

Configuring the Cisco IOS XE DHCP Server

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

In a high availability set up DHCP servers are deployed in an active/standby deployment model where two CiscoIOS XE DHCP servers synchronize DHCP bindings (IP address records). This synchronization ensures that if the active device fails, the standby device seamlessly assumes the Active role, preserving IP address records and maintaining uninterrupted network service.

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

- Prerequisites for Configuring the DHCP Server, on page 1
- Information About the Cisco IOS XE DHCP Server, on page 2
- How to Configure the Cisco IOS XE DHCP Server, on page 7
- Configuration Examples for the Cisco IOS XE DHCP Server, on page 41
- Additional References, on page 48
- Feature Information for the Cisco IOS XE DHCP Server, on page 49

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 XE 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.

The DHCP server assigns IP addresses from specified address pools on a router to DHCP clients and manages them. If the DHCP server cannot give the DHCP client the requested configuration parameters from its database, it forwards the request to one or more secondary DHCP servers defined by the network administrator.

Database Agents

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

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

Address Conflicts

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

DHCP Address Pool Conventions

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

DHCP Address Pool Selection

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

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

- If the client is not directly connected (the giaddr field of the DHCPDISCOVER broadcast message is non-zero), the DHCP server matches the DHCPDISCOVER with a DHCP pool that has the subnet that contains the IP address in the giaddr field. Giaddr field is the gateway IP address field of a DHCP packet.

A DHCP relay agent sets the gateway address and adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

- If the client is directly connected (the giaddr field is zero), the DHCP server matches the DHCPDISCOVER with DHCP pool(s) that contain the subnet(s) configured on the receiving interface. If the interface has secondary IP addresses, the subnets associated with the secondary IP addresses are examined for possible allocation only after the subnet associated with the primary IP address (on the interface) is exhausted.

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

Address Bindings

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

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

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



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

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

Ping Packet Settings

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

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

DHCP Attribute Inheritance

The DHCP server database is organized as a tree. The root of the tree is the address pool for natural networks, branches are subnetwork address pools, and leaves are manual bindings to clients. Subnetworks inherit network

parameters and clients inherit subnetwork parameters. Therefore, common parameters (for example, the domain name) should be configured at the highest (network or subnetwork) level of the tree.

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

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

DHCP Server Address Allocation Using Option 82

The Cisco IOS 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.

DHCP Address Allocation Using Option 82 Feature Design

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

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

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

Usage Scenario for DHCP Address Allocation Using Option 82

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

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

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

DHCP Class Capability

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

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

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

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

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

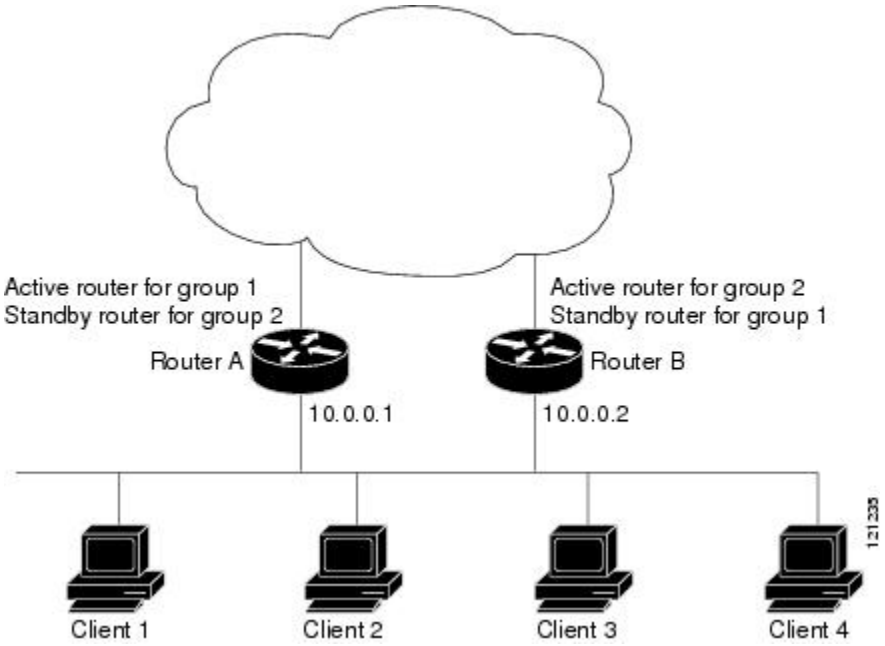
RegEx and Longest Match Support

DHCP server software supports advanced capabilities for IP address allocation. Earlier, DHCP server supported only exact match on hexadecimal codes. Effective with Cisco IOS XE Fuji 16.9.1, DHCP server is enhanced to support Regular expression (RegEx) based match or longest match. DHCP server provides options to set of DHCP clients with Vendor Class ID (VCI). Each set of clients are serviced from specific DHCP pool with one or more Vendor Classes. RegEx based Vendor Class Identifier match is included to support this feature.

