	Specifies the Domain Name System (DNS) IPv6 servers available to a DHCPv6 client.
Step 5	**domain-name** *domain* **Example:** `Device(config-dhcp)# domain-name example.com`	Configures a domain name for a DHCPv6 client.
Step 6	**exit** **Example:** `Device(config-dhcp)# exit`	Exits DHCPv6 pool configuration mode, and returns the device to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface serial 3`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 8	**ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**] **Example:** `Device(config-if)# ipv6 dhcp server dhcp-pool`	Enables DHCPv6 on an interface.
Step 9	**ipv6 nd other-config flag** **Example:** `Device(config-if)# ipv6 nd other-config flag`	Sets the “other stateful configuration” flag in IPv6 router advertisements (RAs).
Step 10	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuring the Stateless DHCPv6 Client

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface serial 3`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 address autoconfig** [**default**] **Example:** `Device(config-if)# ipv6 address autoconfig`	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Enabling Processing of Packets with Source Routing Header Options

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 source-route** **Example:** `Device(config)# ipv6 source-route`	Enables processing of the IPv6 type 0 routing header.
Step 4	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for DHCPv6 Server Stateless Autoconfiguration

Example: Configuring the Stateless DHCPv6 Function

The following example shows how to use the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) function to configure clients with information about the name lookup system. The server is configured with a DHCP pool, which contains the name lookup information that is to be passed to clients. It does not need to contain a prefix pool. This DHCP pool is attached to the access link to customers (Ethernet 0/0) when you enter the **ipv6 dhcp server** command. The access link also has the **ipv6 nd other-config-flag** command enabled. Router advertisement (RA) messages sent from this interface inform clients that they should use DHCPv6 for "other" (for example, nonaddress) configuration information.

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

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

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

Additional References for DHCP Overview

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFC 951	*Bootstrap Protocol (BOOTP)*
RFC 1542	*Clarifications and Extensions for the Bootstrap Protocol*
RFCs for IPv6	*IPv6 RFCs*

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

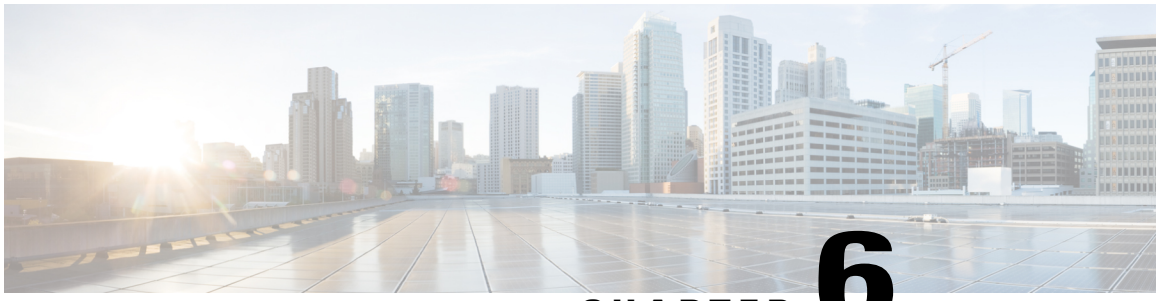
Feature Information for DHCPv6 Server Stateless Autoconfiguration

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 . An account on Cisco.com is not required.

Table 8: Feature Information for DHCPv6 Server Stateless Autoconfiguration

Feature Name	Releases	Feature Information
DHCPv6 Server Stateless Autoconfiguration	Cisco IOS XE Release 3.2SE	Hierarchical DHCPv6 for stateless configuration parameters allows a stateless or stateful DHCPv6 client to export configuration parameters (DHCPv6 options) to a local DHCPv6 server pool. The following commands were introduced or modified: **dns-server**, **domain-name**, **ipv6 address autoconfig**, **ipv6 dhcp pool**, **ipv6 dhcp server**, **ipv6 nd other-config-flag**, **ipv6 source-route**.



CHAPTER 6

DHCPv6 Server Timer Options

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server options are part of DHCP stateless autoconfiguration.

- Finding Feature Information, page 87
- Information About DHCPv6 Server Timer Options, page 87
- How to Configure DHCPv6 Server Timer Options, page 88
- Configuration Examples for DHCPv6 Server Timer Options, page 95
- Additional References, page 95
- Feature Information for DHCPv6 Server Timer Options, page 96

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 DHCPv6 Server Timer Options

Information Refresh Server Option

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

NIS- and NIS+-Related Server Options

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

SNTP Server Option

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

How to Configure DHCPv6 Server Timer Options

Configuring the Information Server Refresh Option

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **information refresh** {*days* [*hours minutes*] | **infinity**}
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**information refresh** {*days* [*hours minutes*] | **infinity**} **Example:** `Device(config-dhcp)# information refresh 1 1 1`	Specifies the information refresh time to be sent to the client.
Step 5	**end** **Example:** `Device(config-dhcp)# end`	Returns to privileged EXEC mode.

Importing the Information Server Refresh Option

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **import information refresh**
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**import information refresh** **Example:** `Device(config-dhcp)# import information refresh`	Imports the information refresh time option to a DHCPv6 client.
Step 5	**end** **Example:** `Device(config-dhcp)# end`	Returns to privileged EXEC mode.

