New and Changed Document for Cisco Unified Communications Manager 7.1(1)

This document highlights information for important features that are supported in Cisco Unified Communications Manager 7.1(1). This document does not contain all information for all features that are available in Cisco Unified Communications Manager 7.1(1). Use this document in conjunction with the documentation and online help that are provided for Cisco Unified Communications Manager 7.1(1).

This document contains the following topics:

- New and Changed Information, page 2
  - Installation, Upgrade, and Migration, page 2
  - Cisco Unified Communications Operating System Administration, page 6
  - Command Line Interface, page 7
  - Cisco Unified Communications Manager Administration, page 10
  - Cisco Unified Communications Manager Features and Applications, page 15
  - Security, page 104
  - Bulk Administration Tool, page 107
  - Cisco Unified Serviceability, page 114
  - Cisco Unified Real-Time Monitoring Tool, page 117
  - Cisco Unified Communications Manager CDR Analysis and Reporting, page 120
  - Cisco Unified Communications Manager Call Detail Records, page 122
  - Cisco Unified Reporting, page 125
  - Cisco Unified IP Phones, page 126
  - Cisco Unified CM User Options, page 154
- Documentation Updates, page 154

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

New and Changed Information

This section contains information on the following topics:

- Installation, Upgrade, and Migration, page 2
- Cisco Unified Communications Operating System Administration, page 6
- Command Line Interface, page 7
- Cisco Unified Communications Manager Administration, page 10
- Cisco Unified Communications Manager Features and Applications, page 15
- Security, page 104
- Bulk Administration Tool, page 107
- Cisco Unified Serviceability, page 114
- Cisco Unified Real-Time Monitoring Tool, page 117
- Cisco Unified Communications Manager CDR Analysis and Reporting, page 120
- Cisco Unified Communications Manager Call Detail Records, page 122
- Cisco Unified IP Phones, page 126
- Cisco Unified CM User Options, page 154

Installation, Upgrade, and Migration

This following sections describe the changes for installation, upgrade, and migration in Cisco Unified Communications Manager 7.1(1):

- Cisco Security Agent for Cisco Unified Communications Manager Log File, page 2
- System History Log for Cisco Unified Communications Manager, page 2
- Data Migration Assistant (DMA), page 5

Cisco Security Agent for Cisco Unified Communications Manager Log File

The CLI command that accesses the Cisco Security Agent file log is changed to **utils create report csa**.

System History Log for Cisco Unified Communications Manager

This system history log provides a central location for getting a quick overview of the initial system install, system upgrades, Cisco option installations, DRS backups and DRS restores, as well as switch version and reboot history.

Description

This section provides a description of the system history log feature.

Overview

The system history log exists as a simple ASCII file, **system-history.log**, and the data is not maintained in the database. Because it does not get excessively large, the system history file does not get rotated.

The system history log provides the following functions:

- Logs the initial software installation on a server.
- Logs the success and failure of every software upgrades (Cisco option files and patches).
- Logs every DRS backup and restore performed.
- Logs every invocation of Switch Version, issued through either the CLI or the GUI.
- Logs every invocation of Restart and Shutdown, issued through either the CLI or the GUI.
- Logs every boot of the system. If not correlated with a restart or shutdown entry, the boot is the result of a manual reboot, power cycle, or kernal panic.
- Maintains a single file that contains the system history, since initial installation or since feature availability.
- Exists in the install folder. The log can be accessed the from the CLI by using the **file** commands and by using the Real Time Monitoring Tool (RTMT).

System History Log Fields

Each system history log entry contains the following fields:

- <*timestamp*> <*userid*> <*action*> <*description*> <*start/result*>

The system history log fields can contain the following values:

- *timestamp*—Displays the local time and date on the server with the format *mm/dd/yyyy hh:mm:ss*.
- *userid*—Displays the user name of the user who invokes the action.
- action—Displays one of the following actions:
  - Basic Install
  - Windows Upgrade
  - Upgrade During Install
  - Upgrade
  - Cisco Option Install
  - Switch Version
  - System Restart
  - Shutdown
  - Boot
  - DRS Backup
  - DRS Restore
- *description*—Displays one of the following messages:
  - *Version*: Displays for the Basic Install, Windows Upgrade, Upgrade During Install, Upgrade, and ServerPak Install actions.
  - *Cisco Option file name*: Displays for the Cisco Option Install action.
  - *Timestamp*: Displays for the DRS Backup and DRS Restore actions.
  - *Active version to inactive version*: Displays for the Switch Version action.
  - *Active version*: Displays for the System Restart, Shutdown, and Boot actions.
- result—Displays the following results:

- Start
- Success or Failure
- Cancel

Example

Example 1 shows a sample of the system history log.

Example 1 System History Log

```
admin:file dump install system-history.log
=====================================
Product Name -    Cisco Unified Communications Manager
Product Version - 6.1.2.9901-117
Kernel Image -    2.4.21-47.EL.cs.3BOOT
=====================================
07/25/2008 14:20:06 | root: Install 6.1.2.9901-117 Start
07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start
07/30/2008 10:08:56 | root: Upgrade 6.1.2.9901-126 Start
07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126 Success
07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Start
07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117 to 6.1.2.9901-126 Success
07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start
08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126 Start
```

CLI Considerations

You can access the system history log by using the CLI **file** command; for example:

- **file view install system-history.log**
- **file get install system-history.log**

Cisco Unified Communications Manager Administration Configuration Tips

No Cisco Unified Communications Manager Administration configuration tips exist for this feature.

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

No service parameter and enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No installation or upgrade consideration exist for this feature.

Serviceability Considerations

To access the system history log in RTMT, navigate to RTMT Trace Collection:

RTMT > Trace Log Collection

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL and CTI considerations exist for this feature.

User Tips

No user tips exist for this feature.

For More Information

For more information about using the CLI, see the *Cisco Unified Communications Operating System Administration Guide* or the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

For more information about RTMT, see the *Real-Time Monitoring Tool Administration Guide*.

Data Migration Assistant (DMA)

Cisco Unified Communications Manager Release 7.1(1) includes the following Data Migration Assistant (DMA) enhancements. For more details, refer to the documents *Data Migration Assistant User Guide 7.1(1)* and *Upgrading to Cisco Unified Communications Manager Release 7.1(1) from Cisco Unified Communications Manager 4.x Releases*:

- The platformConfig.xml file generated by DMA supports upgrades for the first node (publisher database server) as well as for the subsequent nodes (subscribers). DMA provides a screen where you can make detailed configuration specifications. Enter data at the DMA screen Export > Answer File Generator.
- DMA provides a screen where users can customize the behavior of DMA, specifying which types of logs to include in the output file. Enter data at the DMA screen Export > Custom Options
- DMA explicitly lists the pre-DMA export tasks. DMA provides both information and the automation of pre-export tasks when possible to ensure that they know what tasks they needs to complete before running DMA. Enter data at the DMA screen Export > Pre-Export Tasks.
- DMA supports the generation of a license file upon successful DMA validation. The user can upload this license file to Cisco CCO to get the actual license file ready for use. Go to the DMA screen Export > Storage Location and specify a local directory destination for the license file licupgrade.lic Specify the destination in the “Path Name” text box of the screen’s “Destination Option for License File” field.
- DMA displays the latest timestamp of the CDR and CAR data. If these timestamps do not match, DMA displays a message that indicates that users must load the latest CDR records into the CAR database in order for the records to be exported.
- DMA enhances pre-upgrade instructions regarding the CAR database. DMA displays information from the CAR database including current number of CAR records, start date, and end date so that users can determine how many records exist and how many records that DMA can export.
- DMA provides options on how to handle CAR data during the DMA export process. The default option specifies that DMA does not export the CAR database. If you want to have this data included in the DMA TAR file, you must choose to include the CAR records into the DMA TAR file. DMA

indicates the time (in thirty-minute intervals) that DMA requires to migrate the CAR data. DMA displays the approximate number of records that are migrated during this period as well as the total number of CAR records on the server.

For More Information

- Upgrade of CAR Data, page 120

Cisco Unified Communications Operating System Administration

This section describes changes to the Cisco Unified Communications Operating System Administration GUI.

- Customized Log-on Message, page 6
- Ethernet IPv6 Configuration Settings, page 6

Customized Log-on Message

You can upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified Communications Manager Administration, and the command line interface.

To upload a customized log-on message, follow this procedure:

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to Software **Upgrades > Customized Logon Message**.

The Customized Logon Message window displays.

Step 2 To choose the text file that you want to upload, click **Browse**.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10KB.

The system displays the customized log-on message.

Step 4 To revert to the default log-on message, click **Delete**.