For one class option, either Exact Match or Regex Match or Longest Match is supported. The configured Regex or hexadecimal string is matched against VCI string received in DHCP packets. In case of successful match, server assigns an IP address from the address range specified in pool class configuration. In case of multiple class match, the first occurrence of the match is considered. In case of no match, no address is allocated.

DHCP Server High Availability

DHCP server high availability is a feature that configures a DHCP server on two Cisco IOS XE devices, with one device designated as active and the other as standby. This feature synchronizes DHCP Server bindings to prevent conflicts and ensures a seamless, uninterrupted failover. In a high availability deployment when there a DHCP server failure, DHCP discovery is not initiated as IP address bindings are preserved. The active and standby states of the DHCP server are determined by the redundancy group states. The DHCP Server (Cisco IOS XE device) which assumes the role of standby never processes any DHCP packets. For information on redundancy group, see Configuring Stateful Interchassis Redundancy



How to Configure the Cisco IOS XE 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

Procedure

	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, known as a database agent. When setting this up, ensure the file name is added as part of the ftp/tftp URL. Alternatively, you can choose to disable DHCP address conflict logging.

	Command or Action	Purpose
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 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

Procedure

	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.

	Command or Action	Purpose
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.
- If you want to unconfigure the last DHCP pool when the DHCP traffic is active, ensure to have one of the following configurations:
  1. **ip dhcp pool** <*dummy_pool*> any dummy pool without any configuration

     OR
  2. **ip helper-address** x.x.x.x on dummy interface(loopback)

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 section for information on secondary subnets).

- Decide on a NetBIOS node type (b, p, m, or h).
- Decide on a DNS domain name.
- Configure Stateful Interchassis Redundancy to configure pairs of DHCP servers to act as backups for each other. See Configuring Stateful Interchassis Redundancy



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. **redundancy** *redundancy-group id*
5. **utilization mark high** *percentage-number* [**log**]
6. **utilization mark low** *percentage-number* [**log**]
7. **network** *network-number* [*mask* | */prefix-length*] [**secondary**]
8. **domain-name** *domain*
9. **dns-server** *address* [*address2 ... address8*]
10. **bootfile** *filename*
11. **next-server** *address* [*address2 ... address8*]
12. **netbios-name-server** *address* [*address2 ... address8*]
13. **netbios-node-type** *type*
14. **default-router** *address* [*address2 ... address8*]
15. **option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*}
16. **import** {**all** | **interface** *interface_name*
17. **lease** {*days* [*hours* [*minutes*]] | **infinite**}
18. **end**

DETAILED STEPS

Procedure

	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	**redundancy** *redundancy-group id* **Example:** `Device(config)# redundancy 1`	Configures redundancy for the DHCP pool. Only two redundancy groups are supported. One in the active mode and the other in the standby mode.
Step 5	**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 6	**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 7	**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 8	**domain-name** *domain* **Example:**	Specifies the domain name for the client.

	Command or Action	Purpose
	`Device(dhcp-config)# domain-name cisco.com`	
Step 9	**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 10	**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 11	**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. • 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 12	**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 13	**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 14	**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

	Command or Action	Purpose
		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 15	**option** *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | *ip-address*} **Example:** `Device(dhcp-config)# option 19 hex 01`	(Optional) Configures DHCP server options. Configuration supports Longest match and RegEx match for option 60. The **option code** sub command can be used to configure any DHCP options.

Step 16	**import** {**all** | **interface** *interface_name*
	Example:
	`Device(dhcp-config)# import all`
	`Device(dhcp-config) # import interface Ethernet0/0`
		The **import all** command learns options from all the interfaces.
		The **import interface** learns options only from the specified interface.

Step 17	**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.
Step 18	**end** **Example:** `Device(dhcp-config)# end`	Returns to privileged EXEC mode.

