



DHCP Configuration Guide

First Published: 2025-08-25

Last Modified: 2026-07-17

Americas Headquarters

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



Read Me First

Only supported features are documented. To confirm or clarify all the supported features for a platform, go to [Cisco Feature Navigator](#).

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 –2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

[Read Me First](#) **ii**

CHAPTER 1

[Dynamic Host Configuration Protocol](#) **1**

[Feature History for DHCP](#) **1**

[Introduction to DHCP](#) **2**

[What is DHCP?](#) **2**

[How DHCP Works](#) **2**

[DHCP Components](#) **3**

[DHCP Zero Touch](#) **4**

[How to Configure DHCP](#) **4**

[Configure a DHCPv4 Server](#) **4**

[Configure a DHCPv4 client](#) **5**

[Configure a DHCPv4 Relay Agent](#) **6**

[Configure a DHCPv6 Server](#) **7**

[Configure a DHCPv6 Client](#) **8**

[Configure a DHCPv6 Relay Agent](#) **9**

CHAPTER 2

[Advanced DHCP Features](#) **11**

[Feature History for Advanced DHCP Features](#) **11**

[Advanced DHCPv4 features](#) **12**

[DHCP option 12: host name](#) **12**

[Configure DHCP option 12](#) **12**

[DHCP Option 43: vendor-specific information](#) **13**

[Configure DHCP Option 43](#) **13**

[DHCP Option 82: relay agent information](#) **14**

[Configure DHCP Option 82 - configurable Circuit ID and Remote ID](#) **14**

Configure DHCP Option 82 - data insertion	15
Configure DHCP Option 82 - pass through	15
DHCP Server configuration to ignore all BOOTP requests	16
Configure DHCP server to ignore BOOTP requests	16
DHCP relay agent support on unnumbered interfaces	17
Configure DHCP relay agent on unnumbered interfaces	17
DHCP syslog	18
Advanced DHCPv6 features and DHCPv6 options	18
DHCPv6 - NIS, NISP, SNTP and Information Refresh Options	19
Configure DHCPv6 NIS, NISP, SNTP, and Information Refresh Options	19
DHCPv6 bulk lease query - RFC 5460	20
How BLQ works	20
DHCPv6 Relay Agent notification for prefix delegation	20
Configure DHCPv6 Relay Agent notification for prefix delegation	21
DHCPv6 Relay source	21
Configure DHCPv6 Relay source	21
DHCPv6 Server Stateless Address Autoconfiguration	22
Configure DHCPv6 Server Stateless AutoConfiguration	22
VRF-aware DHCPv6 Server and Relay for IANA and prefix delegation	23
Configure VRF-aware DHCPv6 Server and Relay for IANA and prefix delegation	23

CHAPTER 3

Specialized DHCP deployments and client customization 25

Feature history for specialized DHCP deployments and client customization	25
Configurable DHCP clients	26
Configure DHCP client ID	26
Configure DHCP client to request specific options	27
SSO - DHCP ODAP client-server	27
How SSO - DHCP ODAP works	28
Configure DHCP server for ODAP	28



CHAPTER 1

Dynamic Host Configuration Protocol

- [Feature History for DHCP, on page 1](#)
- [Introduction to DHCP, on page 2](#)
- [What is DHCP?, on page 2](#)
- [How DHCP Works, on page 2](#)
- [DHCP Components, on page 3](#)
- [DHCP Zero Touch, on page 4](#)
- [How to Configure DHCP, on page 4](#)

Feature History for DHCP

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature history for DHCP

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1ea	DHCP: The DHCP feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Dynamic Host Configuration Protocol: DHCP provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP Server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP Server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Introduction to DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses, to connected devices. This automation simplifies network administration by eliminating the need for manual IP address assignment and management.

What is DHCP?

DHCP is a client-server protocol that automatically provides an IP host with its IP address and other related configuration information, such as the subnet mask, default gateway, and DNS server addresses. This enables devices to connect to a network without requiring manual configuration, making network management more efficient and less prone to errors.

How DHCP Works

The DHCP process typically involves four main steps, often referred to by the acronym DORA: Discover, Offer, Request, and Acknowledge. This process ensures that a client successfully obtains an IP address and other necessary network configuration from a DHCP server.

Summary

These stages describe how DHCP servers work:

1. Discover
2. Offer
3. Request
4. Acknowledge

Discover:

- Actor: DHCP Client
- Action: The client broadcasts a DHCP Discover message on the network to locate available DHCP servers. This message typically contains the client's MAC address

Offer

- Actor: DHCP Server
- Action: Upon receiving a Discover message, the DHCP server responds with a DHCP Offer message. This message includes a proposed IP address for the client, along with other configuration parameters (subnet mask, default gateway, DNS servers, lease time).

Request

- Actor: DHCP Client

- Action: The client receives one or more DHCP Offer messages and broadcasts a DHCP Request message. This message explicitly requests the offered IP address from a specific server (if multiple offers were received) and implicitly declines other offers.

Acknowledge

- Actor: DHCP Server
- Action: The selected DHCP server receives the DHCP Request message and sends a DHCP Acknowledge (ACK) message to the client. This message confirms the IP address lease and all other configuration parameters, officially assigning the IP address to the client.