Configuring NIS- and NISP-Related Server Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **nis address** *ipv6-address*
5. **nis domain-name** *domain-name*
6. **nisp address** *ipv6-address*
7. **nisp domain-name** *domain-name*
8. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**nis address** *ipv6-address* **Example:** `Device(config-dhcp)# nis address 2001:DB8:1000:1000::30`	Specifies the NIS address of an IPv6 server to be sent to the client.
Step 5	**nis domain-name** *domain-name* **Example:** `Device(config-dhcp)# nis domain-name domain1`	Enables a server to convey a client's NIS domain name information to the client.
Step 6	**nisp address** *ipv6-address* **Example:** `Device(config-dhcp)# nisp address 2001:DB8:3000:3000::42`	Specifies the NIS+ address of an IPv6 server to be sent to the DHCPv6 client.
Step 7	**nisp domain-name** *domain-name* **Example:** `Device(config-dhcp)# nisp domain-name domain2`	Enables a server to convey a client's NIS+ domain name information to the DHCPv6 client.
Step 8	**end** **Example:** `Device(config-dhcp)# end`	Returns to privileged EXEC mode.

Importing NIS- and NIS+-Related Server Options

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**import nis address** **Example:** `Device(config-dhcp)# import nis address`	Imports the NIS servers option to a DHCPv6 client.
Step 5	**import nis domain-name** **Example:** `Device(config-dhcp)# import nis domain-name`	Imports the NIS domain name option to a DHCPv6 client.

	Command or Action	Purpose
Step 6	**import nisp address** **Example:** `Device(config-dhcp)# import nisp address`	Imports the NISP address option to a DHCPv6 client.
Step 7	**import nisp domain-name** **Example:** `Device(config-dhcp)# import nisp domain-name`	Imports the NISP domain name option to a DHCPv6 client.
Step 8	**end** **Example:** `Device(config-dhcp)# end`	Returns to privileged EXEC mode.

Configuring the SNTP Server Option

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**sntp address** *ipv6-address* **Example:** `Device(config-dhcp)# sntp address 2001:DB8:2000:2000::33`	Specifies the SNTP server list to be sent to the client.
Step 5	**end** **Example:** `Device(config-dhcp)# end`	Returns to privileged EXEC mode.

Importing the SNTP Server Option

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool pool1`	Configures a DHCPv6 configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**import sntp address** *ipv6-address* **Example:** `Device(config-dhcp)# import sntp address 2001:DB8:2000:2000::33`	Imports the SNTP server option to a DHCPv6 client.
Step 5	**end** **Example:** `Device(config-dhcp)# end`	Returns to privileged EXEC mode.

Configuration Examples for DHCPv6 Server Timer Options

Example: Configuring DHCPv6 Server Timer Options

```
Device# show ipv6 dhcp pool

DHCPv6 pool: pool1
  Domain name: domain1
  NIS server domain name: ndomain1
  NIS server domain name: ndomain2
  SNTP server address: 2001:DB8::1
  Imported Information refresh: 90060
  Active clients: 0
```

Additional References

Related Documents

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

Related Topic	Document Title
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

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

Technical Assistance

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

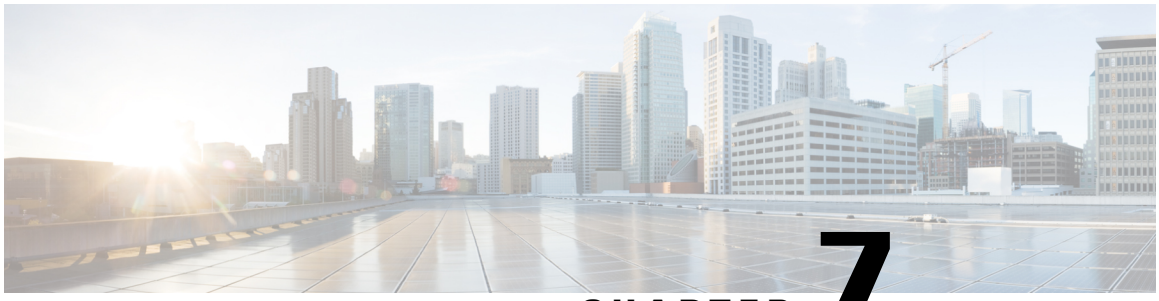
Feature Information for DHCPv6 Server Timer Options

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 . An account on Cisco.com is not required.

Table 9: Feature Information for DHCPv6 Server Timer Options

Feature Name	Releases	Feature Information
DHCPv6 Client Information Refresh Option	Cisco IOS XE Release 3.2SE	The DHCPv6 information refresh option can specify an upper boundary for the length of time a client should wait before refreshing information retrieved from DHCPv6. The following commands were introduced or modified: **import information refresh**, **information refresh**, **ipv6 dhcp pool**, **show ipv6 dhcp pool**.
DHCPv6 Server Timer Options	Cisco IOS XE Release 3.2SE	The DHCPv6 server options are part of DHCP stateless autoconfiguration. The following commands were introduced or modified: **import nis-address**, **import nis domain-name**, **import nisp address**, **import nisp domain-name**, **ipv6 dhcp pool**, **nis address**, **nis domain-name**, **nisp address**, **nisp domain-name**, **show ipv6 dhcp pool**.



CHAPTER 7

DHCPv6 Individual Address Assignment

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Individual Address Assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected.

- Finding Feature Information, page 99
- Prerequisites for Configuring DHCPv6 Address Assignment, page 99
- Information About DHCPv6 Individual Address Assignment, page 100
- How to Configure DHCPv6 Individual Address Assignment, page 100
- Configuration Examples for DHCPv6 Individual Address Assignment, page 105
- Additional References, page 106
- Feature Information for DHCPv6 Individual Address Assignment, page 107

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 DHCPv6 Address Assignment

By default, no Dynamic Host Configuration Protocol for IPv6 (DHCPv6) features are configured on the device.