Sample configuration for DHCP High Availability

This configuration sets up redundancy groups for DHCP synchronization between interfaces and configures VRF-specific DHCP pools with associated network ranges. It also assigns IP addresses to interfaces with VRF forwarding and configures VRRP for high availability with priority and tracking for failover control.

```
redundancy
 mode none
 application redundancy
  group 1
   name dhcp_sync_portchannel_1
   timers delay 10 reload 180
```

```
   control TenGigabitEthernet0/0/2 protocol 1

   data TenGigabitEthernet0/0/2

   track-enable 1
   priority 110
   preempt
  group 2

   name dhcp_sync_portchannel_2

   timers delay 10 reload 180

   control TenGigabitEthernet0/0/2 protocol 1

   data TenGigabitEthernet0/0/2

   track-enable 2
   priority 100
   preempt
!
interface TenGigabitEthernet0/0/2
 ip address 10.2.30.18 255.255.255.0
 no ip redirects
 load-interval 30
 speed 1000
 arp timeout 1200
!

ip dhcp pool vrf-1-TenGigabitEthernet0/1/3

 vrf 1

 network 10.20.0.0 255.255.0.0

 redundancy 1

!

ip dhcp pool vrf-2-TenGigabitEthernet0/1/0

 vrf 2

 network 192.168.0.0 255.255.0.0

 redundancy 2
!
interface TenGigabitEthernet0/1/3
 vrf forwarding 1
 ip address 10.20.24.18 255.255.0.0
 no ip redirects
 load-interval 30
 speed 1000
redundancy group 1 ip 10.20.24.100 exclusive
decrement 20
redundancy rii 40
arp timeout 1200
 vrrp 2 address-family ipv4
  track 1 decrement 10
priority 110
  address 10.20.24.100 primary
  exit-vrrp
!
```

```
interface TenGigabitEthernet0/0/6
 vrf forwarding 2
 ip address 192.168.1.18 255.255.0.0
 speed 1000
redundancy group 1 ip 192.168.1.100 exclusive
decrement 20
redundancy rii 50
 vrrp 1 address-family ipv4
  track 2 decrement 10
priority 100
  address 192.168.1.100 primary
  exit-vrrp
```

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

Procedure

	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	**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.

	Command or Action	Purpose
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. • 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:**	(Optional) Specifies the NetBIOS node type for a Microsoft DHCP client.

	Command or Action	Purpose
	`Device(dhcp-config)# netbios-node-type h-node`	
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.
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.

	Command or Action	Purpose
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

Procedure

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

	Command or Action	Purpose
	`Device> enable`	
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.
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

Procedure

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

	Command or Action	Purpose
	`Device# configure terminal`	
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.
		  • 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 fo

Step 6	**hardware-address** *hardware-address* [*protocol-type* | *hardware-number*] **Example:**	Specifies a hardware address for the client. • This command is used for BOOTP requests.

	Command or Action	Purpose
	`Device(dhcp-config)# hardware-address b708.1388.f166 ethernet`	**Note** The hardware address specified here is c 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

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**

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/arp-parameters.xhtml in the “Number Hardware Type” list.

Field	Description
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/arp-parameters.xhtml 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 https://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

Procedure

	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 URL using the **origin file** command, you mu 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.
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.



Note It is not recommended to use DHCP ping checks on Cisco Catalyst switches implemented in switch stack or VSS.

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

Procedure

	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. • 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:**	(Optional) Specifies the duration the DHCP server waits for a ping reply from an address pool.

	Command or Action	Purpose
	`Device(config)# ip dhcp ping timeout 850`	
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

Procedure

	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:

Note When two servers provide DHCP addresses to a single device configured with **ip address dhcp** on two different interfaces, the imported information is merged and, for those options that take a single value, the last known option value will be used.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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.

Step 5	**import** {**all**	**interface** *interface_name*
		Example:
		`Device(dhcp-config)# import all`
		`Device(dhcp-config) # import interface Ethernet0/0`
			Imports DHCP option parameters into the DHCP server database.

Step 6	**exit** **Example:**	Exits DHCP pool configuration mode and enters global configuration mode.

	Command or Action	Purpose
	`Device(dhcp-config)# exit`	
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

Restrictions for DHCP Address Allocation Using Option 82

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

Enabling Option 82 for DHCP Address Allocation

By default, the Cisco 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

Procedure

	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

Procedure

	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. • 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:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(dhcp-class-relayinfo)# end`	

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 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

Procedure

	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# 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:**	Configures the subnet and mask for a DHCP address pool on a Cisco IOS DHCP server.

	Command or Action	Purpose
	`Device(dhcp-config)# network 10.0.20.0`	
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

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

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

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

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

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

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 router option 3.