Your customized log-on message gets deleted, and the system displays the default log-on message.

Ethernet IPv6 Configuration Settings

Use the following procedure to enable and configure IPv6 on the server.

Note All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings > IP > Ethernet IPv6**.

The Ethernet IPv6 Configuration window displays.

Step 2 To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet IPv6 Configuration window, see Table 1.

Step 3 To preserve your changes, click **Save**.

Note If you check the Update with Reboot check box, the system reboots after you click Save. For the IPv6 settings to take effect, you must reboot the system.

Table 1 Ethernet IPv6 Configuration Fields and Descriptions

Field	Description
Enable IPv6	Check this check box to enable IPv6 on the server.
Address Source	Choose one of the following IP address source: • Router Advertisement • DHCP • Manual Entry/Mask The three IP address sources are mutually exclusive. **Note** Unless you specify Manual Entry, the IP Address and Mask fields are read only.
IPv6 Address	If you chose Manual Entry, enter the IPv6 address of the server; for example: fd6:2:6:96:21e:bff:fecc:2e3a
IPv6 Mask	If you chose Manual Entry, enter the IPv6 mask; for example: 64
Update with Reboot	If you want the system to reboot immediately after you click Save, check this check box. If you want to reboot later, leave the check box blank. **Note** For the IPv6 settings to take effect, you must reboot the system.

Command Line Interface

This section contains information about the Command Line Interface (CLI).

- Spaces in File Names, page 8
- Relative Paths, page 8
- New Commands and Parameters, page 8

Spaces in File Names

You can use CLI commands to directly work with file names that contain spaces. For example, you could use the **file delete** command to delete a log file with the name cisco test log in the Platform directory:

file delete activelog platform cisco test log

Relative Paths

When you download a file to your local computer with the **file get** command, the system prompts you to enter a download directory. You can specify a relative path for the download directory by using the **./** notation, as shown in the following example:

Download directory: ./RepStat

If you specify a download directory that does not exist on your local computer, the **file get** command creates it for you.

New Commands and Parameters

This section provides information about the new CLI commands for Cisco Unified Communications Manager Release 7.1(1).

For more information about command syntax and parameters, see the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

- **utils auditd {enable|disable|status}**

  This command enables, disables, and provides the status of audit logging. When enabled, the system monitors and records user actions in both Cisco Unified Communications Manager and Cisco Unified Serviceability.

  You can also use the CLI **file** commands to manipulate the audit log, including the following:

  - **file list activelog audit**
  - **file view activelog audit** <filename>
  - **file dump activelog audit** <filename>
  - **file get activelog audit** <filename>
  - **file search activelog audit** <filename>

Note Cisco recommends that you retrieve the audit log by using the Real-Time Monitoring Tool.

- **utils create report csa**

  This command collects all the files that are required for CSA diagnostics and assembles them into a single CSA diagnostics file. You can retrieve this file by using the **file get** command.

- **set password complexity character {enable|disable}**

  Use this command to enable password complexity rules for the type of characters in a password.

  When you enable password complexity, you must follow these guidelines when assigning a password:

  - It must have at least one lower-case character.
  - It must have at least one uppercase, one digit, and one special character.

  - You cannot use adjacent characters on the keyboard.
  - You cannot reuse any of the previous ten passwords.
  - The admin user password can only be changed only once in 24 hours.
- **set password complexity minimum-length**

Note Use this command only after you enable password character complexity.

  Use this command to modify the value for the minimum password length for Cisco Unified Communications Operating System accounts.

  Acceptable values must be equal-to or greater-than 6.

- **set password age maximum**

  Use this command to modify the value for maximum password age, in days, for Cisco Unified Communications Operating System accounts.

  Acceptable values must be equal-to or greater-than 90 days.

In the Command Line Interface, you can run the following IPv6 commands on each server in the cluster:

- Mandatory command—To enable IPv6 in the Cisco Unified Communications Operating System, run the command, **set network ipv6 service enable**.
- Optional command, depending on the requirements of your network—If you want the DHCPv6 server to issue a non-link-local IPv6 address to the Cisco Unified Communications Manager server, run the command, **set network ipv6 dhcp enable**.

Tip Ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address. If the server has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected.

- Optional command, depending on the requirements of your network—If you want to use a static IPv6 address for the Cisco Unified Communications Manager, run the CLI command, **set network ipv6 static_address <addr> <mask>**. Running this command assumes that you do not want the Cisco Unified Communications Manager to get the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration.
- Optional command—To view the IPv6 configuration for the Cisco Unified Communications Manager server, run the command, **show network ipv6 settings**.
- Optional command, depending on your network—To verify that you can ping other servers in the network, run the command, **utils network ipv6 ping <ipv6 address>**.

Tip Running these commands requires that you restart the server.

Cisco Unified Communications Manager Administration

This section contains information on the following topics:

- New and Updated Enterprise and System Parameters, page 10
- Menu Changes, page 11
- Cisco Unified Communications Manager Features and Applications, page 15

New and Updated Enterprise and System Parameters

The following sections contain information on new and updated enterprise and service parameters:

- Enterprise Parameters, page 10
- Service Parameters, page 10

Enterprise Parameters

To access the enterprise parameters in Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. To display the help for the service parameter, click the name of the enterprise parameter in the window.

- Enable IPv6—See the "Internet Protocol Version 6 (IPv6)" section on page 32.
- IP Addressing Mode Preference for Media—See the "Internet Protocol Version 6 (IPv6)" section on page 32.
- IP Addressing Mode Preference for Signaling—See the "Internet Protocol Version 6 (IPv6)" section on page 32.
- Allow Auto-Configuration for Phones—See the "Internet Protocol Version 6 (IPv6)" section on page 32.
- Enable Logical Partitioning—See the "Logical Partitioning" section on page 77.
- Default Geolocation—See the "Logical Partitioning" section on page 77.
- Logical Partitioning Default Policy—See the "Logical Partitioning" section on page 77.
- Logical Partitioning Default Filter—See the "Logical Partitioning" section on page 77.

Service Parameters

To access the service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**. Choose the server and the service name that the parameter supports. For some parameters, you may need to click Advanced to display the service parameter. To display the help for the service parameter, click the name of the service parameter in the window.

- Party Entrance Tone—This parameter supports the Cisco CallManager service for the"Viewing Held Calls on Shared Lines" feature.
- Always Use Prime Line—This parameter supports the Cisco CallManager service for the "Always Use Prime Line" feature.
- Always Use Prime Line for Voice Message—This parameter supports the Cisco CallManager service for the "Always Use Prime Line for Voice Message" feature.
- Table Out Of Sync—This parameter supports the Cisco CallManager service for the "Table Out of Sync Detection" feature.
- Send Multicast MOH in H.245 OLC Message—This parameter supports the Cisco CallManager service for the "Multicast Music On Hold Over H.323 Intercluster Trunks" feature.

- Call Counting CAC Enabled—This parameter supports the Cisco CallManager service for the "Internet Protocol Version 6 (IPv6)" feature.
- Audio Bandwidth For Call Counting CAC—This parameter supports the Cisco CallManager service for the "Internet Protocol Version 6 (IPv6)" feature.
- Video Bandwidth For Call Counting CAC—This parameter supports the Cisco CallManager service for the "Internet Protocol Version 6 (IPv6)" feature.
- TFTP IPv6 Address—This parameter supports the Cisco TFTP service for the "Internet Protocol Version 6 (IPv6)" feature.
- Server IP Track—This parameter supports the Cisco TFTP service for the "Internet Protocol Version 6 (IPv6)" feature.
- Alternate Cisco File Server(s)—This parameter supports the Cisco TFTP service for the "Internet Protocol Version 6 (IPv6)" feature.

Menu Changes

This section contains information on the following menus in Cisco Unified Communications Manager Administration:

- Main Window, page 11
- System, page 12
- Call Routing, page 12
- Media Resources, page 12
- Voice Mail, page 12
- Device, page 13
- Application, page 13
- User Management, page 14
- Bulk Administration, page 14

Main Window

- After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the current state of licenses for Cisco Unified Communications Manager. For more information, see the "Licensing Enhancements" section on page 70.
- Customized Log-on Message—You can upload a text file that contains a customized log-on message that appears on the initial Cisco Unified Communications Manager Administration window. For more information and the procedure for uploading your customized log-on message, refer to Chapter 7 in the Cisco Unified Communications Operating System Administration Guide.
- Last Successful Logon—When you log into Cisco Unified Communications Manager Administration, the initial Cisco Unified Communications Manager Administration window displays the date and time of the last successful system logon.