When you configure DHCPv6 address assignment, remember that the specified interface must be one of these Layer 3 interfaces:

- Switch virtual interface (SVI): a VLAN interface created when you enter the **interface vlan** *vlan-id* command.

- EtherChannel port channel in Layer 3 mode: a port-channel logical interface created when you enter the **interface port-channel** *port-channel-number* command.

Information About DHCPv6 Individual Address Assignment

DHCPv6 Address Assignment

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

How to Configure DHCPv6 Individual Address Assignment

Enabling the DHCPv6 Server Function on an Interface

Perform this task to enable the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server function on an interface. Note that to delete a DHCPv6 pool, you must use the **no ipv6 dhcp pool** *poolname* global configuration command. Use the **no** form of the DHCP pool configuration mode commands to change the DHCPv6 pool characteristics. To disable the DHCPv6 server function on an interface, use the **no ipv6 dhcp server** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **address prefix** *ipv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]
5. **link-address** *ipv6-prefix*
6. **vendor-specific** *vendor-id*
7. **suboption** *number* {**address** *ipv6-address* | **ascii** *ascii-string* | **hex** *hex-string*}
8. **exit**
9. **exit**
10. **interface** *type number*
11. **ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]
12. **end**
13. Do one of the following:
    - **show ipv6 dhcp pool**
    - **show ipv6 dhcp interface**
14. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device(config)# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool engineering`	Enters DHCP for IPv6 pool configuration mode, and defines the name of the IPv6 DHCP pool.
Step 4	**address prefix** *ipv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]	(Optional) Specifies an address prefix for address assignment.

	Command or Action	Purpose
	Example: `Device(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite`	• This address must be in hexadecimal, using 16-bit values between colons. • **lifetime** *valid-lifetime preferred-lifetime*—Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state.
Step 5	**link-address** *ipv6-prefix* **Example:** `Device(config-dhcpv6)# link-address 2001:1001::0/64`	(Optional) Specifies a link-address IPv6 prefix. • When an address on the incoming interface or a link address in the packet matches the specified IPv6 prefix, the server uses the configuration information pool.
Step 6	**vendor-specific** *vendor-id* **Example:** `Device(config-dhcpv6)# vendor-specific 9`	(Optional) Enters DHCPv6 vendor-specific configuration mode with the vendor-specific identification number.
Step 7	**suboption** *number* {**address** *ipv6-address* | **ascii** *ascii-string* | **hex** *hex-string*} **Example:** `Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1`	(Optional) Enters a vendor-specific suboption number.
Step 8	**exit** **Example:** `Device(config-dhcpv6-vs)# exit`	Returns to DHCP pool configuration mode.
Step 9	**exit** **Example:** `Device(config-dhcpv6)# exit`	Returns to global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Enters interface configuration mode, and specifies the interface to configure.
Step 11	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]	Enables the DHCPv6 server function on an interface.

	Command or Action	Purpose
	Example: `Device(config-if)# ipv6 dhcp server rapid-commit`	
Step 12	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 13	Do one of the following: • **show ipv6 dhcp pool** • **show ipv6 dhcp interface** **Example:** `Device# show ipv6 dhcp pool`	Verifies DHCPv6 pool configuration or verifies that the DHCPv6 server function is enabled on an interface.
Step 14	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling the DHCPv6 Client Function on an Interface

Perform this task to enable the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client function on an interface. To disable the DHCPv6 client function, use the **no ipv6 address dhcp** interface configuration command. To remove the DHCPv6 client request, use the **no ipv6 address dhcp client request vendor** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address dhcp** [**rapid-commit**]
5. **ipv6 address dhcp client request vendor**
6. **end**
7. **show ipv6 dhcp interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Enters interface configuration mode, and specifies the interface to configure.
Step 4	**ipv6 address dhcp** [**rapid-commit**] **Example:** `Device(config-if)# ipv6 address dhcp rapid-commit`	Enables the interface to acquire an IPv6 address from the DHCPv6 server.
Step 5	**ipv6 address dhcp client request vendor** **Example:** `Device(config-if)# ipv6 adress dhcp client request vendor`	(Optional) Enables the interface to request the vendor-specific option.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show ipv6 dhcp interface** **Example:** `Device# show ipv6 dhcp interface`	Verifies that the DHCPv6 client is enabled on an interface.

Configuration Examples for DHCPv6 Individual Address Assignment

Examples: Configuring the DHCPv6 Server Function

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

```
ipv6 dhcp pool dhcp-pool
 prefix-delegation pool client-prefix-pool1 lifetime 1800 600
 dns-server 2001:DB8:3000:3000::42
 domain-name example.com
!
interface Ethernet 0/0
 description downlink to clients
 ipv6 address FEC0:240:104:2001::139/64
 ipv6 dhcp server dhcp-pool
!
ipv6 local pool client-prefix-pool1 2001:DB8:1200::/40 48
```

The following example from the **show ipv6 dhcp** command shows the DHCP unique identifier (DUID) of the device:

```
Device# show ipv6 dhcp

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

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

```
Device# show ipv6 dhcp binding

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

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

```
Device# show ipv6 dhcp database

Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
```

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

Example: Configuring the DHCPv6 Client Function

In the following example, this Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client has three interfaces. Ethernet interface 0/0 is the upstream link to a service provider, which has a DHCPv6 server function enabled. The Fast Ethernet interfaces 0/0 and 0/1 are links to local networks.