Table 2: When the DHCP process completes successfully:

When the DHCP server...	Then...	And...
receives a DHCP Request message	it assigns the IP address to the client from its pool of available addresses	it updates its internal database to reflect the assigned IP address and lease time.
fails to receive a DHCP Request message	it reclaims the offered IP address	it makes the IP address available for other clients.
receives a DHCP Discover message	it checks its available IP address pools	it sends a DHCP Offer message to the client.

DHCP Components

DHCP relies on the interaction of three primary components: the client, the server, and optionally, the relay agent. Each plays a distinct role in the dynamic IP address assignment process.

DHCP client

A DHCP client is any network-enabled device (e.g., computer, smartphone, printer, router interface) configured to obtain its IP address and other network configuration parameters automatically from a DHCP server.

DHCP server

A DHCP server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. The server maintains a pool of IP addresses and information about client configurations.

DHCP relay

A DHCP relay agent is a network device, such as a router, that forwards DHCP messages between clients and servers when they are not on the same local network segment (broadcast domain). Relay agents are essential in larger networks where DHCP servers are centralized and clients are distributed across multiple subnets.

DHCP Zero Touch

DHCP Zero Touch is a provisioning method that leverages DHCP to automatically configure new devices when they are first connected to the network, minimizing manual intervention.

DHCP Zero Touch streamlines the deployment of network devices by allowing them to automatically discover the network, obtain an IP address via DHCP, and then download their configuration or software image from a centralized server (e.g., TFTP, HTTP) without requiring an administrator to manually configure each device. This process significantly reduces deployment time and human error, especially in large-scale rollouts.

How to Configure DHCP

This section provides basic configuration tasks for DHCPv4 clients, servers, and relay agents.

Configure a DHCPv4 Server

Use this procedure to configure your switch to act as a DHCPv4 server, providing IPv6 addresses to clients within a specified network segment.

This configuration is suitable for providing stateful IPv6 addresses and other parameters to clients.

Before you begin

- Identify the IP address range for the DHCP pool.
- Identify the default gateway, DNS servers, and domain name to be provided to clients.
- Ensure the interface connected to the clients is configured with an IP address within the same subnet as the DHCP pool.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Exclude IP addresses from the DHCP pool that should not be assigned to clients.

Example:

```
Device(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Note

These are typically static assignments for network devices like routers, servers, or other switches

Step 3 Create a DHCP pool and enter DHCP pool configuration mode.

Example:

```
Device(config)# ip dhcp pool VLAN10_POOL
Device(config-dhcpv6)#
```

Note

Replace VLAN10_POOL with a descriptive name for your DHCP pool

Step 4 Specify the network address for the DHCP pool.

Example:

```
Device(dhcp-config)# Device(dhcp-config)# network 192.168.1.0 255.255.255.0
```

Step 5 Configure the default gateway for clients.

Example:

```
Device(dhcp-config)# default-router 192.168.1.1
```

Step 6 Configure the DNS servers for clients.

Example:

```
Device(dhcp-config)# dns-server 8.8.8.8 8.8.4.4
```

Step 7 Configure the domain name for clients (optional).

Example:

```
Device(dhcp-config)# domain-name example.com
```

Step 8 Exit DHCP pool configuration mode and global configuration mode.

Example:

```
Device(dhcp-config)# exit
```

```
Device(dhcp-config)# end
```

What to do next

Verify DHCP server operation using commands like **show ip dhcp binding** and **show ip dhcp pool**.

.

Configure a DHCPv4 client

Use this procedure to configure a network interface on your switch to obtain its IPv4 address and other network parameters dynamically from a DHCP server.

This configuration is typically applied to interfaces that need to receive dynamic IP addresses, such as a management interface or an interface connecting to an ISP.

Before you begin

Ensure the interface is physically connected and administratively up.

Follow these steps to configure a DHCPv4 client:

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter interface configuration mode for the desired interface.

Example:

```
Device(config)# interface GigabitEthernet1/0/1
```

Step 3 Configure the interface to obtain an IP address via DHCP.

Example:

```
Device(config-if)# ip address dhcp
```

Step 4 Exit interface configuration mode.

Example:

```
Device(config-if)# end
```

What to do next

Verify the IP address assignment using the **show ip interface brief** command.

Configure a DHCPv4 Relay Agent

Use this procedure to configure your switch to act as a DHCPv4 relay agent, forwarding DHCP requests from clients to a DHCP server located on a different subnet.

This configuration is crucial in larger networks where a centralized DHCP server serves multiple VLANs or subnets.

-

Before you begin

- Identify the IP address of the DHCP server(s).
- Ensure the switch has IP connectivity to the DHCP server.
- Ensure the interface connected to the clients is configured with an IP address.

Follow these steps to configure a DHCPv4 relay agents.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter interface configuration mode for the interface connected to the DHCP clients.

Example:

```
Device(config)# interface Vlan10
```

Step 3 Configure the IP helper address to forward DHCP requests to the DHCP server.

Example:

```
Device(config-if) # ip helper-address 10.0.0.10
```

Note

Replace 10.0.0.10 with the actual IP address of your DHCP server. You can configure multiple helper addresses for redundancy.

Step 4 Exit interface configuration mode.

Example:

```
Device(config-if) # end
```

What to do next

Verify relay agent operation by checking DHCP server logs or by observing client IP address assignments.

Configure a DHCPv6 Server

Use this procedure to configure your switch to act as a DHCPv6 server, providing IPv6 addresses to clients within a specified network segment.

This configuration is suitable for providing stateful IPv6 addresses and other parameters to clients.

Before you begin

- Identify the IPv6 address range for the DHCPv6 pool.
- Ensure the interface connected to the clients is configured with an IPv6 address.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create a DHCPv6 pool and enter DHCPv6 pool configuration mode.

Example:

```
Device(config) # ipv6 dhcp pool VLAN20_IPV6_POOL  
Device(config-dhcpv6) #
```

Note

Replace *VLAN20_IPV6_POOL* with a descriptive name for your DHCPv6 pool.

Step 3 Specify the address prefix for the DHCPv6 pool.

Example:

```
DDevice(config-dhcpv6) # address prefix 2001:DB8:0:1::/64 lifetime infinite infinite  
Device(config-dhcpv6) #
```

Step 4 Configure the DNS servers for clients.

Example:

```
Device(config-dhcpv6) # dns-server 2001:4860:4860::8888
```

Step 5 Configure the domain name for clients (optional).

Example:

```
Device(config-dhcpv6) # domain-name example.com
```

Step 6 Exit DHCPv6 pool configuration mode and global configuration mode.

Example:

```
Device(config-dhcpv6) # exit
Device(config) # end
```

Step 7 Enable the DHCPv6 server on the relevant interface.

Example:

```
Device# configure terminal
Device(config) # interface Vlan20
Device(config-if) # ipv6 dhcp server VLAN20_IPV6_POOL
Device(config-if) # end
```

Note

This is typically a VLAN interface (SVI).

What to do next

Verify DHCPv6 server operation using commands like **show ipv6 dhcp binding** and **show ipv6 dhcp pool**.

Configure a DHCPv6 Client

Use this procedure to configure a network interface on your switch to obtain its IPv6 address and other network parameters dynamically from a DHCPv6 server.

This configuration is applied to interfaces that need to receive dynamic IPv6 addresses, often in conjunction with IPv6 stateless autoconfiguration (SLAAC).

Before you begin

Ensure the interface is physically connected and administratively up.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter interface configuration mode for the desired interface.

Example:

```
Device(config)# interface GigabitEthernet1/0/1
```

Step 3 Configure the interface to obtain an IPv6 address via DHCP.

Example:

```
Device(config-if)# ipv6 address dhcp
```

Step 4 Exit interface configuration mode.

Example:

```
Device(config-if)# end
```

What to do next

Verify the IPv6 address assignment using the **show ipv6 interface brief** command.

Configure a DHCPv6 Relay Agent

-
-

Before you begin

-

Procedure

Example:

-

Table 3:

If...	Then...

-

What to do next

-



CHAPTER 2

Advanced DHCP Features

This chapter delves into advanced configurations and functionalities for both DHCPv4 and DHCPv6, enabling more granular control, enhanced security, and improved scalability for IP address management. It covers various DHCP Options, server behaviors, and relay agent capabilities beyond basic address assignment.

- [Feature History for Advanced DHCP Features, on page 11](#)
- [Advanced DHCPv4 features, on page 12](#)
- [Advanced DHCPv6 features and DHCPv6 options, on page 18](#)

Feature History for Advanced DHCP Features

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 4: Feature History for Advanced DHCP Features

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1 ea	Advanced DHCP Features: The support for advanced DHCP features has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Advanced DHCP Features: Introduced the support for advanced configurations and functionalities for both DHCPv4 and DHCPv6, enabling more granular control, enhanced security, and improved scalability for IP address management. It covers various DHCP options, server behaviors, and relay agent capabilities beyond basic address assignment.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Advanced DHCPv4 features

DHCP Options

DHCP Options are additional configuration parameters that a DHCP server can provide to a client beyond the basic IP address, subnet mask, and default gateway. These Options are defined by RFCs, for example, RFC 2132 and allow for highly customized client configurations, supporting various network services and device types.

This section explores advanced features within DHCPv4, including the use of DHCP Options to provide specific client configurations, server behaviors for handling legacy requests, and relay agent enhancements.

DHCP option 12: host name

DHCP Option 12 allows a DHCP client to send its host name to the DHCP server, and conversely, allows the DHCP server to provide a host name to the client. This is useful for network identification and management.

Configure DHCP option 12

Use this procedure to configure DHCP Option 12 in a DHCPv4 pool, allowing the server to assign a host name to a client.

This is useful for environments where client devices are expected to have dynamically assigned host names or for logging purposes.

Before you begin

A DHCPv4 pool must already be configured on the switch.

Procedure

Step 1 Enter DHCP pool configuration mode for the desired pool.

Example:

```
Device# configure terminal  
Device(config)# ip dhcp pool VLAN10_POOL
```

Step 2 Configure the host name to be assigned to clients.

Example:

```
Device(dhcp-config)# option 12 ascii YOUR-HOSTNAME  
Device(dhcp-config)#exit  
Device(config)#end  
Device#
```

Note

The host name can be a static string or derived from client information.

What to do next

Verify client host name assignment on the client device or through DHCP server logs.

DHCP Option 43: vendor-specific information

DHCP Option 43 provides a mechanism for vendors to encapsulate their own vendor-specific information within DHCP messages. This is particularly useful for provisioning devices like IP phones, wireless access points, or other network appliances that require specific configuration parameters from their manufacturer.

Configure DHCP Option 43

Use this procedure to configure DHCP Option 43 in a DHCPv4 pool. The format of the data depends on the vendor specification.

This is essential for deploying specific vendor devices that rely on DHCP for initial configuration.

Before you begin

- A DHCPv4 pool must already be configured.
- Obtain the exact format and values for Option 43 from the vendor documentation.

Procedure

Step 1 Enter DHCP pool configuration mode for the desired pool.

Example:

```
Device# configure terminal
Device(config)# ip dhcp pool VLAN10_POOL
Device(dhcp-config)#
```

Step 2 Configure the vendor-specific information.

Example:

```
Device(dhcp-config)# option 43 hex <VENDOR_CODE> <HEX_DATA>
Device(dhcp-config)#
```

The **hex** keyword allows entering hexadecimal values, while **ascii** allows ASCII strings. Replace `VENDOR_CODE` and `HEX_DATA` with actual values.

Example for Cisco IP Phone TFTP server:

```
Device(dhcp-config)# option 43 ascii "24150.10.10.10.10"
Device(dhcp-config)# exit
Device(config)# end
Device#
```

In this example, 241 is the sub-option code for TFTP server, 50 is the length of the IP address, and 10.10.10.10 is the TFTP server IP.

What to do next

Verify that the vendor device correctly interprets and applies the received Option 43 data.

DHCP Option 82: relay agent information

DHCP Option 82, also known as the Relay Agent Information Option, allows a DHCP relay agent to insert information about itself and the client into a DHCP message before forwarding it to the DHCP server. This information helps the server make more intelligent decisions about IP address assignment, such as assigning addresses based on the client's physical location or the relay agent.

Configure DHCP Option 82 - configurable Circuit ID and Remote ID

Use this procedure to configure the content of the Remote ID and Circuit ID sub-options within DHCP Option 82 on a relay agent interface.

This is crucial for granular client identification and policy enforcement on the DHCP server.

Before you begin

The interface must be configured as a DHCP relay agent with the **ip helper-address** command.

Procedure

-
- Step 1** Enter interface configuration mode for the interface connected to the DHCP clients.

Example:

```
Device# configure terminal
Device(config)# interface Vlan222
Device(config-if)#
```

- Step 2** Configure the DHCP Option 82 information for the Circuit ID and Remote ID.

Example:

```
Device(config)#int hu1/0/29
Device(config-if)#switchport
Device(config-if)#ip dhcp snooping vlan 222 information option format-type circuit-id string
CODX_CIRCUIT_222
Device(config-if)#
```

Remote ID:

```
Device(config)#ip dhcp snooping information option format remote-id string CODX_REMOTE_9550
Device(config)#
```

You can specify the format for the Circuit ID and the Remote ID.

What to do next

Verify on the DHCP server that Option 82 data is received and correctly interpreted.

Configure DHCP Option 82 - data insertion

Use this procedure to enable the insertion of DHCP Option 82 information by the relay agent into client requests.

Before you begin

The interface must be configured as a DHCP relay agent with the **ip helper-address** command.

Procedure

-
- Step 1** Enter interface configuration mode for the interface connected to the DHCP clients.

Example:

```
Device# configure terminal
Device(config)# interface Vlan10
```

- Step 2** Enable the insertion of Option 82 information.

Example:

```
Device(config-if)# ip dhcp relay information option
Device(config-if)# end
Device#
```

By default, this command enables insertion. To disable, use **no ip dhcp relay information option** command.

What to do next

Monitor DHCP server logs for the presence of Option 82 data.

Configure DHCP Option 82 - pass through

Use this procedure to configure the DHCP relay agent to pass through DHCP Option 82 information received from other relay agents or clients, rather than stripping or modifying it.

This is important in multi-relay scenarios where Option 82 information needs to be preserved end-to-end.

Procedure

-
- Step 1** Enter global configuration mode.

Example:

```
Device# configure terminal
Device(config)#
```

- Step 2** Enable DHCP Option 82 - pass through.

Example:

```
Device(config)# ip dhcp snooping information option allow-untrusted
Device(config)# end
Device#
```

What to do next

Verify that the DHCP server receives Option 82 data from downstream relays as expected.

DHCP Server configuration to ignore all BOOTP requests

The Bootstrap Protocol (BOOTP) is an older protocol that DHCP superseded. While DHCP is backward compatible with BOOTP, in modern networks, it may be desirable for a DHCP server to ignore BOOTP requests to reduce processing overhead or prevent unintended IP assignments to legacy devices.

Configure DHCP server to ignore BOOTP requests

Use this procedure to configure the switch, when acting as a DHCP server, to ignore incoming BOOTP requests.

This is useful in environments where BOOTP is no longer used, or where a dedicated BOOTP server handles such requests.

Before you begin

The switch must be configured as a DHCP server.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Disable the BOOTP service.

Example:

```
Device(config)# ip dhcp bootp ignore
Device(config)#
```

Step 3 Exit global configuration mode.

Example:

```
Device(config)# end
Device#
```

What to do next

Confirm that no BOOTP clients are relying on this server for IP addresses.

DHCP relay agent support on unnumbered interfaces

Traditionally, DHCP relay agents operate on interfaces configured with an IP address. However, in some network designs, interfaces might be unnumbered. That is, they borrow an IP address from another interface. Supporting DHCP relay on unnumbered interfaces allows for more flexible network topologies, especially in point-to-point links.

Configure DHCP relay agent on unnumbered interfaces

Use this procedure to configure a DHCPv4 relay agent on an unnumbered interface.

This is typically used on point-to-point links where assigning a dedicated IP address to the interface is unnecessary.

Before you begin

- The unnumbered interface must be configured to borrow an IP address from another interface. For example, **ip unnumbered Loopback0**.
- The **ip helper-address** command must be applied to the unnumbered interface.

Procedure

Step 1 Enter interface configuration mode for the unnumbered interface.

Example:

```
Device# configure terminal  
Device(config)# interface GigabitEthernet1/0/2
```

Step 2 Configure the interface as unnumbered.

Example:

```
Device(config-if)# ip unnumbered Loopback0
```

Step 3 Configure the IP helper address on the unnumbered interface.

Example:

```
Device(config-if)# ip helper-address 10.0.0.10  
Device(config-if)# end  
Device#
```

For this step, use the IP address of your DHCP server.

What to do next

Verify DHCP client connectivity through the unnumbered interface.

DHCP syslog

DHCP Syslog refers to the logging of DHCP-related events and messages to a syslog server. This provides valuable insights into DHCP operations, including IP address assignments, lease renewals, errors, and other diagnostic information, which is crucial for network monitoring, troubleshooting, and auditing.

Information available through DHCP syslog

- IP address lease events: records when an IP address is assigned, renewed, released, or expired. This includes the client's MAC address and the assigned IP.
- DHCP pool utilization: provides notifications when DHCP pools are nearing exhaustion or are empty, indicating potential capacity issues
- DHCP Server errors: logs errors encountered by the DHCP server, such as conflicts, database issues, or communication failures
- DHCP Client activity: details client requests, offers, and acknowledgments, aiding in tracing specific client interactions
- DHCP Relay activity: logs events related to DHCP relay operations, including forwarded messages and any issues encountered

Benefits of DHCP Syslog

- Troubleshooting: quickly diagnose DHCP-related connectivity issues.
- Auditing and compliance: maintain records of IP address assignments for security and regulatory compliance
- Capacity planning: monitor pool utilization to proactively expand IP address ranges
- Security: detect unauthorized DHCP servers or suspicious client activity

System logging

DHCP syslog messages are typically enabled as part of the broader system logging configuration on Cisco devices. There isn't a dedicated DHCP Syslog command; rather, DHCP events are included in the standard syslog output based on the configured logging level. To enable logging, use commands like **logging host ip-address** and **logging trap level** in global configuration mode.

Advanced DHCPv6 features and DHCPv6 options

This section covers advanced features specific to DHCPv6, including various options for providing additional client information, bulk lease query capabilities, and enhanced relay agent functionalities.

Similar to DHCPv4, DHCPv6 utilizes options to provide clients with more than just an IPv6 address. These options are crucial for delivering comprehensive network configurations in IPv6 environments, supporting services like DNS, NTP, and other specialized information.

DHCPv6 - NIS, NISP, SNTP and Information Refresh Options

DHCPv6 can provide clients with Network Information Service (NIS), NISP (Network Information Service Plus), Simple Network Time Protocol (SNTP) server addresses, and information refresh parameters. These options ensure clients have access to essential network services.

Configure DHCPv6 NIS, NISP, SNTP, and Information Refresh Options

Use this procedure to configure DHCPv6 options for NIS, NISP, SNTP, and information refresh within a DHCPv6 pool.

Before you begin

A DHCPv6 pool must already be configured.

Procedure

- Step 1** Enter DHCPv6 pool configuration mode for the desired pool.

Example:

```
Device# configure terminal
Device(config)# ipv6 dhcp pool testv6
Device(config-dhcpv6)#
```

- Step 2** Configure NIS server addresses.

Example:

```
Device(config-dhcpv6)# nis server 2001:DB8::10
```

- Step 3** Configure NISP server addresses.

Example:

```
Device(config-dhcpv6)# nisp server 2001:DB8::11
```

- Step 4** Configure SNTP server addresses.

Example:

```
Device(config-dhcpv6)# sntp server 2001:DB8::12
```

- Step 5** (Optional) Configure the information refresh time.

Example:

```
Device(config-dhcpv6)# information refresh 86400
```

This specifies how often clients should refresh their non-address configuration information.

- Step 6** Exit DHCPv6 pool configuration mode and global configuration mode.

Example:

```
Device(config-dhcpv6) # exit
Device(config) # end
```

Clients will receive the configured NIS, NISP, and SNTP server addresses, and the specified information refresh time.

What to do next

Verify client configuration and service accessibility.

DHCPv6 bulk lease query - RFC 5460

DHCPv6 Bulk Lease Query (BLQ), defined in RFC 5460, provides a mechanism for a DHCPv6 server to query a client for a bulk list of its active leases. This is particularly useful for network management systems, lawful intercept, or other applications that require a comprehensive view of IP address assignments without querying individual clients.

Benefits of BLQ

- Centralized lease management: Network administrators can obtain a complete picture of active leases from a single point.
- Enhanced monitoring: facilitates real-time tracking of IP address usage
- Troubleshooting: aids in identifying rogue devices or unexpected lease activity

How BLQ works

This differs from standard DHCPv6 interactions where clients only request or renew their own leases.

Summary

The BLQ mechanism is typically implemented on DHCPv6 servers and clients, rather than directly configured on relay agents or intermediate devices.

The process distinguishes bulk lease query behavior from standard DHCPv6 interactions where clients request or renew only their own leases.

Workflow

A BLQ-capable DHCPv6 client, upon receiving a BLQ message from a server, responds with a list of its current DHCPv6 leases.

While your switches can act as DHCPv6 servers, the direct configuration for initiating or responding to bulk lease queries is typically part of the DHCPv6 server's internal logic and not a user-configurable CLI command on the switch itself. Network management applications would interact with the server using this protocol.

DHCPv6 Relay Agent notification for prefix delegation

When a DHCPv6 client requests a prefix delegation (PD) from a DHCPv6 server, the relay agent can be configured to notify other network elements, such as routing protocols, about the delegated prefix. This allows

for dynamic routing updates based on delegated prefixes, simplifying network management for service providers.

Configure DHCPv6 Relay Agent notification for prefix delegation

Use this procedure to configure the DHCPv6 relay agent to send notifications for prefix delegation.

Before you begin

The interface must be configured as a DHCPv6 relay agent.

Procedure

Step 1 Enter interface configuration mode for the interface connected to the DHCPv6 clients.

Example:

```
Device# configure terminal
```

Step 2 Enable DHCPv6 relay agent notification for prefix delegation.

Example:

```
Device(config)#ipv6 dhcp pool testv6
Device(config-dhcpv6)# ipv6 dhcp relay prefix-delegation pool
Device(config-dhcpv6)# exit
Device(config)# end
Device#
```

What to do next

Verify that routing protocols or other services are receiving and acting upon these notifications.

DHCPv6 Relay source

When a DHCPv6 Relay Agent forwards a client's request, it typically uses the interface's IPv6 address as the source. However, it can be beneficial to configure a specific source address, such as a loopback interface address, for consistency or to ensure reachability even if the physical interface changes.

Configure DHCPv6 Relay source

Use this procedure to configure a specific source address for DHCPv6 Relay messages.

This is useful for ensuring that the DHCPv6 server always sees a consistent source address from the Relay, regardless of which physical interface the message egresses.

Before you begin

- The interface must be configured as a DHCPv6 Relay Agent.
- A loopback interface with an IPv6 address is recommended as the source.

Procedure

Step 1 Enter interface configuration mode for the interface connected to the DHCPv6 clients.

Example:

```
Device# configure terminal
Device(config)# interface Vlan20
```

Step 2 Configure the DHCPv6 relay source interface.

Example:

```
Device(config-if)# ipv6 dhcp relay source-interface Loopback0
Device(config-if)# end
Device#
```

Replace *Loopback0* with the actual interface name to be used as the source.

What to do next

Verify on the DHCPv6 server that the source address of received relay messages is the configured loopback address.

DHCPv6 Server Stateless Address Autoconfiguration

In IPv6, Stateless Address Autoconfiguration (SLAAC) allows devices to generate their own IPv6 addresses. DHCPv6 SLAAC complements SLAAC by providing additional network configuration information like, DNS server addresses or domain names without assigning the IPv6 address itself. This is achieved through *managed-config-flag* and *other-config-flag* in Router Advertisements (RAs).

Configure DHCPv6 Server Stateless AutoConfiguration

Use this procedure to configure a DHCPv6 server to provide stateless configuration information.

This is a common deployment model for IPv6, where SLAAC handles address assignment, and DHCPv6 provides supplementary details.

Before you begin

- Configure the interface with an IPv6 address
- Enable Router Advertisements

Procedure

Step 1 Enter interface configuration mode for the interface where clients will receive stateless configuration.

Example:

```
Device# configure terminal
Device(config)# interface Vlan20
```

Step 2 Enable Router Advertisements and set the other-config-flag.

Example:

```
Device(config-if)# ipv6 nd other-config-flag
```

Alternatively, to force stateful DHCPv6 address assignment, set the managed-config-flag:

```
Device(config-if)# ipv6 nd managed-config-flag
```

The other-config-flag tells clients to use DHCPv6 for non-address configuration.

Step 3 Associate a DHCPv6 pool for stateless configuration, if not already done.

Example:

```
Device(config-if)# ipv6 dhcp server VLAN20_IPV6_POOL
Device(config-if)# end
Device#
```

This pool contains the non-address options like DNS servers.

What to do next

Verify client IPv6 configuration, including DNS servers.

VRF-aware DHCPv6 Server and Relay for IANA and prefix delegation

Virtual Routing and Forwarding (VRF) allows a single router to host multiple independent routing tables. VRF-aware DHCPv6 enables DHCPv6 server and relay functionalities to operate within specific VRF instances, providing isolated and secure IP address management for different tenants or network segments. This applies to both IPv6 address assignment (IANA - Identity Association for Non-temporary Addresses) and prefix delegation (PD).

Configure VRF-aware DHCPv6 Server and Relay for IANA and prefix delegation

Use this procedure to configure VRF-aware DHCPv6 Server or Relay functionalities.

This is critical in multi-tenant environments or for segmenting network services where each segment requires its own DHCPv6 service.

Before you begin

VRF instances must be configured, and interfaces must be assigned to the respective VRFs.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal Device(config)#
```

Step 2 Define the DHCPv6 pool within the VRF context for Server functionality.

Example:

```
Device(config)# vrf definition RED
Device(config-vrf)# add
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
Device(config-vrf)# exit
Device(config)# ipv6 dhcp pool testv6
Device(config-dhcpv6)# vrf RED
Device(config-dhcpv6)# address prefix 2001:DB8:1:1::/64
Device(config-dhcpv6)# dns-server 2001::1
Device(config-dhcpv6)#
```

Step 3 Enter interface configuration mode for the interface within the VRF.

Example:

```
Device(config)# interface Vlan30
Device(config-if)# vrf forwarding VRF_TENANT_A Device
Device(config-if)# ipv6 address 2001:DB8:1:1::1/64
```

This interface is associated with *VRF_TENANT_A*.

Step 4 Enable DHCPv6 server on the interface for IANA address assignment.

Example:

```
Device(config-if)# ipv6 dhcp server VLAN30_IPV6_POOL
```

Step 5 If acting as a Relay, then configure DHCPv6 Relay within the VRF.

Example:

```
Device(config)# interface HundredGigE1/2/0/21
Device(config-if)# switchport access vlan 2268
Device(config-if)# exit
Device(config)# interface Vlan2268
Device(config-if)# vrf forwarding CODX_DHCPV6_PD_VRF
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8:2268::1/64
Device(config-if)# ipv6 enable
Device(config-if)# ipv6 nd managed-config-flag
Device(config-if)# ipv6 nd other-config-flag
Device(config-if)# ipv6 dhcp relay destination global 138::2 sourceaddress 138::1
```

Replace *2001:DB8:2268::1* with the DHCPv6 Server address.

What to do next

Verify DHCPv6 lease assignments or relay operations within the VRF context.



CHAPTER 3

Specialized DHCP deployments and client customization

This chapter explores advanced client-side configurations and introduces specialized DHCP functionalities such as Single Sign-On (SSO) with On-Demand Application Provisioning (ODAP). It also provides a concluding overview of the comprehensive DHCP features covered throughout this guide.

- [Feature history for specialized DHCP deployments and client customization, on page 25](#)
- [Configurable DHCP clients, on page 26](#)
- [SSO - DHCP ODAP client-server, on page 27](#)

Feature history for specialized DHCP deployments and client customization

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 5: Feature history for specialized DHCP deployments and client customization

Release	Feature name and description	Supported platform
Cisco IOS XE 26.2.1ea	Specialized DHCP Deployments and Client Customization: The feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Specialized DHCP Deployments and Client Customization: Introduced the support for advanced client-side configurations and specialized DHCP functionalities such as Single Sign-On (SSO) with On-Demand Application Provisioning (ODAP).	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Configurable DHCP clients

Beyond simply obtaining an IP address, DHCP clients can be configured with specific parameters, behaviors, or identifiers to influence their interaction with DHCP servers and to meet particular network requirements. This section details how to customize a DHCP client's behavior.

DHCP Client ID

A DHCP client can be configured with a unique Client ID. This identifier is used by the DHCP server to track specific clients, regardless of their MAC address, which can change. For example, when a device's network adapter is replaced). Using a Client ID ensures that a client always receives the same IP address from the server, even if its hardware changes, or allows for specific policies to be applied based on the ID.

Configure DHCP client ID

Use this procedure to configure a specific client ID for a DHCPv4 client interface on your switch.

This is useful for devices that require a fixed IP address but are still managed by DHCP, or for tracking specific devices in a network.

Before you begin

Configure the interface as a DHCPv4 client using the **ip address dhcp** command.

Procedure

Step 1 Enter interface configuration mode for the desired interface.

Example:

```
Device# configure terminal
Device(config)# interface GigabitEthernet1/0/1
```

Step 2 Configure the DHCP client identifier.

Example:

```
Device(config-if)# ip dhcp client client-id GigabitEthernet1/0/1
```

The string keyword allows a user-defined ASCII string.

Example:

Example with a custom string:

```
Device(config-if)# ip dhcp client client-id string "MyOfficePC-001"
Device(config-if)# end
Device#
```

What to do next

Verify on the DHCP server that the client is recognized by its configured Client ID and receives the expected IP address.