System

The System menu contains the following changes:

- System > Server—The IPv6 Name field displays, as described in the "Internet Protocol Version 6 (IPv6)" section on page 32.
- System > Device Pool—The Incoming Calling Party National Digits to Strip field, Incoming Calling Party International Digits to Strip field, Incoming Calling Party Unknown Digits to Strip field, Incoming Calling Party Subscriber Digits to Strip field, Incoming Calling Party Transformation CSS for National Number drop-down list box, Incoming Calling Party Transformation CSS for International Number drop-down list box, Incoming Calling Party Transformation CSS for Unknown Number drop-down list box, and Incoming Calling Party Transformation CSS for Subscriber Number drop-down list box display, as described in the "Calling Party Normalization Enhancements" section on page 24. The Geolocation and Geolocation Filter fields are added in the new Geolocation Pane, as described in the "Logical Partitioning" section on page 77.
- System > Enterprise Parameters—For information on new or updated enterprise parameters, see the "New and Updated Enterprise and System Parameters" section on page 10.
- System > Service Parameters —For information on new or updated service parameters, see the "New and Updated Enterprise and System Parameters" section on page 10.
- System > Licensing > License File Upload—This window displays a message that uploading the license file removes the demo licenses for the feature. For more information, see the "Licensing Enhancements" section on page 70.
- System > Licensing > License File Upload—This window displays the status of a license file. For example, the Status column for each license type may display Demo, Missing, or Uploaded. For more information, see the "Licensing Enhancements" section on page 70.
- System > Geolocation Configuration—This menu option allows configuration of a geolocation. For more information, see the "Logical Partitioning" section on page 77.
- System > Geolocation Filter—This menu option allows configuration of a geolocation filter. For more information, see the "Logical Partitioning" section on page 77.

Call Routing

The Call Routing menu provides the following new and updated settings.

- Call Routing > SIP Route Pattern—The IPv6 Pattern field displays, as described in the "Internet Protocol Version 6 (IPv6)" section on page 32.
- Call Routing > Directory Number—The Log Missed Calls check box displays, as described in the "Logging Missed Calls For Shared Lines" section on page 74.
- Call Routing > Logical Partitioning Policy—This window allows configuration of a logical partition policy. For more information, see the "Logical Partitioning" section on page 77.

Media Resources

No changes exist for the Media Resources menu.

Voice Mail

No changes exist for the Voice Mail menu.

Device

- Device > CTI Route Point—The Geolocation field displays, as described in the "Logical Partitioning" section on page 77.
- Device > Gateway—The Incoming Calling Party National Digits to Strip field, Incoming Calling Party International Digits to Strip field, Incoming Calling Party Unknown Digits to Strip field, Incoming Calling Party Subscriber Digits to Strip field, Incoming Calling Party Transformation CSS for National Number drop-down list box, Incoming Calling Party Transformation CSS for International Number drop-down list box, Incoming Calling Party Transformation CSS for Unknown Number drop-down list box, and Incoming Calling Party Transformation CSS for Subscriber Number drop-down list box display, as described in the "Calling Party Normalization Enhancements" section on page 24. The Geolocation and Geolocation Filter fields display, as described in the "Logical Partitioning" section on page 77.
- Device > Phone—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 16. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 19. The Geolocation field displays, as described in the "Logical Partitioning" section on page 77.
- Device > Trunk—The Destination Address IPv6 field displays for SIP trunks, as described in the "Internet Protocol Version 6 (IPv6)" section on page 32. The Incoming Calling Party National Digits to Strip field, Incoming Calling Party International Digits to Strip field, Incoming Calling Party Unknown Digits to Strip field, Incoming Calling Party Subscriber Digits to Strip field, Incoming Calling Party Transformation CSS for National Number drop-down list box, Incoming Calling Party Transformation CSS for International Number drop-down list box, Incoming Calling Party Transformation CSS for Unknown Number drop-down list box, and Incoming Calling Party Transformation CSS for Subscriber Number drop-down list box display, as described in the "Calling Party Normalization Enhancements" section on page 24. In the Geolocation Configuration pane, the Geolocation and Geolocation Filter fields and the Send Geolocation Information check box display, as described in the "Logical Partitioning" section on page 77.
- Device > Device Settings > Default Device Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 16. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 19.
- Device > Device Settings > Device Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 16. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 19.
- Device > Device Settings > SIP Profile—The Enable ANAT check box displays, as described in the "Internet Protocol Version 6 (IPv6)" section on page 32.
- Device > Device Settings > Common Device Configuration—The IP Addressing Mode drop-down list box, the IP Addressing Mode Preference for Signaling drop-down list box, and the Allow Auto-Configuration for Phones drop-down list box displays, as described in the "Internet Protocol Version 6 (IPv6)" section on page 32.
- Device > Device Settings > Common Phone Profile—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 16. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 19.

Application

No updates or new fields exist for this menu.

User Management

The User Manager menu displays the following new settings:

- User Management > Role—The Find and List Roles window displays the Standard Audit Log Administration role, as described in the "Standard Audit Log Administration Role" section on page 94.
- User Management > User Group—The Find and List User Groups window displays the Standard Audit Users user group, as described in the "Standard Audit Users User Group" section on page 96.

Bulk Administration

The Bulk Administration menu displays the following new and updated settings.

- Bulk Administration > Phones > Phone Template—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 16. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 19.
- Bulk Administration > User Device Profile > UDP Template—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 16. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 19.
- Bulk Administration > Phones > Update Phones—The Always Use Prime Line drop-down list box displays, as described in the "Always Use Prime Line" section on page 16. The Always Use Prime Line For Voice Mail drop-down list box displays, as described in the "Always Use Prime Line for Voice Message" section on page 19.
- Bulk Administration > Phones > Phone Template. Click Add New DN in the Associated Information Area—Log Missed Calls Check Box displays as described in the "Logging Missed Calls For Shared Lines" section on page 74.
- Bulk Administration > User Device Profile > UDP Template. Click Add New DN in the Associated Information Area—Log Missed Calls Check Box displays as described in the "Logging Missed Calls For Shared Lines" section on page 74.
- Bulk Administration > Phones > Add/Update Lines > Update Lines—Log Missed Calls Check Box displays as described in the "Logging Missed Calls For Shared Lines" section on page 74.
- Bulk Administration > User device Profiles > Add/Update Lines > Update Lines—Log Missed Calls Check Box displays as described in the "Logging Missed Calls For Shared Lines" section on page 74.
- Bulk Administration > Phones > Phone Template Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Party Entrance Tone" section on page 88.
- Bulk Administration > User Device Profile > UDP Template Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Party Entrance Tone" section on page 88.
- Bulk Administration > Gateways > Gateway Template. Click Add New DN in the Associated Information Area—Party Entrance Tone drop-down list box displays, as described in the "Party Entrance Tone" section on page 88.
- Bulk Administration > Gateways > Gateway Template—VG202 and VG204 gateways now display in the Gateway Type drop-down list box as described in the "Support for VG202 and VG204 Gateways" section on page 111.

- Bulk Administration > Gateways > Insert Gateways—VG202 and VG204 gateways now display in the Gateway Type drop-down list box as described in the "Support for VG202 and VG204 Gateways" section on page 111.
- Bulk Administration > Gateways > Insert Gateways. Select Gateway type and click next. The second Insert Gateways Configuration page displays—Sample insert gateways link now displays VG202 and VG204 sample files along with other BAT supported gateways as described in the "Support for VG202 and VG204 Gateways" section on page 111.
- Bulk Administration > Phone Migration—The Phone Migration page displays, as described in the "Phone Migration in BAT" section on page 112.
- Bulk Administration > Phones > Phone Template—The GeoLocation drop-down list box displays, as described in the "Support for Logical Partitioning" section on page 113.
- Bulk Administration > Gateways > Gateway Templates: Phone Template Configuration Page—The GeoLocation drop-down list box displays, as described in the "Support for Logical Partitioning" section on page 113.
- Bulk Administration > Import/Export > Export—New fields supported for export by the Import/Export tool are described in the "New fields supported for Export by Import/Export" section on page 113.
- Bulk Administration > Phones > Add/Update Lines > Update Lines—Park Monitoring fields display, as described in the "Support for Park Monitoring" section on page 113.
- Bulk Administration > Phones > Phone Template; click Add a new DN in the Associated Information area—Park Monitoring fields display, as described in the "Support for Park Monitoring" section on page 113.
- Bulk Administration > Phones > Update Phones—The Apply Config button displays, as described in the "Support for Seamless Integration (Apply Config)" section on page 114.
- Bulk Administration > Phones > Reset/Restart Phones—The Apply Config button displays, as described in the "Support for Seamless Integration (Apply Config)" section on page 114.