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

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

```
interface Ethernet 0/0
 description uplink to provider DHCP IPv6 server
 ipv6 dhcp client pd prefix-from-provider
!
interface FastEthernet 0/0
 description local network 0
 ipv6 address prefix-from-provider ::5:0:0:0:100/64
!
interface FastEthernet 0/1
 description local network 1
 ipv6 address prefix-from-provider ::6:0:0:0:100/64
```

Additional References

Related Documents

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

Related Topic	Document Title
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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

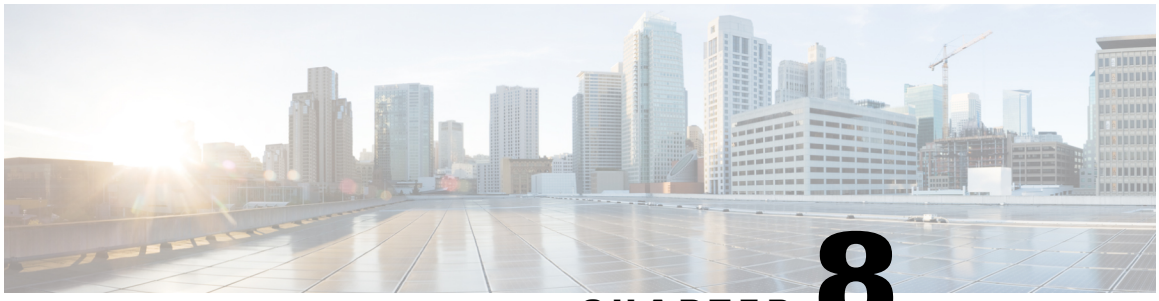
Feature Information for DHCPv6 Individual Address Assignment

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 . An account on Cisco.com is not required.

Table 10: Feature Information for DHCPv6 Individual Address Assignment

Feature Name	Releases	Feature Information
DHCPv6 Individual Address Assignment	Cisco IOS XE Release 3.2SE	The DHCPv6 Individual Address Assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. The following commands were introduced or modified: **clear ipv6 dhcp bindings**, **debug ipv6 dhcp**, **ipv6 address dhcp**, **ipv6 dhcp pool**, **show ipv6 dhcp bindings**, **show ipv6 dhcp interface**, **show ipv6 dhcp pool**.



CHAPTER 8

DHCPv6 Ethernet Remote ID Option

The DHCPv6 Ethernet Remote ID Option feature adds the remote ID option to relayed (RELAY-FORWARD) DHCP for IPv6 (DHCPv6) packets. The information contained in the remote ID option can be used in the server's decision making about the prefixes and configuration parameters that the client receives.

- Finding Feature Information, page 109
- Information About DHCPv6 Ethernet Remote ID Option, page 109
- Restrictions for DHCPv6 Ethernet Remote ID Option, page 110
- Additional References for DHCPv6 Ethernet Remote ID Option, page 110
- Feature Information for DHCPv6 Ethernet Remote ID Option, page 111

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 DHCPv6 Ethernet Remote ID Option

DHCPv6 Ethernet Remote ID Option Overview

The DHCPv6 Ethernet Remote ID Option feature adds the remote ID option to relayed (RELAY-FORWARD) DHCP for IPv6 (DHCPv6) packets.

The remote ID option provides information to the DHCPv6 server, including port information, the system's DHCPv6 Unique Identifier (DUID), and the VLAN ID. Collectively, this information can be used to uniquely identify both the relay and the port on the relay through which the client's packet arrived. The DHCPv6 server

uses this information to select parameters specific to a particular user, host, or subscriber modem. This feature works only for Ethernet interfaces.

No user configuration is required for this feature. The addition of the remote ID option to the RELAY-FORWARD packet occurs automatically.

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

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

Restrictions for DHCPv6 Ethernet Remote ID Option

Depending on your release, the DHCPv6 Ethernet Remote ID Option feature works only on Ethernet interfaces.

Additional References for DHCPv6 Ethernet Remote ID Option

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS IP Addressing Services commands	Cisco IOS IP Addressing Services Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 4649	*Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option*

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

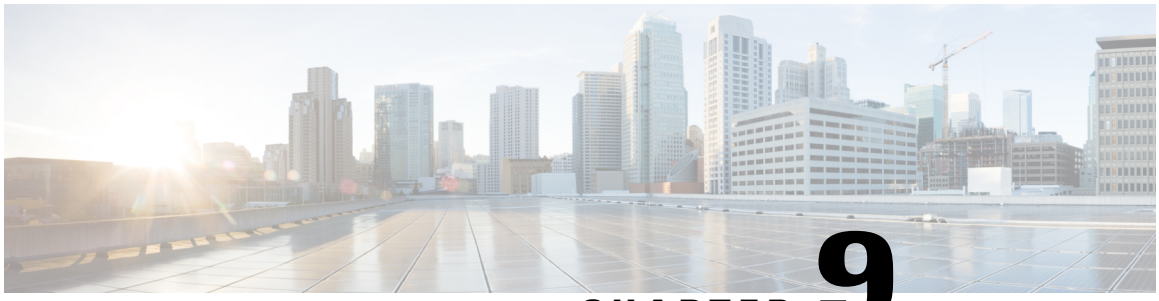
Feature Information for DHCPv6 Ethernet Remote ID Option

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 . An account on Cisco.com is not required.

Table 11: Feature Information for DHCPv6 Ethernet Remote ID Option

Feature Name	Releases	Feature Information
DHCPv6 Ethernet Remote ID Option	Cisco IOS XE Release 3.2SE	The DHCPv6 Ethernet Remote ID Option feature adds the remote-ID option to relayed (RELAY-FORWARD) DHCPv6 packets.



