



# Dynamic Host Configuration Protocol

---

This chapter provides information about Dynamic Host Configuration Protocol (DHCP) server which enables Cisco Unified IP Phones, connected to either the customer data or voice Ethernet network, to dynamically obtain their IP addresses and configuration information. It uses Domain Name System (DNS) to resolve host names both within and outside the cluster.

- [DHCP Server, page 1](#)
- [Domain Name System, page 2](#)
- [Configure DHCP Server, page 3](#)
- [TFTP Server Device Identification, page 3](#)
- [Migration, page 3](#)
- [Alarms, page 3](#)

## DHCP Server

Because DHCP server is a standalone server, no backup server exists in case the Cisco Unified Communications Manager that is configured as DHCP server fails.

Cisco Unified Communications Manager administrator configures the DHCP servers and subnets. You can configure one server for each node and multiple subnets for each server.



### Note

You must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before using that information to configure the Cisco Unified Communications Manager server.

For Cisco Unified Communications Manager, you must reboot the node if an IP address changes. As long as the node is up, it will keep refreshing the lease period for which the DHCP server provides an IP address, and hence retain the same IP address. However, hostname of the node must remain the same, even if the IP address changes.

# Domain Name System

Two types of implementations exist for DNS.

- Corporate DNS, if available
- Internal DDNS service transparent to the user

The Cisco Unified Communications Manager Administration provides support to configure different scopes for the DHCP server. For each scope, you can enter a range of IP addresses and subnet masks and you can also configure options.

For configuring DNS with Corporate DNS, the corporate DNS infrastructure is used, and default DNS configuration will act as a cache only service to this corporate DNS service.

When no corporate DNS service exists, Dynamic Domain Name System (DDNS) service, a service that allows dynamic updates to hostname and IP addresses, is used to implement a clusterwide DNS infrastructure. This also serves other devices on the network that are interacting with the cluster. Each node has DNS running on it. These DNS servers get configured with hostname and IP address information for all the nodes and any other devices in the cluster. The DNS on the first node in the cluster gets configured as primary DNS, while all other nodes get configured as secondary nodes.

When any change to DNS configuration occurs to the first node of Cisco Unified Communications Manager, the change automatically gets transferred to other nodes. Other devices in the network can point to any of the nodes in the cluster for the DNS lookups.

**Note**

Any change to the host name of a node will require the node to be reinserted in the cluster. Before you change the host name of a node, review the document, *Changing the IP Address and Host Name for Cisco Unified Communications Manager*.

When nodes are being configured using by DHCP, the DHCP client on the node will get configured to dynamically update DDNS.

Whenever nodes are configured by using DHCP, one the following events occurs:

- The corporate DNS can accept dynamic updates.
- DNS gets updated within the cluster
- DHCP configuration for the nodes gets tied with their MAC addresses of the node for which you are requesting an IP address. If the node requests an IP address again, DHCP matches the MAC address to the previous request and provides the same IP address.

You must update the DNS server with the appropriate Cisco Unified Communications Manager name and address information before using that information to configure the Cisco Unified Communications Manager server.

**Caution**

If the AAAA record or A record do not map correctly, calls may fail.

# Configure DHCP Server

Use the following steps to configure DHCP Process:

## Procedure

---

- Step 1** Enable the DHCP functionality from the serviceability window.
  - Step 2** Verify the DHCP monitor process is started on the node where the DHCP is enabled.
  - Step 3** Use Cisco Unified Communications Manager Administration to configure the scopes and options.
  - Step 4** Verify that configuration is captured in the /etc/dhcpd.conf file of targeted Cisco Unified Communications Manager.
  - Step 5** Verify the DHCP server daemon is running with new configuration.
  - Step 6** Make sure DHCP monitor process logs at the specific trace settings.
  - Step 7** Make sure the error alarm is raised when the DHCP daemon is stopped and the info alarm is raised when the daemon is restarted.
- 

## TFTP Server Device Identification

For information about the TFTP server, see [Configure TFTP](#).

## Migration

Because no migration is provided from Window 2000 based DHCP configuration to the DHCP configuration, the administrator must reconfigure the system.

## Alarms

Two alarms get generated for DHCP.

- CiscoDhcpdFailure
- CiscoDhcpdRestarted