Cisco Unified Communications Manager Features and Applications

This section contains information on the following Cisco Unified Communications Manager Administration features and applications:

- Always Use Prime Line, page 16
- Always Use Prime Line for Voice Message, page 19
- Barge, cBarge, and Single Button Barge Support for PLAR, page 22
- Calling Party Normalization Enhancements, page 24
- Cisco Unified Communications Manager Assistant, page 31
- Cisco Web Dialer Configured in Application Server Window, page 31
- Internet Protocol Version 6 (IPv6), page 32
- Licensing Enhancements, page 70
- Logging Missed Calls For Shared Lines, page 74
- Multicast Music On Hold Over H.323 Intercluster Trunks, page 84
- Off-Hook Abbreviated Dial, page 86
- Party Entrance Tone, page 88

- Phone Migration in Cisco Unified Communications Manager Administration, page 91
- QSIG Variant Configuration for a Gateway or Trunk, page 93
- Synchronization of Configuration Settings, page 97
- Standard Audit Log Administration Role, page 94
- Standard Audit Users User Group, page 96
- Table Out of Sync Detection, page 100
- Unconfigured Device Registration Attempts Restricted, page 101
- Viewing Held Calls on Shared Lines, page 103

Always Use Prime Line

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

After you configure the Always Use Prime Line setting in Cisco Unified Communications Manager Administration, when the phone is idle (offhook) and receives a call on any line, the primary line gets chosen for the call.

Tip To configure the Always Use Prime Line feature in previous releases of Cisco Unified Communications Manager (except for 6.1(3)), you configured the Always Use Prime Line service parameter for the Cisco CallManager service, which applied to the entire cluster. In Cisco Unified Communications Manager 7.1(1) and 6.1(3), you can configure the Always Use Prime Line setting for devices and device profiles.

Cisco Unified Communications Manager Administration Configuration Tips

When you configure this feature, going offhook makes only the first line active, even when a call rings on another line on the phone; that is, the call does not get answered on that line. In this case, the phone user must choose the other line to answer the call.

For more configuration considerations, see Table 2 on page 17.

GUI Changes

The Always Use Prime Line setting displays in the following windows in Cisco Unified Communications Manager Administration.

- System > Service Parameters (for Cisco CallManager service)
- Device > Phone
- Device > Common Phone Profile
- Device > Device Settings > Default Device Profile
- Device > Device Settings > Device Profile

For information on how the Always Use Prime Line setting works when a phone idle or busy, see Table 2 on page 17.

Tip If you configure the Always Use Prime Line setting in the Service Parameter, Common Phone Profile, and in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the Phone Configuration window.

Table 2 Always Use Prime Line Configuration

State of Phone	Configuration for Always Use Prime Line	How Feature Works
Idle	On	When the phone is idle (offhook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. If you choose On for the Always Use Prime Line setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.
Idle	Off	When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received; that is, when the phone is offhook.
Idle	Default	If you choose Default for the Always Use Prime Line setting in the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration windows, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter when determining whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the for the Always Use Prime Line setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.
Busy	On	When the phone already has a call on a line, Cisco Unified Communications Manager uses the configuration for the Maximum Number of Calls and Busy Trigger settings to determine how to route the call.
Idle	On, but you also configured Auto Answer With Headset or Auto Answer with Speakerphone	If you choose the Auto Answer with Headset option or Auto Answer with Speakerphone option from the Auto Answer drop-down list box in Cisco Unified Communications Manager Administration, the Auto Answer configuration overrides the configuration for the Always Use Prime Line setting.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature via the clusterwide service parameter, Always Use Prime Line, which supports the Cisco CallManager service, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Always Use Prime Line drop-down list box, choose **True**.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 7.1(1), you can configure this feature per device or per device profile.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so activate the service by choosing **Tools > Service Activation** in Cisco Unified Serviceability. In addition, you can run SDI trace for the Cisco CallManager service. When you view the log in RTMT, you can see the configured value that is used by the device; for example, alwaysPrimeLine=1, which indicates that the device uses On for the configuration.

BAT Considerations

The Bulk Administration GUI has the following updates to support the Always Use Prime Line feature: Always Use Prime Line drop-down list box—choose one of the following options:

- Off
- On
- Default

Note For details of configuration options for the Always Use Prime Line feature, refer to Table 2.

Note The Always Use Prime Line drop-down list boxes displays on the Phone Template, UDP Template, and Update Phone pages.

- Insert, Export, and Validate Details support for always use prime line—the following insert, export, and validate details features have support for the always use prime line feature:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details

  - Insert Phones/Users
  - Validate Phones/Users
- UDP File Format—UDP File Format Configuration page lists the Always Use Prime Line, and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration page lists the Always Use Prime Line, and Always Use Prime Line for Voice Message fields in the Device Fields section.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For a list of phones that support this feature, see the "Line Select" section on page 145.

For More Information

- Always Use Prime Line for Voice Message, page 19
- Line Select, page 145

Always Use Prime Line for Voice Message

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

After you configure the Always Use Prime Line for Voice Message setting in Cisco Unified Communications Manager Administration, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone.

Tip To configure the Always Use Prime Line for Voice Message feature in previous releases of Cisco Unified Communications Manager (except for 6.1(3)), you configured the Always Use Prime Line service parameter for the Cisco CallManager service, which applied to the entire cluster. In Cisco Unified Communications Manager 7.1(1) and 6.1(3), you can configure the Always Use Prime Line for Voice Message setting for devices and device profiles.

Cisco Unified Communications Manager Administration Configuration Tips

For configuration considerations, see Table 3 on page 20.

GUI Changes

The Always Use Prime Line for Voice Message setting displays in the following windows in Cisco Unified Communications Manager Administration.

- System > Service Parameters (for Cisco CallManager service)
- Device > Phone
- Device > Common Phone Profile
- Device > Device Settings > Default Device Profile
- Device > Device Settings > Device Profile

For information on how the Always Use Prime Line for Voice Message setting works when a phone idle or busy, see Table 3 on page 20.

Tip If you configure the Always Use Prime Line for Voice Message setting in the Service Parameter, Common Phone Profile, and in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the Phone Configuration window.

Table 3 Always Use Prime Line for Voice Mail Configuration

State of Phone	Configuration for Always Use Prime Line for Voice Message	How Feature Works
Idle	On	If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. If you choose On for the Always Use Prime Line for Voice Mail setting in the Device Profile or Default Device Profile Configuration window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility; that is, if you configure Cisco Extension Mobility correctly.
Idle	Off	If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. It will always select the first line that has a VM. If no line has a voice message, the primary line gets used when the phone user presses the Messages button.
Idle	Default	If you choose Default for the Always Use Prime Line for Voice Mail setting in the Phone Configuration, the Common Phone Profile, the Device Profile, or the Default Device Profile Configuration windows, Cisco Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter when determining whether a user, including a Cisco Extension Mobility user, can use this feature. If you choose Default for the Always Use Prime Line for Voice Mail setting in the Phone Configuration window, Cisco Unified Communications Manager uses the configuration from the common phone profile.
Busy	On	If the device is busy, this feature does not work.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature via the clusterwide service parameter, Always Use Prime Line for Voice Message, which supports the Cisco CallManager service, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Always Use Prime Line for Voice Message drop-down list box, choose **True**.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 7.1(1), you can configure this feature per device.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so activate the service by choosing **Tools > Service Activation** in Cisco Unified Serviceability. In addition, you can run SDI trace for the Cisco CallManager service. When you view the log in RTMT, you can see the configured value that is used by the device; for example, alwaysUsePrimeLineForVM=2, which indicates that the device uses the default.

BAT Considerations

The Bulk Administration GUI has the following updates to support the Always Use Prime Line for Voice Mail feature:

Always Use Prime Line for Voice Message drop-down list box—choose one of the following options:

- Off
- On
- Default

Note For details of configuration options for the Always Use Prime Line for Voice Mail feature, refer to Table 3.

Note The Always Use Prime Line for Voice Message drop-down list boxes display in the Phone Template, UDP Template, and Update Phone windows.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For a list of phones that support this feature, see the "Line Select" section on page 145.

For More Information

- Always Use Prime Line, page 16
- Line Select, page 145

Barge, cBarge, and Single Button Barge Support for PLAR

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

Barge, cBarge, or single-button barge allow a phone user to get added to a remotely active call that is on a shared line. Private Line Automatic Ringdown (PLAR) allows the phone user to dial a preconfigured number, and only this number, from the PLAR line. In Cisco Unified Communications Manager 7.1(1), a barge, cBarge, or single-button barge initiator can barge into a call via a shared line that is configured for PLAR; that is, the initiator can barge into the call if the barge target uses the preconfigured number that is associated with the PLAR line while on the call.