CHAPTER 9

DHCPv6 Relay—Reload Persistent Interface ID Option

The DHCPv6 Relay—Reload Persistent Interface ID Option feature makes the interface-ID option persistent. The interface ID option is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet. The interface ID DHCP for IPv6 (DHCPv6) option added to the DHCPv6 relayed message is formed by the interface name concatenated with the VLAN identifier when available. This way the value of the interface-ID option is persistent after a router reload.

- Finding Feature Information, page 113
- Information About DHCPv6 Relay—Reload Persistent Interface ID Option, page 114
- Additional References for DHCPv6 Relay—Reload Persistent Interface ID Option, page 114
- Feature Information for DHCPv6 Relay—Reload Persistent Interface ID Option, page 115

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 DHCPv6 Relay—Reload Persistent Interface ID Option

DHCPv6 Relay—Reload Persistent Interface ID Option Overview

The DHCPv6 Relay—Reload Persistent Interface ID Option feature makes the interface ID option persistent. The interface ID option is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet. A persistent interface ID option does not change if the device acting as a relay agent goes offline (such as during a reload or a power outage). When the device acting as a relay agent returns online, it is possible that changes to the internal interface index of the relay agent may have occurred in certain scenarios (such as cases where the relay agent reboots and has a change in the number of interfaces in the interface index, or the relay agent boots up and has more virtual interfaces than it did before the reboot). This feature prevents this scenario from causing any problems.

This feature changes the DHCPv6 interface ID option to be expressed as simply the short form of the interface name. This short form helps avoid potential problems that could arise due to physical or logical interfaces changing on the relay agent after a reload. No user configuration is required for this feature.

Additional References for DHCPv6 Relay—Reload Persistent Interface ID Option

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS IP Addressing Services commands	Cisco IOS IP Addressing Services Command Reference

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

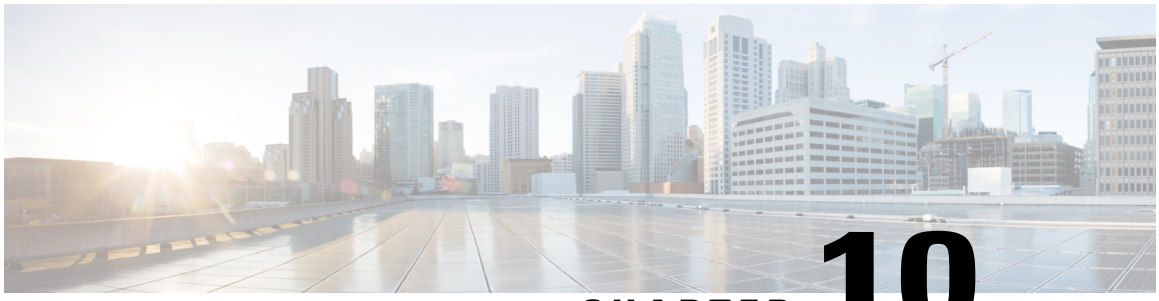
Feature Information for DHCPv6 Relay—Reload Persistent Interface ID Option

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 . An account on Cisco.com is not required.

Table 12: Feature Information for DHCPv6 Relay—Reload Persistent Interface ID Option

Feature Name	Releases	Feature Information
DHCPv6 Relay—Reload Persistent Interface ID Option	Cisco IOS XE Release 3.2SE	The DHCPv6 Relay—Reload Persistent Interface ID Option feature makes the interface-ID option persistent. The interface-ID option is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet.



CHAPTER 10

DHCP Server Port-Based Address Allocation

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

- Finding Feature Information, page 117
- Restrictions for DHCP Server Port-Based Address Allocation, page 117
- Information About DHCP Server Port-Based Address Allocation, page 118
- How to Configure DHCP Server Port-Based Address Allocation, page 119
- Configuration Examples for DHCP Server Port-Based Address Allocation, page 123
- Additional References, page 124
- Feature Information for DHCP Server Port-Based Address Allocation, page 125

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Restrictions for DHCP Server Port-Based Address Allocation

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

Information About DHCP Server Port-Based Address Allocation

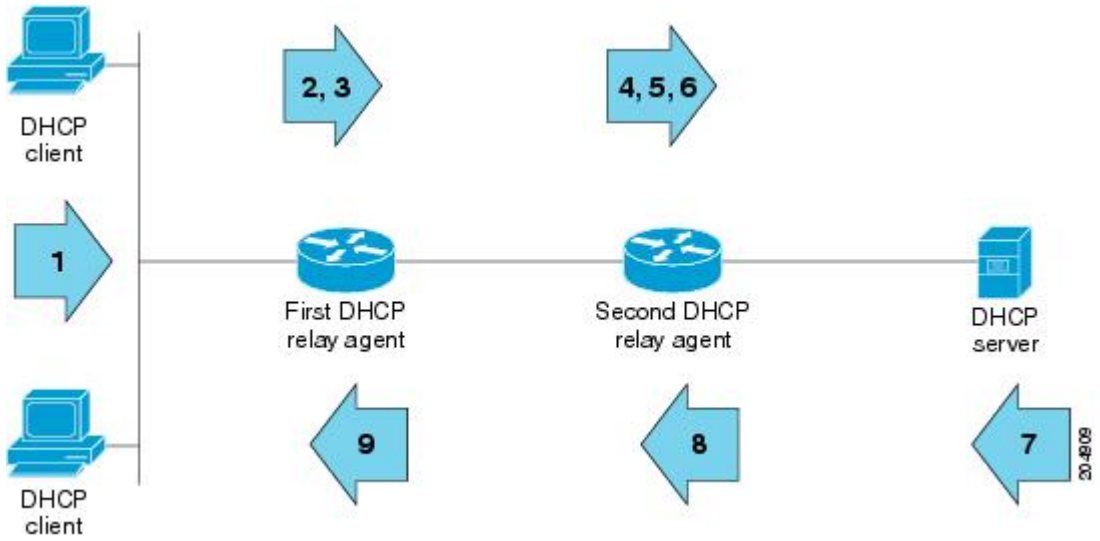
DHCP Server Port-Based Address Allocation Feature Design