Configure DHCP client to request specific options

Use this procedure to configure a DHCPv4 client interface to request specific DHCP options.

A DHCP client can explicitly request specific options from the DHCP server. While servers typically provide a standard set of options, a client might need additional, non-standard information to function correctly. This configuration allows the client to signal its requirements to the server.

This is useful when client applications or services require particular information such as, specific server addresses, custom parameters, and so on, that are delivered through DHCP options.

Before you begin

Configure the interface as a DHCPv4 client using the **ip address dhcp** command.

Procedure

Step 1 Enter interface configuration mode for the desired interface.

Example:

```
Device# configure terminal  
Device(config)# interface GigabitEthernet1/0/1
```

Step 2 Configure the DHCP client to request specific DHCP Options.

Example:

```
Device(config-if)# ip dhcp client request option 6  
Device(config-if)# ip dhcp client request option 15  
Device(config-if)# end  
Device#
```

Specify the numeric code of the desired DHCP option. You can specify multiple options.

This example shows DHCP client requesting Option 6—DNS servers and Option 15—Domain Name.

Step 3 Verify that the client received the requested DHCP Options.

SSO - DHCP ODAP client-server

Single Sign-On (SSO) with DHCP On-Demand Application Provisioning (ODAP) is a specialized solution that leverages DHCP to facilitate the initial setup and configuration of client devices for SSO-enabled applications. This typically involves Cisco Identity Services Engine (ISE) or similar platforms.

SSO - DHCP ODAP is a mechanism where a DHCP server, in conjunction with an identity management system like, Cisco ISE, provides network configuration and directs a newly connected client to an application

or portal for initial provisioning or authentication. This enables a 'zero-touch' experience for users, allowing them to quickly access required applications after connecting to the network.

How SSO - DHCP ODAP works

The SSO - DHCP ODAP process guides a user from initial network connection to authenticated application access, often without manual configuration.

Summary

The process involves these key components:

- DHCP server: provides initial IP address and network parameters
- Identity Management System: such as Cisco ISE, that authenticates users or devices, authorizes access, and provides provisioning instructions
- ODAP client: the end device such as, laptop, mobile device, and so on, that receives DHCP information and is directed to the provisioning portal
- ODAP application or portal: the web-based interface where users complete their SSO setup or application registration

Workflow

These stages describe how SSO - DHCP ODAP works:

1. Client connects and obtains IP: The client connects to the network and sends a DHCP Discover message. The DHCP server—potentially with a relay agent—assigns an IP address and provides specific DHCP options, including a URL for the ODAP portal.
2. Client redirection to ODAP portal: Upon receiving the DHCP options, the client's browser, or a built-in agent is automatically redirected to the specified ODAP portal URL.
3. User authentication and authorization: The user attempts to access the ODAP portal. The identity management system intercepts the request, authenticates the user—for example, using corporate credentials—and authorizes their access based on policies.
4. Application provisioning and SSO setup: After successful authentication, the ODAP portal guides the user through the necessary steps to provision applications, install certificates, or configure SSO for future access to corporate resources. This might involve downloading client software or configuring browser settings.
5. Network access and application use: Once provisioning is complete, the identity management system updates the client's network access policy, allowing full access to the corporate network and SSO-enabled applications.

Configure DHCP server for ODAP

Use this procedure to configure a DHCP server pool to provide the ODAP portal URL to clients. This is typically done using a custom DHCP option or a standard option like Option 43 if the ODAP client supports it.

Configuring SSO - DHCP ODAP involves setting up the DHCP server to provide specific options that direct clients to the ODAP portal, and configuring the identity management system to handle the provisioning process.

This is typically implemented in enterprise environments using Cisco ISE for user and device onboarding.

This step ensures that clients are directed to the correct provisioning portal upon connecting to the network.

Before you begin

- Configure a DHCPv4 or DHCPv6 pool.
- Deploy and configure Cisco ISE or similar identity management system with the ODAP portal URL and authentication policies.
- A DHCP pool must exist.

Procedure

Step 1 Enter DHCP pool configuration mode for the desired pool.

Example:

```
Device# configure terminal
Device(config)# ip dhcp pool ODAP_POOL
Device(dhcp-config)#
```

Step 2 Configure the ODAP portal URL.

The exact option and format may vary. Often, Option 43—Vendor-Specific Information—or a custom user-defined option is used. Consult your identity management system's documentation for the precise option and value.

Example:

Example using a generic string option:

```
Device(dhcp-config)# option 240 ascii "https://ise.example.com/portal/odap"
```

Example:

Example using Option 43, if supported by the client or ODAP system:

```
Device(dhcp-config)# option 43 hex
010468747470733A2F2F6973652E6578616D706C652E636F6D2F706F7274616 C2F6F646170
Device(dhcp-config)# exit
Device(config)# end
Device#
```

In this example of Option 43, 01 is the sub-option code for URL, 04 is the length of URL, followed by the hex representation of `https://ise.example.com/portal/odap`. The exact sub-option and format depend on the ODAP client implementation.

What to do next

Verify client redirection and successful provisioning through the ODAP portal.