Note

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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 route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} **dhcp** [*distance*]
	Example:
	`Device(config)# ip route 209.165.200.225 255.255.255.255 GigabitEthernet 0/0/0 dhcp`
	Example:
	`Device(config)# ip route 209.165.200.226 255.255.255.255 GigabitEthernet 0/0/1 dhcp 20`
		Assigns a static route for the default next-hop router when the DHCP server is accessed for an IP address.
		• If more than one interface on a router is configured to obtain an IP address from a DHCP server, use the **ip route** *prefix mask interface-type interface-number* **dhcp** command for each interface. If the interface is not specified, the route is added to the routing table as soon as any of the interfaces obtain an IP address and default router.

Step 4	**end** **Example:** `Device(config)# end`	Returns to global configuration mode.
Step 5	**show ip route**	(Optional) Displays the current state of the routing table.

	Command or Action	Purpose
	Example: `Device# show ip route`	• Use this command to display assigned static routes once the DHCP client obtains an address and a default router address from the DHCP server.

Clearing DHCP Server Variables

Perform this task to clear DHCP server variables:

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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*	*****} **Example:** `Device# clear ip dhcp binding *`	Deletes an automatic address binding from the DHCP database. • Specifying the *address* argument clears the automatic binding for a specific (client) IP address, whereas specifying an asterisk (*****) clears all automatic bindings.
Step 3	**clear ip dhcp conflict** {*address*	*****} **Example:** `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 XE 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

Pool 0 (Network 172.16.0.0)	Pool 1 (Subnetwork 172.16.1.0)	Pool 2 (Subnetwork 172.16.2.0)			
DNS server	172.16.1.102 172.16.2.102	—	—	—	—
NetBIOS name server	172.16.1.103 172.16.2.103	—	—	—	—
NetBIOS node type	h-node	—	—	—	—

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

The following example shows how to configure DHCP pool to support RegEx feature:

```
!
ip dhcp pool test
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
 dns-server 40.0.0.100
 class cisco_devices
  address range 192.168.10.2 192.168.10.100
!
class smart_phones
  address range 192.168.10.101 192.168.10.220
!
!
ip dhcp class cisco_devices
 option 60 cisco_string ----------------------<this is option 60 VCI string, exact match>
!
ip dhcp class smart_phones
 option 60 smartphone* ----------------------<option 60 VCI string, regex match>
!
```

The following example shows how to configure DHCP server class:

```
Router#
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp class HATHWAY_STB
Router(config-dhcp-class)#?
```

```
DHCP class configuration commands:
  exit        Exit from DHCP class configuration mode
  no         Negate a command or set its defaults
 option   Raw DHCP options
  relay    Enter relay agent information option configuration submode
  remark  Specify a remark for this class

Router(config-dhcp-class)#option ?
  <0-254>  DHCP option code

Router(config-dhcp-class)#option 60 ?
  hex  Specify hex value of the option
  WORD  Specify a regular expression string

Router(config-dhcp-class)#option 60 stb*  ?
<cr>
```

The following example shows how to Import options learnt on specific interface to LAN side DHCP pool:

```
!
ip dhcp pool LAN_Pool
import interface Ethernet0/0
!

Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ip dhcp pool pc_pool
Router(dhcp-config)# import ?
  all              all DHCP options
  interface   Select an interface to import options
Router(dhcp-config)# import interface Ethernet0/1
```

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	—	—	—	—
NetBIOS node type	h-node	—	—	—	—

```
ip dhcp database ftp://user:password@172.16.4.253/router-dhcp write-delay 120
ip dhcp excluded-address 172.16.0.100 172.16.1.103
ip dhcp excluded-address 172.16.1.100 172.16.1.101
!
ip dhcp pool pool3
 network 172.16.0.0 /16
 default-router 172.16.0.100 172.16.2.101 172.16.0.102 172.16.0.103
 domain-name cisco.com
 dns-server 172.16.1.102 172.16.2.102
 netbios-name-server 172.16.1.103 172.16.2.103
 netbios-node-type h-node
 lease 30
!
 network 172.16.1.0 /24 secondary
  override default-router 172.16.1.100 172.16.1.101
  end
!
 network 172.16.2.0 /24 secondary
```

Configuring Manual Bindings Example

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

```
ip dhcp pool Mars
 host 172.16.2.254
```

```
 hardware-address 02c7.f800.0422 ieee802
 client-name Mars
```

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

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

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:

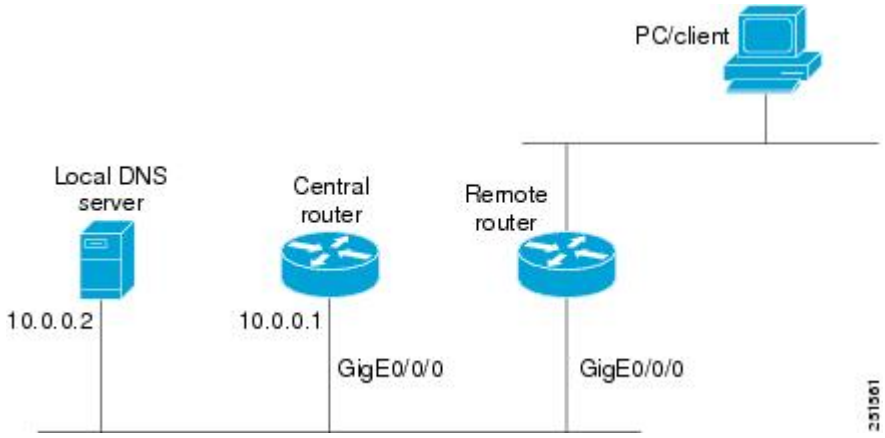
```
no service dhcp
service dhcp
ip dhcp pool abcpool
origin file tftp://10.1.0.1/staticfilename
```

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*.

Importing DHCP Options Example

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

Figure 1: DHCP Example Network Topology



Central Router

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

Remote Router

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

Configuring DHCP Address Allocation Using Option 82 Example

This example configures two DHCP classes. CLASS1 defines the group of DHCP clients whose address requests contain the relay agent information option with the specified hexadecimal values. CLASS2 defines the group of DHCP clients whose address requests contain the configured relay agent information suboptions.

CLASS3 has no pattern configured and is treated as a “match to any” class. This type of class is useful for specifying a “default” class.

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

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

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

```
! Defines the DHCP classes and relay information patterns
ip dhcp class CLASS1
 relay agent information
  relay-information hex 01030a0b0c02050000000123
  relay-information hex 01030a0b0c02*
  relay-information hex 01030a0b0c02050000000000 bitmask 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 11.0.20.0 255.255.255.0
 class CLASS1
  address range 11.0.20.1 11.0.20.64
 class CLASS2
```

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

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

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

Additional References

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 XE DHCP Relay Agent" module
DHCP client configuration	"Configuring the Cisco IOS XE DHCP Client" module
DHCP On-Demand Address Pool Manager	"Configuring the DHCP On-Demand Address Pool Manager" module

Standards and RFCs

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

Technical Assistance

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

Feature Information for the Cisco IOS XE DHCP Server

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

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

Table 4: Feature Information for the Cisco IOS XE DHCP Server

Feature Name	Releases	Feature Configuration Information
DHCP Server	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.9S	Cisco routers running Cisco IOS XE software include Dynamic Host Configuration Protocol (DHCP) server and relay agent software. The Cisco IOS XE DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. The DHCP server can be configured to assign additional parameters such as the IP address of the domain name system (DNS) server and the default router.
DHCP Address Allocation Using Option 82	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.9S	The Cisco IOS XE DHCP server can allocate dynamic IP addresses based on the relay information option (option 82) information sent by the relay agent. The following commands were introduced by this feature: **address range**, **class**, **ip dhcp class**, **ip dhcp use class**, **relay agent information**, **relay-information hex**.
DHCP Statically Configured Routes Using a DHCP Gateway	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.9S	This feature enables the configuration of static routes that point to an assigned DHCP next hop router. The following commands were modified by this feature: **ip route**, **show ip route**.
DHCP Server Options - Import and Autoconfiguration	Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.9S	Options imported by multiple subsystems can co-exist in the DHCP address pool. When the session is terminated or the lease is released, the imported options are cleared.
DHCP Server Multiple Subnet	12.4(15)T 12.2(33)SRB 15.3(1)S Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.9S	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**.

Feature Name	Releases	Feature Configuration Information
DHCP Static Mapping	Cisco IOS XE Release 3.9S	Configuring static mapping pools enables the DHCP server to read the static bindings from a separate text file (similar in format to the DHCP database file) that is stored in special pools. The following commands were introduced or modified: **origin**.
DHCP Server Import All Enhancement	Cisco IOS XE Release 3.9S	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.
DHCPv4 Client options	Cisco IOS XE Fuji Release 16.9.1	The following features are supported on Cisco 4000 Series ISRs: • Regular Expression support for options 60, 77, 124 and 125 • Generic support to configure all applicable client DHCP options • Import options learnt on specific interface to DHCP pool • Longest Match support for option 60, 77, 124 and 125
DHCP Server High Availability	Cisco IOS XE 17.18.2	Enables an active or standby deployment of DHCP servers on two Cisco IOS XE devices. This feature synchronizes DHCP bindings between peers to ensure IP address preservation during a failover event. Implementation requires Stateful Interchassis Redundancy and introduces the `redundancy` command within the DHCP pool configuration mode.