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

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

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

Figure 6: DHCP Server Port-Based Address Assignment to Directly Connected Manufacturing Devices



How to Configure DHCP Server Port-Based Address Allocation

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp use subscriber-id client-id** **Example:** `Router(config)# ip dhcp use subscriber-id client-id`	Configures the DHCP server to globally use the subscriber ID as the client ID on all incoming DHCP messages. • DHCP uses the subscriber ID configured on the interface to generate the client ID. If no subscriber ID is configured then the client ID is automatically generated based on the short name of the interface. The client ID already present in the message is ignored.

	Command or Action	Purpose
		• For port based address allocation, do not configure any subscriber ID on the interface. It must be generated automatically from interface name.
Step 4	**interface type number** **Example:** `Router(config)# interface Ethernet 0/0`	(Optional) Configures an interface and enters interface configuration mode.
Step 5	**ip dhcp server use subscriber-id client-id** **Example:** `Router(config-if)# ip dhcp server use subscriber-id client-id`	(Optional) Configures the DHCP server to use the subscriber ID as the client ID on all incoming DHCP messages on the interface.

Troubleshooting Tips

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

- **debug ip dhcp server packets**

Preassigning IP Addresses and Associating Them to a Client

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

For port-based address assignment, you must perform the task in the Automatically Generating a Subscriber Identifier for a DHCP Message Received on a Port, on page 119 task to associate the client ID with the subscriber ID. The subscriber ID value is based on the short name of the port to which the directly connected device is attached.

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

Note

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

>

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 6	**address** *ip-address* **hardware-address** *mac-address* [*hardware-number*] **Example:** `Router(dhcp-config)# address 10.10.10.3 hardware-address b708.1388.f166`	(Optional) Reserves an IP address for a client identified by the hardware address. • This command is used for clients identified by the hardware address included in the fixed-size header of the DHCP message.
Step 7	**end** **Example:** `Router(dhcp-config)# end`	Returns to privileged EXEC mode.
Step 8	**show ip dhcp pool** [*name*] **Example:** `Router> show ip dhcp pool`	(Optional) Displays information about DHCP address pools.
Step 9	**show ip dhcp binding** **Example:** `Router> show ip dhcp binding` **Example:**	(Optional) Displays infinite binding for the configured addresses.

Preassigning IP Addresses and Associating Them to a Client

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

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

>

SUMMARY STEPS

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

DETAILED STEPS

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

Configuration Examples for DHCP Server Port-Based Address Allocation

DHCP Server Port-Based Address Allocation Example

In the following example, a subscriber ID will be automatically generated based on the short name of the interface (port) specified by the **address client-id** command. The DHCP server will ignore any client ID fields

in the DHCP messages and use this subscriber ID as the client ID. The DHCP client is preassigned IP address 10.1.1.7.

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

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

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

Additional References

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

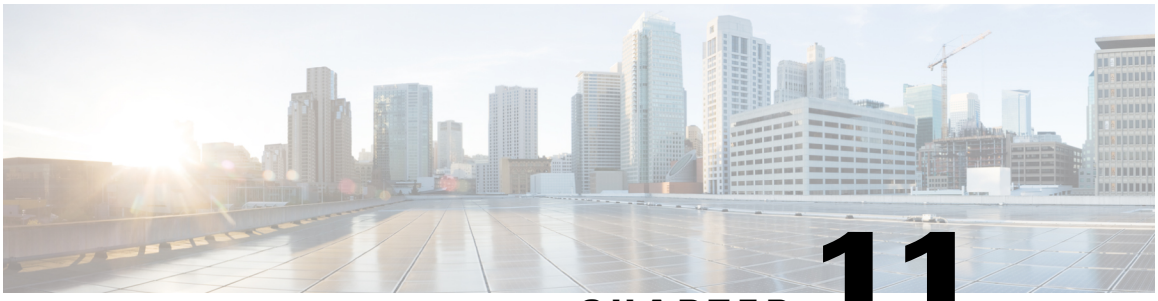
Feature Information for DHCP Server Port-Based Address Allocation

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

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

Table 13: Feature Information for DHCP Port-Based Address Allocation

Feature Name	Releases	Feature Information
DHCP Server Port-Based Address Allocation	Cisco IOS XE Release 3.2SE	The DHCP Server Port-Based Address Allocation feature provides port-based address allocation support on the Cisco IOS DHCP server for the industrial Ethernet platform. The DHCP server provides address assignment support based on the point of attachment of the client to the network. The following commands were introduced or modified: **address client-id**, **address hardware-address**, **ip dhcp server use subscriber-id client-id**, **ip dhcp subscriber-id interface-name**, **ip dhcp use subscriber-id client-id**, **reserved-only**, and **show ip dhcp pool**.



CHAPTER 11

DHCPv6 Repackaging

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) repackaging feature consists of DHCPv6 individual address assignment and stateless DHCPv6.