In previous releases of Cisco Unified Communications Manager (except for 6.1(3)), Cisco Unified Communications Manager sent the cBarge invocation to the PLAR line before connecting the barge call. If the PLAR line was busy in previous releases, the initiator heard a busy reorder tone. In Cisco Unified Communications Manager 7.1(1) and 6.1(3), Cisco Unified Communications Manager does not send the barge invocation to the PLAR line before connecting the barge call, so the barge occurs no matter what the state of the PLAR destination is.

Cisco Unified Communications Manager Administration Configuration Tips

To make barge, cBarge, or single-button barge work with PLAR, you must configure barge, cBarge, or single-button barge, as described in the “Barge and Privacy” chapter in the *Cisco Unified Communications Manager Features and Services Guide*. In addition, you must configure the PLAR destination, a directory number that is used specifically for PLAR. The following examples describe how to enable PLAR functionality for phones that are running SCCP and for phones that are running SIP.

A and A’ represent shared-line devices that you configured for barge, cBarge, or single-button barge, and B1 represents the directory number for the PLAR destination. To enable PLAR functionality from A/A’, which are running SIP, see the following example:

Tip Step 1 through Step 4 apply if you want to configure PLAR for phones that are running SCCP. For phones that are running SIP, you must perform Step 1 through Step 6.

Example for How to Configure PLAR

Step 1 Create a partition, for example, P1, and a calling search space, for example CSS1, so that CSS1 contains P1. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Class of Control > Partition** or **Calling Search Space**.)

Step 2 Create a translation pattern, for example, TP1, which contains calling search space CSS1 and partition P1. Create a null pattern (blank pattern), but make sure that you enter the directory number for the B1 PLAR destination in the Called Party Transformation Mask field. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Translation Pattern**.)

Step 3 Assign the calling search space, CS1, to either A or A’. (In Cisco Unified Communications Manager Administration, choose **Device > Phone**.)

Step 4 Assign the P1 partition to the directory number for B1, which is the PLAR destination. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Directory Number**.)

Step 5 For phones that are running SIP, create a SIP dial rule. (In Cisco Unified Communications Manager Administration, choose **Call Routing > Dial Rules > SIP Dial Rules**. Choose **7940_7960_OTHER**. Enter a name for the pattern; for example, PLAR1. Click **Save**; then, click **Add Plar.** Click **Save**.)

Step 6 For phones that are running SIP, assign the SIP dial rule configuration that you created for PLAR to the phones, which, in this example, are A and A'. ((In Cisco Unified Communications Manager Administration, choose **Device > Phone**. Choose the SIP dial rule configuration from the SIP Dial Rules drop-down list box.)

GUI Changes

No new configuration settings display in Cisco Unified Communications Manager Administration for this feature.

Service Parameter and Enterprise Parameter Changes

For parameters that you configure for barge, refer to the "Barge and Privacy" chapter in the *Cisco Unified Communications Manager Features and Services Guide* and the "Party Entrance Tone" section on page 88.

Installation/Upgrade (Migration) Considerations

You can use this feature after you install or upgrade to Cisco Unified Communications Manager 7.1(1).

Serviceability Considerations

No special serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

By pressing the Barge, cBarge, or Single Button Barge softkey in the remote in use call state, the initiator gets added to the call with all parties, and all parties receive a barge beep tone (if configured).

For a list of phones that support this feature, see the "Barge Tone Enhancements" section on page 127.

For More Information

- "Barge and Privacy," *Cisco Unified Communications Manager Administration Guide*
- Party Entrance Tone, page 88
- Barge Tone Enhancements, page 127

Calling Party Normalization Enhancements

Description

In the Incoming Number of Digits To Strip fields in Cisco Unified Communications Manager Administration 7.1(1), you can configure the number of leading digits that you want Cisco Unified Communications Manager to strip before applying the prefix to the calling party number. If you configured this functionality in Cisco Unified Communications Manager Administration 7.0(1), see the "Installation/Upgrade (Migration) Considerations" section on page 30 for information on how the configuration is handled after an upgrade to 7.1(1).

Tip You configure the digit-to-strip fields based on the various calling party number types; that is, Subscriber, Unknown, International, and National.

In Cisco Unified Communications Manager 7.1(1), you can configure the Incoming Calling Party Transformation CSS settings for various calling party number types (Subscriber, International, and so on). Configuring these calling search spaces in the device pool, for the gateway, or for the trunk, allows the device to globalize the calling party number for the various calling party number types.

Cisco Unified Communications Manager Administration Configuration Tips

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the fields in Table 4 to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number.

Before you configure the number of leading digits that Cisco Unified Communications Manager must strip from the calling party number, consider the following information.

- The Incoming Prefix service parameters allow you to configure the number of digits that Cisco Unified Communications Manager must strip from the calling party number. For information on how to configure the service parameters for this functionality, see the "Service Parameter and Enterprise Parameter Changes" section on page 28.
- If the word, Default, displays in the field in the Gateway or Trunk Configuration window, Cisco Unified Communications Manager applies the device pool configuration for the incoming calling party number digits- to-strip field. If the word, Default, displays in the digits-to-strip field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the appropriate incoming calling party prefix.
- Be aware that Cisco Unified Communications Manager can strip up to 24 digits. If you enter a value that is larger than 24 in the field, for example, 26, Cisco Unified Communications Manager Administration displays a message and does not allow the configuration.
- To strip digits without prefixing anything, you can configure the fields in Table 4 without configuring the incoming prefix fields. If you do not configure a prefix in the incoming prefix settings, Cisco Unified Communications Manager strips the number of leading digits that you specify in the incoming number of digits to strip settings (Table 4) and does not apply a prefix to the calling party number.
- If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix.

- If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).
- If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

GUI Changes

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can configure the fields in Table 4 to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number.

Table 4 Configuration Settings for Stripping the Number of Digits

Setting	Description
Incoming Calling Party National Digits to Strip	Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of National type before it applies the prefixes. This setting displays in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool)—Applies the configuration to all digital gateways and trunks; that is, if you choose the device pool for the device. • Gateway (Device > Gateway)—Displays setting in the H.323 gateway configuration window and in the port windows (Gateway Configuration window) for MGCP (T1-PRI/BRI) and MGCP (E1-PRI/BRI). • Trunk (Device > Trunk)—Displays setting in all trunk configuration windows except the SIP trunk.
Incoming Calling Party International Digits to Strip	Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of International type before it applies the prefixes. This setting displays in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool)—Applies the configuration to all digital gateways and trunks; that is, if you choose the device pool for the device. • Gateway (Device > Gateway)—Displays setting in H.323 gateway configuration window and in the port windows (Gateway Configuration) for MGCP (T1-PRI/BRI) and MGCP (E1-PRI/BRI). • Trunk (Device > Trunk)—Displays setting in all trunk configuration windows except the SIP trunk.

Table 4 Configuration Settings for Stripping the Number of Digits (continued)

Setting	Description
Incoming Calling Party Subscriber Digits to Strip	Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before it applies the prefixes. This setting displays in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool)—Applies the configuration to all digital gateways and trunks; that is, if you choose the device pool for the device. • Gateway (Device > Gateway)—Displays setting in H.323 gateway configuration window and in the port windows for MGCP (T1-PRI/BRI) MGCP (E1-PRI/BRI). • Trunk (Device > Trunk)—Displays setting in all trunk configuration windows except the SIP trunk.
Incoming Calling Party Unknown Digits to Strip	Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before it applies the prefixes. This setting displays in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool)—Applies the configuration to all digital gateways and trunks; that is, if you choose the device pool for the device. • Gateway (Device > Gateway)—Displays setting in H.323 gateway configuration window and in the port windows for MGCP (T1-PRI/BRI) MGCP (E1-PRI/BRI). • Trunk (Device > Trunk)—Displays setting in all trunk configuration windows, including the SIP trunk.

Table 5 describes the various Incoming Calling Party Transformation CSS settings and lists the configuration windows in Cisco Unified Communications Manager Administration where you assign the settings.