The DHCPv6 Individual Address Assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected.

The stateless DHCPv6 feature allows DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node.

- Finding Feature Information, page 127
- Information About DHCPv6 Repackaging, page 128
- How to Configure DHCPv6 Repackaging, page 129
- Configuration Examples for DHCPv6 Repackaging, page 137
- Additional References, page 140
- Feature Information for DHCPv6 Repackaging, page 140

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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 DHCPv6 Repackaging

DHCPv6 Prefix Delegation

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

- Stateful prefix delegation—Address assignment is centrally managed and clients must obtain configuration information such as address autoconfiguration and neighbor discovery that is not available through protocols.
- Stateless prefix delegation—Stateless configuration parameters do not require a server to maintain any dynamic state for individual clients, such as Domain Name System (DNS) server addresses and domain search list options.

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

Node Configuration Without Prefix Delegation

Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6) allows the DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. The use of stateless DHCPv6 is controlled by router advertisement (RA) messages that are multicast by devices. The DHCPv6 client invokes stateless DHCPv6 when it receives an RA. The DHCPv6 server responds to a stateless DHCPv6 request with configuration parameters, such as the Domain Name System (DNS) servers and domain search list options.

DHCPv6 Address Assignment

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

How to Configure DHCPv6 Repackaging

Configuring DHCPv6 Address Assignment

Prerequisites for Configuring DHCPv6 Address Assignment

By default, no Dynamic Host Configuration Protocol for IPv6 (DHCPv6) features are configured on the device.

When you configure DHCPv6 address assignment, remember that the specified interface must be one of these Layer 3 interfaces:

- Switch virtual interface (SVI): a VLAN interface created when you enter the **interface vlan** *vlan-id* command.
- EtherChannel port channel in Layer 3 mode: a port-channel logical interface created when you enter the **interface port-channel** *port-channel-number* command.

Enabling the DHCPv6 Server Function on an Interface

Perform this task to enable the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server function on an interface. Note that to delete a DHCPv6 pool, you must use the **no ipv6 dhcp pool** *poolname* global configuration command. Use the **no** form of the DHCP pool configuration mode commands to change the DHCPv6 pool characteristics. To disable the DHCPv6 server function on an interface, use the **no ipv6 dhcp server** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp pool** *poolname*
4. **address prefix** *ipv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}]
5. **link-address** *ipv6-prefix*
6. **vendor-specific** *vendor-id*
7. **suboption** *number* {**address** *ipv6-address* | **ascii** *ascii-string* | **hex** *hex-string*}
8. **exit**
9. **exit**
10. **interface** *type number*
11. **ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]
12. **end**
13. Do one of the following:
    - **show ipv6 dhcp pool**
    - **show ipv6 dhcp interface**
14. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device(config)# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool engineering`	Enters DHCP for IPv6 pool configuration mode, and defines the name of the IPv6 DHCP pool.
Step 4	**address prefix** *ipv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime*	**infinite**}]	(Optional) Specifies an address prefix for address assignment.

	Command or Action	Purpose
	Example: `Device(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite`	• This address must be in hexadecimal, using 16-bit values between colons. • **lifetime** *valid-lifetime preferred-lifetime*—Specifies a time interval (in seconds) that an IPv6 address prefix remains in the valid state.
Step 5	**link-address** *ipv6-prefix* **Example:** `Device(config-dhcpv6)# link-address 2001:1001::0/64`	(Optional) Specifies a link-address IPv6 prefix. • When an address on the incoming interface or a link address in the packet matches the specified IPv6 prefix, the server uses the configuration information pool.
Step 6	**vendor-specific** *vendor-id* **Example:** `Device(config-dhcpv6)# vendor-specific 9`	(Optional) Enters DHCPv6 vendor-specific configuration mode with the vendor-specific identification number.
Step 7	**suboption** *number* {**address** *ipv6-address* | **ascii** *ascii-string* | **hex** *hex-string*} **Example:** `Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1`	(Optional) Enters a vendor-specific suboption number.
Step 8	**exit** **Example:** `Device(config-dhcpv6-vs)# exit`	Returns to DHCP pool configuration mode.
Step 9	**exit** **Example:** `Device(config-dhcpv6)# exit`	Returns to global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Enters interface configuration mode, and specifies the interface to configure.
Step 11	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**]	Enables the DHCPv6 server function on an interface.

	Command or Action	Purpose
	Example: `Device(config-if)# ipv6 dhcp server rapid-commit`	
Step 12	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 13	Do one of the following: • **show ipv6 dhcp pool** • **show ipv6 dhcp interface** **Example:** `Device# show ipv6 dhcp pool`	Verifies DHCPv6 pool configuration or verifies that the DHCPv6 server function is enabled on an interface.
Step 14	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling the DHCPv6 Client Function on an Interface

Perform this task to enable the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client function on an interface. To disable the DHCPv6 client function, use the **no ipv6 address dhcp** interface configuration command. To remove the DHCPv6 client request, use the **no ipv6 address dhcp client request vendor** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address dhcp** [**rapid-commit**]
5. **ipv6 address dhcp client request vendor**
6. **end**
7. **show ipv6 dhcp interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/0`	Enters interface configuration mode, and specifies the interface to configure.
Step 4	**ipv6 address dhcp** [**rapid-commit**] **Example:** `Device(config-if)# ipv6 address dhcp rapid-commit`	Enables the interface to acquire an IPv6 address from the DHCPv6 server.
Step 5	**ipv6 address dhcp client request vendor** **Example:** `Device(config-if)# ipv6 adress dhcp client request vendor`	(Optional) Enables the interface to request the vendor-specific option.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show ipv6 dhcp interface** **Example:** `Device# show ipv6 dhcp interface`	Verifies that the DHCPv6 client is enabled on an interface.

Configuring the Stateless DHCPv6 Function

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

Configuring the Stateless DHCPv6 Server

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp pool** *poolname* **Example:** `Device(config)# ipv6 dhcp pool dhcp-pool`	Configures a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) configuration information pool and enters DHCPv6 pool configuration mode.
Step 4	**dns-server** *ipv6-address* **Example:** `Device(config-dhcp)# dns-server 2001:DB8:3000:3000::42`	Specifies the Domain Name System (DNS) IPv6 servers available to a DHCPv6 client.
Step 5	**domain-name** *domain* **Example:** `Device(config-dhcp)# domain-name example.com`	Configures a domain name for a DHCPv6 client.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-dhcp)# exit`	Exits DHCPv6 pool configuration mode, and returns the device to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface serial 3`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 8	**ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*] [**allow-hint**] **Example:** `Device(config-if)# ipv6 dhcp server dhcp-pool`	Enables DHCPv6 on an interface.
Step 9	**ipv6 nd other-config flag** **Example:** `Device(config-if)# ipv6 nd other-config flag`	Sets the “other stateful configuration” flag in IPv6 router advertisements (RAs).
Step 10	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuring the Stateless DHCPv6 Client

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface serial 3`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 address autoconfig** [**default**] **Example:** `Device(config-if)# ipv6 address autoconfig`	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Enabling Processing of Packets with Source Routing Header Options

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 source-route** **Example:** `Device(config)# ipv6 source-route`	Enables processing of the IPv6 type 0 routing header.
Step 4	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for DHCPv6 Repackaging

Examples: Configuring the DHCPv6 Server Function

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

```
ipv6 dhcp pool dhcp-pool
 prefix-delegation pool client-prefix-pool1 lifetime 1800 600
 dns-server 2001:DB8:3000:3000::42
 domain-name example.com
!
interface Ethernet 0/0
 description downlink to clients
 ipv6 address FEC0:240:104:2001::139/64
 ipv6 dhcp server dhcp-pool
```

```
!
ipv6 local pool client-prefix-pool1 2001:DB8:1200::/40 48
```

The following example from the **show ipv6 dhcp** command shows the DHCP unique identifier (DUID) of the device:

```
Device# show ipv6 dhcp

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

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

```
Device# show ipv6 dhcp binding

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

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

```
Device# show ipv6 dhcp database

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

Example: Configuring the DHCPv6 Client Function

In the following example, this Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client has three interfaces. Ethernet interface 0/0 is the upstream link to a service provider, which has a DHCPv6 server function enabled. The Fast Ethernet interfaces 0/0 and 0/1 are links to local networks.

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

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

```
interface Ethernet 0/0
 description uplink to provider DHCP IPv6 server
 ipv6 dhcp client pd prefix-from-provider
!
interface FastEthernet 0/0
 description local network 0
 ipv6 address prefix-from-provider ::5:0:0:0:100/64
!
interface FastEthernet 0/1
 description local network 1
 ipv6 address prefix-from-provider ::6:0:0:0:100/64
```

Example: Configuring the Stateless DHCPv6 Function

The following example shows how to use the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) function to configure clients with information about the name lookup system. The server is configured with a DHCP pool, which contains the name lookup information that is to be passed to clients. It does not need to contain a prefix pool. This DHCP pool is attached to the access link to customers (Ethernet 0/0) when you enter the **ipv6 dhcp server** command. The access link also has the **ipv6 nd other-config-flag** command enabled. Router advertisement (RA) messages sent from this interface inform clients that they should use DHCPv6 for “other” (for example, nonaddress) configuration information.

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

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

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

Additional References

Related Documents

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

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

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 DHCPv6 Repackaging

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 . An account on Cisco.com is not required.

Table 14: Feature Information for DHCPv6 Repackaging

Feature Name	Releases	Feature Information
DHCPv6 Repackaging	Cisco IOS XE Release 3.2SE	The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) repackaging feature consists of DHCPv6 individual address assignment and stateless DHCPv6. The DHCPv6 Individual Address Assignment feature manages nonduplicate address assignment in the correct prefix based on the network where the host is connected. The stateless DHCPv6 feature allows DHCPv6 to be used for configuring a node with parameters that do not require a server to maintain any dynamic state for the node. The following commands were introduced or modified: **address prefix**, **dns-server**, **domain-name**, **ipv6 address autoconfig**, **ipv6 dhcp pool**, **ipv6 dhcp server**, **ipv6 nd other-config-flag**, **ipv6 source-route**, **link-address**, **show ipv6 dhcp interface**, **show ipv6 dhcp pool**, **suboption**, **vendor-specific**.

INDEX

B

binding database 49

C

configuring nodes without prefix delegation 48, 128
creating and configuring the DHCP for IPv6 configuration pool, task 53

D

DHCP for IPv6 automatic binding 49
DHCP for IPv6 client function 49
DHCP for IPv6 configuration information pool 49
DHCP for IPv6 server function 49
DHCP for IPv6 server selection 49
DHCP unique identifier (DUID) 48
DHCPv6 129
  configuration guidelines 129
  default configuration 129

I

Identity Association for Prefix Delegation (IAPD) 49

P

prefix assignment in DHCP for IPv6 49

R

rapid commit in DHCP for IPv6 48
router advertisement message 48, 128