Table 5 Configuring the Incoming Calling Party Transformation CSS

Setting	Description
Incoming Calling Party Transformation CSS for National Number	This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. If you choose None from the drop-down list box, Cisco Unified Communications Manager uses the configuration from the device pool that is assigned to the device. If you did not configure this setting in the device pool, Cisco Unified Communications Manager uses the configuration from the service parameter. You can access this setting in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool) • Gateway (Device > Gateway)—Depending on the gateway type, the setting may display in the port configuration window or the gateway configuration window. • Trunk (Device > Trunk)—The SIP Trunk Configuration window does not display this setting.
Incoming Calling Party Transformation CSS for International Number	This setting allows you to globalize the calling party number of International calling party number type on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. If you choose None from the drop-down list box, Cisco Unified Communications Manager uses the configuration from the device pool that is assigned to the device. If you did not configure this setting in the device pool, Cisco Unified Communications Manager uses the configuration from the service parameter. You can access this setting in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool) • Gateway (Device > Gateway)—Depending on the gateway type, the setting may display in the port configuration window or the gateway configuration window. • Trunk (Device > Trunk)—The SIP Trunk Configuration window does not display this setting.

Table 5 Configuring the Incoming Calling Party Transformation CSS (continued)

Setting	Description
Incoming Calling Party Transformation CSS for Unknown Number	This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. If you choose None from the drop-down list box, Cisco Unified Communications Manager uses the configuration from the device pool that is assigned to the device. If you did not configure this setting in the device pool, Cisco Unified Communications Manager uses the configuration from the service parameter. You can access this setting in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool) • Gateway (Device > Gateway)—Depending on the gateway type, the setting may display in the port configuration window or the gateway configuration window. • Trunk (Device > Trunk)
Incoming Calling Party Transformation CSS for Subscriber Number	This setting allows you to globalize the calling party number of Subscriber calling party number type on the device. Make sure that the Calling Party Transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device. If you choose None from the drop-down list box, Cisco Unified Communications Manager uses the configuration from the device pool that is assigned to the device. If you did not configure this setting in the device pool, Cisco Unified Communications Manager uses the configuration from the service parameter. You can access this setting in the following windows in Cisco Unified Communications Manager Administration: • Device Pool (System > Device Pool) • Gateway (Device > Gateway)—Depending on the gateway type, the setting may display in the port configuration window or the gateway configuration window. • Trunk (Device > Trunk)—The SIP Trunk Configuration window does not display this setting.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameters changes occurred for this feature in 7.1(1).

Tip To locate the service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**; choose the server and the Cisco CallManager service. After the parameters display, click **Advanced**. For information on the service parameter, click the hyperlink for the service parameter name or the question mark that displays in the upper, right corner of the window.

If your service provider prepends leading digits (for example, a zero) to the calling party number and you want to strip these digits before prepending other digits (for example, if the leading digits are not part of the E.164 number and you want to transform the calling party number to the E.164 format), you can enter a colon (:) followed by the number of digits that you want to strip in the Incoming Calling Party National Number Prefix, Incoming Calling Party International Number Prefix, Incoming Calling Party Unknown Number Prefix, and/or Incoming Calling Party Subscriber Number Prefix service parameters to ensure that Cisco Unified Communications Manager strips the leading digits before applying the prefixes to an incoming calling party number. The value that you configure before the colon (:) represents the prefix; the value that you configure after the colon (:) specifies the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number before it applies the prefix.

For example, you configure +:1 in the incoming prefix service parameters, which alerts Cisco Unified Communications Manager to strip the first digit from the calling party number and then apply the international escape character +. If an incoming call arrives as 04423452345, Cisco Unified Communications Manager strips the first digit, in this case, zero, from the calling party number and prefixes the international escape character + to the calling party number. As a result, the calling party number gets transformed to +4423452345.

To strip digits without prefixing anything, you can configure the colon (:) in the incoming prefix service parameters without configuring a prefix. If you do not enter a prefix before the colon (:), Cisco Unified Communications Manager strips the number of leading digits that you specify and does not apply a prefix to the calling party number. For example, if you configure :2, Cisco Unified Communications Manager strips 2 leading digits without applying a prefix.

If you want Cisco Unified Communications Manager to strip a certain number of leading digits, and the entire number of digits for the calling party number equals or specifies less than the value that you configure, Cisco Unified Communications Manager strips all digits but still applies the prefix; that is, if you configure a prefix. For example, if you enter +1:6 in the incoming prefix fields, and the calling party number contains 6 or fewer digits, Cisco Unified Communications Manager strips all digits and applies the prefix +1.

If you configure Cisco Unified Communications Manager to strip more digits than exist in the calling party number, Cisco Unified Communications Manager clears the calling party number (makes it blank).

If you do not configure a colon (:) in the incoming prefix service parameters, Cisco Unified Communications Manager does not strip any digits from the calling party number; that is, unless you configure the incoming fields that are described Table 4, which support the configuration at the device level.

If you configure a prefix but the calling party number that arrives is empty, Cisco Unified Communications Manager does not apply the prefix.

Cisco Unified Communications Manager can strip up to 24 digits from the calling party number. If you enter :26 in the incoming prefix service parameters, Cisco Unified Communications Manager Administration displays a message and does not allow the configuration.

If an error occurs when Cisco Unified Communications Manager attempts to strip the digits and apply the prefix to the calling party number, Cisco Unified Communications Manager does not manipulate the digits or apply the prefixes; instead, Cisco Unified Communications Manager uses the calling party number that arrived for the call.

Tip If you configure the incoming fields that display in the device configuration windows and the service parameters, Cisco Unified Communications Manager uses the configuration that you configured in the device configuration window.

- Incoming Calling Party National Number Prefix - MGCP
- Incoming Calling Party International Number Prefix - MGCP
- Incoming Calling Party Subscriber Number Prefix - MGCP
- Incoming Calling Party Unknown Number Prefix - MGCP

Tip If you have a single H.323, MGCP (T1-PRI/BRI), or MGCP (E1-PRI/BRI) gateway in your network, you can configure the prefix service parameters, which support the Cisco CallManager service, for the particular gateway type in the Service Parameter Configuration window. If you configure the prefix service parameters for a particular gateway type, for example, H.323, be aware that all H.323 gateways that you configure in Cisco Unified Communications Manager Administration use the configuration from the service parameter unless you configure the prefix settings for a particular gateway in the Gateway Configuration window.

- Incoming Calling Party National Number Prefix - H.323
- Incoming Calling Party International Number Prefix - H.323
- Incoming Calling Party Subscriber Number Prefix - H.323
- Incoming Calling Party Unknown Number Prefix - H.323

Tip If the incoming prefix service parameters for H.323 use the same prefix as the incoming prefix service parameters for the phone, the prefix gets used twice for the calling party; first, when the incoming call gets to the gateway and again, when the call terminates at the phone.

- Incoming Calling Party Unknown Number Prefix - SIP

Installation/Upgrade (Migration) Considerations

If you upgrade from Cisco Unified Communications Manager 7.0(1) to 7.1(1), be aware that Cisco Unified Communications Manager moves the numbers of digits that you want stripped from the Incoming Prefix 7.0 fields in the Device Pool, Trunk, or Gateway Configuration windows to the Incoming Digits-to-Strip fields in the same windows in Cisco Unified Communications Manager Administration 7.1(1). For example, if you configured :12 in the Incoming Calling Party International Number Prefix field in the Trunk Configuration window in 7.0(1), 12 displays in the Incoming Calling Party International Digits to Strip field in the Trunk Configuration window after you upgrade to 7.1(1).

If you configured the Incoming Prefix service parameters in 7.0(1) so that Cisco Unified Communications Manager strips leading digits, Cisco Unified Communications Manager 7.1(1) does not change the configuration; that is, Cisco Unified Communications Manager 7.1(1) uses the value, including the : (colon), that you configured in 7.0(1).

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that this service is activated in Cisco Unified Serviceability.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

Depending on your configuration, a phone user may not need to edit the call log directory entry on the phone before placing a call. Depending on your configuration, the phone user may see the international escape character, +, in the call log directories on the phone.

For More Information

- "Calling Party Normalization" chapter, *Cisco Unified Communications Manager Features and Services Guide*

Cisco Unified Communications Manager Assistant

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3) support numeric user ID login for Cisco Unified Communications Manager Assistants from their Cisco Unified IP Phones.

To configure numeric user ID login, perform the following steps:

Procedure

Step 1 When adding a Cisco Unified Communications Manager Assistant user (in Cisco Unified Communications Manager Administration, go to **User Management -> End User**), assign a User ID that is numeric only.

Step 2 In Cisco Unified Communications Manager Administration, go to the Service Parameters window (**System> Service Parameters)**, then select your server and select the Cisco IP Manager Assistant service.

In the section "Clusterwide Parameters (Parameters that apply to all servers)" set Alpha Numeric UserID to **False**.

Step 3 Restart the Cisco IP Manager Assistant service for this configuration change to take effect.

Cisco Web Dialer Configured in Application Server Window

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

In previous releases of Cisco Unified Communications Manager (except for 6.1(3)), the List of WebDialers field in the Service Parameter window supported a maximum of 255 characters, which limited the scalability of the Redirector. In Cisco Unified Communications Manager 7.1(1) and 6.1(3), you configure the WebDialer servers in the Application Server Configuration window instead of the Service Parameters Configuration window.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

It is now possible for you to add a Cisco Web Dialer application server through the Application Server Configuration window. You access the Application Server Configuration window by choosing **System > Application Server** in Cisco Unified Communications Manager Administration. Cisco Web Dialer appears as one of the options in the Application Server Type drop-down list box.

If you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service.

Service Parameter and Enterprise Parameter Changes

In Cisco Unified Communications Manager 7.1(1), you can configure either the List of WebDialers service parameter or the Cisco Web Dialer application server through the Application Server Configuration window. If you add a Cisco Web Dialer application server in the Application Server Configuration window, the server displays in the List of WebDialers field in the Service Parameter Configuration window for the Cisco WebDialer Web Service. You can access the Service Parameter Configuration window by choosing **System > Service Parameters** in Cisco Unified Communications Manager Administration.

Installation/Upgrade (Migration) Considerations

If you install Cisco Unified Communications Manager 7.1(1) and plan to use Cisco Web Dialer, configure the Cisco Web Dialer application server in the Application Server Configuration window. You do not need to configure the List of WebDialers field in the Service Parameter Configuration window if you configure the application server in the Application Server Configuration window.

Serviceability Considerations

Cisco Web Dialer relies on the Cisco WebDialer Web Service. If you have not already done so, activate this service in the Service Activation window in Cisco Unified Serviceability.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

User Tips

For user enhancements for Cisco Web Dialer, see the "WebDialer Enhancements" section on page 149.

For More Information

- "Cisco Web Dialer" chapter, *Cisco Unified Communications Manager Features and Services Guide*
- WebDialer Enhancements, page 149

Internet Protocol Version 6 (IPv6)

This section, which describes IPv6 support for Cisco Unified Communications Manager 7.1(1), contains information on the following topics:

- Description for IPv6 Support, page 33

- Interactions and Restrictions for IPv6, page 34
- IPv6 Configuration Tips, page 36
- CLI Command Changes for IPv6, page 40
- Cisco Unified Communications Operating System IPv6 GUI Changes, page 40
- Cisco Unified Communications Manager Administration IPv6 GUI Changes, page 41
- Service Parameter and Enterprise Parameter Changes for IPv6, page 45
- Installation/Upgrade (Migration) Considerations for IPv6, page 48
- Serviceability and RTMT Considerations for IPv6, page 48
- CAR/CDR Considerations for IPv6, page 50
- Security Considerations for IPv6, page 51
- Supported Phone Models for IPv6, page 52
- Phone Considerations, page 53
- For More Information, page 70

Description for IPv6 Support

Internet Protocol version 6 (IPv6), which is the latest version of the Internet Protocol (IP) that uses packets to exchange data, voice, and video traffic over digital networks, increases the number of network address bits from 32 bits in IPv4 to 128 bits. IPv6 support in the Cisco Unified Communications Manager network allows the network to behave transparently in a dual-stack environment and provides additional IP address space and autoconfiguration capabilities to devices that are connected to the network.

The "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide* contains descriptive information on the following topics:

- Cisco Unified Communications Manager, *Cisco Unified Communications Manager Features and Services Guide*
- Cisco Unified IP Phones, *Cisco Unified Communications Manager Features and Services Guide*
- DHCPv6, *Cisco Unified Communications Manager Features and Services Guide*
- DNS, *Cisco Unified Communications Manager Features and Services Guide*
- Gateways, *Cisco Unified Communications Manager Features and Services Guide*
- Media Termination Points, *Cisco Unified Communications Manager Features and Services Guide*
- SIP Trunks, *Cisco Unified Communications Manager Features and Services Guide*
- TFTP Server, *Cisco Unified Communications Manager Features and Services Guide*

Tip Before you configure IPv6, review the "Internet Protocol Version 6 (IPv6)" chapter carefully. For example, this chapter describes how to configure the Cisco Unified Communications Manager server and phones in dual-stack mode. For example, it also describes how Cisco Unified Communications Manager uses MTPs to translate IPv4 to IPv6 (or vice versa) and so on.

Interactions and Restrictions for IPv6

Some Cisco Unified Communications Manager features do not work for devices with an IP Addressing Mode of IPv6 Only. Before you configure IPv6 Only for a device, review the following section, which describes Cisco Unified Communications Manager feature interactions and restrictions for IPv6.

- Annunciator—Annunciator supports IPv4; if annunciator connects to a device with an IP Addressing Mode of IPv6 Only, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6. If no MTP that can translate IP address versions is available, no announcement plays on the phone.
- Call Detail Records—See the "CAR/CDR Considerations for IPv6" section on page 50.
- Cisco Extension Mobility—Cisco Extension Mobility supports IPv4, so you cannot use phones with an IP Addressing Mode of IPv6 Only for Cisco Extension Mobility. If you want to use Cisco Extension Mobility with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.
- Cisco Unity Connection and Cisco Unity—Cisco Unity Connection and Cisco Unity communicate with Cisco Unified Communications Manager by using IPv4.
- Cisco Unified Communications Manager Assistant—Cisco Unified Communications Manager Assistant does not support IPv6, so you cannot use phones with an IP Addressing Mode of IPv6 Only with Cisco Unified Communications Manager Assistant. If you want to use Cisco Unified Communications Manager Assistant with the phone, make sure that you configure the phone with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6.
- Cisco Unified Communications Operating System—See the "Cisco Unified Communications Operating System IPv6 GUI Changes" section on page 40.
- Cisco Unified Serviceability—See the "Serviceability and RTMT Considerations for IPv6" section on page 48.
- Cisco Web Dialer—Cisco Web Dialer supports IPv4, so to connect to CTI Manager, Cisco Web Dialer uses an IPv4 address. Cisco Web Dialer works with devices with an IP Addressing Mode of IPv4 and IPv6.
- Command Line Interface—See the "CLI Command Changes for IPv6" section on page 40.
- Device Mobility—Device mobility supports IPv4 addresses only, so you cannot use phones with an IP Addressing Mode of IPv6 Only with device mobility.
- Differentiated Services Control Point (DSCP)—Differentiated Services Control Point (DSCP) values are the same for both IPv6 and IPv4.
- DNS—You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.
- H.323 Devices—H.323 clients, gateways, and H.225 intercluster trunks do not support IPv6. To communicate with IPv6 Only devices that connect to these gateways, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 during a call.
- Intercom—Intercom can support phones with an IP Addressing Mode of IPv4 Only or IPv4 and IPv6. During an intercom call, the talkback mode establishes media streams with the same IP version as the media stream that is used when the caller initiated intercom.

- Music On Hold—The IP Voice Media Streaming Application supports IPv4. Cisco Unified Communications Manager does not support IPv6 with multicast music on hold, so devices with an IP Addressing Mode of IPv6 Only cannot support multicast music on hold; under these circumstances, Cisco Unified Communications Manager plays a tone, instead of music, when the phone is on hold. For IPv6 Only devices that uses unicast music on hold, Cisco Unified Communications Manager inserts an MTP that can translate IPv4 to IPv6 (or vice versa) into the media stream.
- QRT—The Quality Report Tool supports IPv6 if the device uses an IP Addressing Mode of IPv4 or IPv4 and IPv6; users with phones with an IP Addressing Mode of IPv6 Only cannot report audio and other problems by pressing the QRT softkey on the phone. In addition, the QRT report does not include the streaming statistics for a phone that has an IP Addressing Mode of IPv6 Only.
- RTMT—See the "Serviceability and RTMT Considerations for IPv6" section on page 48.
- RSVP—RSVP calls support IPv4. If RSVP is required for the call and any of the devices in the call is configured for or uses an IPv6 address, Cisco Unified Communications Manager rejects the call, and the caller hears a busy tone.
- Security—See the "Security Considerations for IPv6" section on page 51.
- SDL—SDL TCP connections support IPv6, but SDL links support IPv4. If you configure a host name in the Server Configuration window in Cisco Unified Communications Manager Administration, SDL queries the DNS A record, which ensures that IPv4 is used. If you specify an IP address, an IPv4 address gets passed down to the SDL layer.
- SIP Phones and TFTP—Phones that run SIP do not support IPv6 addresses. If you configure IPv6 Only as the IP Addressing Mode for a phone that runs SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.
- T.38 Fax—Whether a T.38 fax call uses IPv4 or IPv6 depends on the preference of Cisco Unified Communications Manager and the capabilities of the devices in the call. If one device in the call uses IPv6 and the other device can use IPv4 and IPv6, the call uses IPv6, regardless of the configuration for the signaling and media enterprise parameters in Cisco Unified Communications Manager Administration.

  Cisco Unified Communications Manager supports the following types of T.38 fax calls:

  - SIP-to-SIP call that uses IPv6
  - SIP-to-SIP call that uses IPv4
  - SIP-to-non-SIP call that uses IPv4
  - SIP-to-non-SIP call where the SIP device uses IPv6 and the non-SIP device uses IPv4 with an MTP that can do IPv4/IPv6 conversions

    During the middle of a T.38 fax call, Cisco Unified Communications Manager does not insert an MTP that converts the IP version types; the MTP must already exist in the call.
- Transfer—The transfer components in Cisco Unified Communications Manager uses the IP Addressing Mode and the IP address of the device to determine how to handle the transfer. If the IP capabilities do not match when you transfer a call, Cisco Unified Communications Manager allocates an IPv4/IPv6-capable MTP that can translate IP version, so the transfer can occur.
- Web Browser on the Phone—On the Cisco Unified IP Phone, the http interface for the web browser supports IPv4 addresses, so the phone does not allow web access to servers that use an IPv6 address.
- Video—Cisco Unified Communications Manager supports video IPv6 calls in the following cases:
  - Video devices do not support IPv6, so when the media preference is IPv6, video uses IPv4.

- The audio and video portions of a call negotiate the same IP type for the initial call; that is, if two dual-stack phones are in a call that uses both audio and video, the call uses IPv4 for both the audio and video portions of the initial call, even when the media preference is IPv6.
- If two dual-stack phones negotiate IPv6 for the audio call based on the media preference and then you add video mid-call, the video portion of the call uses IPv4, even if the media preference is IPv6.
- MTPs do not get allocated for video support. For example, a call occurs between two dual-stack phones over a SIP trunk with an IP Addressing Mode of IPv6 Only; IPv6 gets negotiated for the audio portion of the call, and video cannot occur because the video device does not support IPv6. No MTP gets allocated to support the video portion of the call.

IPv6 Configuration Tips

Table 6 displays the configuration checklist for IPv6, which is documented in the "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. Before you configure IPv6 in your network, review Table 6.

Table 6 IPv6 Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Review all IPv6-related documentation before you configure IPv6.	For example, review the following documents: • *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1* • *Cisco IOS IPv6 Configuration Library* • *Implementing VoIP for IPv6* • "Internet Protocol Version 6 (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide*
Step 2	Make sure you have compatible network hardware and Cisco IOS software installed and configured; for example, configure your gateways and Cisco IOS MTP for IPv6.	• *Implementing VoIP for IPv6* • Configuring a Media Termination Point, *Cisco Unified Communications Manager Administration Guide* • Media Termination Points section of "Internet Protocol Version 6 (IPv6) chapter, *Cisco Unified Communications Manager Features and Services Guide*

Table 6 IPv6 Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 3	Provision a local IPv6-capable DNS and DHCP server. **Caution** You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.	Refer to the documentation that supports your DNS and DHCP server(s); for example, *Cisco Network Registrar User's Guide, 6.2.*
Step 4	Install Cisco Unified Communications Manager 7.1 (or upgrade to this release).	Cisco Unified Communications Manager installation or upgrade 7.1 documentation
Step 5	To enable IPv6, perform one of the following tasks: • From Cisco Unified Communications Operating System Administration, navigate to **Settings > IP > Ethernet IPv6** and check the **Enable IPv6** check box. • Run the CLI command, **set network ipv6 service enable**, to enable IPv6 in the operating system on the server. **Tip** For each server in the cluster, perform this task. Running this command requires a reboot of the server.	For more information on accessing Cisco Unified Communications Operating System Administration, refer to the *Cisco Unified Communications Operating System Administration Guide*. For information on how to run CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.
Step 6	If you want the DHCPv6 server to issue a non-link-local IPv6 address to the Cisco Unified Communications Manager, perform one of the following tasks: • From Cisco Unified Communications Operating System Administration, navigate to **Settings > IP > Ethernet IPv6** and choose **DHCP** for the Address Source. • Run the CLI command, **set network ipv6 dhcp enable**. **Tip** For each server in the cluster, perform this task. Running this command requires a reboot of the server. **Tip** Ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address from the DHCPv6 server.	For more information on accessing Cisco Unified Communications Operating System Administration, refer to the *Cisco Unified Communications Operating System Administration Guide*. For information on how to run CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Table 6 IPv6 Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 7	If you want to use a static IPv6 address for the Cisco Unified Communications Manager, perform one of the following tasks: • From Cisco Unified Communications Operating System Administration, navigate to **Settings > IP > Ethernet IPv6**, choose **Manual Entry** for the Address Source, and enter the IPv6 address and mask. • Run the CLI command, **set network ipv6 static_address <addr> <mask>**. **Note** Manually configuring the IPv6 and mask assumes that you do not want the Cisco Unified Communications Manager to get the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration (SLAAC). **Tip** For each server in the cluster, perform this task. Running this command requires a reboot of the server.	For more information on accessing Cisco Unified Communications Operating System Administration, refer to the *Cisco Unified Communications Operating System Administration Guide*. For information on how to issue CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.
Step 8	In the Enterprise Parameters Configuration window in Cisco Unified Communications Manager Administration, choose **True** for the Enable IPv6 enterprise parameter. **Tip** After you update this enterprise parameter, restart the Cisco CallManager, CTIManager, and the Certificate Authority Proxy Function services in Cisco Unified Serviceability.	Service Parameter and Enterprise Parameter Changes for IPv6, page 45

Table 6 IPv6 Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 9	For the server that you are configuring in Cisco Unified Communications Manager Administration, choose **System > Server** and enter the non-link-local IPv6 address or a host name that can resolve to IPv6 addresses in the IPv6 Name field. **Tip** For each server in the cluster, perform this task. **Tip** For each server in the cluster, you must also configure the Host Name/IP Address field, which supports either an IPv4 address or a host name that can resolve to an IPv4 address. **Tip** Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information. **Caution** You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot. To display the non-link-local IPv6 address for the Cisco Unified Communications Manager server, you can run the CLI command, **show network ipv6 settings**.	• Configuring a Server, *Cisco Unified Communications Manager Administration Guide* • CLI Command Changes for IPv6, page 40 • Cisco Unified Communications Manager Administration IPv6 GUI Changes, page 41
Step 10	In Cisco Unified Communications Manager Administration, configure phone-related and SIP trunk-related IPv6 settings. For example, configure the IP Addressing Mode and Allow Auto-Configuration of Phones settings in the Common Device Profile Configuration window; then, apply the common device profile configuration to the phone or SIP trunk.	• Cisco Unified Communications Manager Administration IPv6 GUI Changes, page 41 • Configuring a SIP Route Pattern, *Cisco Unified Communications Manager Administration Guide* • Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide* • Configuring a Common Device Configuration, *Cisco Unified Communications Manager Administration Guide*
Step 11	Restart the Cisco CallManager, CTIManager, and Cisco Certificate Authority Proxy services in Cisco Unified Serviceability.	*Cisco Unified Serviceability Administration Guide*

CLI Command Changes for IPv6

In the Command Line Interface, you can run the following IPv6 commands on each server in the cluster:

- Mandatory command—To enable IPv6 in the Cisco Unified Communications Operating System, run the command, **set network ipv6 service enable**.
- Optional command, depending on the requirements of your network—If you want the DHCPv6 server to issue a non-link-local IPv6 address to the Cisco Unified Communications Manager server, run the command, **set network ipv6 dhcp enable**.

Tip Ensure that the Cisco Unified Communications Manager server only obtains one non-link-local IPv6 address. If the server has more than one IPv6 address, Cisco Unified Communications Manager may not behave as expected.

- Optional command, depending on the requirements of your network—If you want to use a static IPv6 address for the Cisco Unified Communications Manager, run the CLI command, **set network ipv6 static_address <addr> <mask>**. Running this command assumes that you do not want the Cisco Unified Communications Manager to get the IPv6 address from the DHCPv6 server or via stateless address autoconfiguration.
- Optional command—To view the IPv6 configuration for the Cisco Unified Communications Manager server, run the command, **show network ipv6 settings**.
- Optional command, depending on your network—To verify that you can ping other servers in the network, run the command, **utils network ipv6 ping <ipv6 address>**.

Running these commands requires that you restart the server. For information on how to run CLI commands, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*.

Cisco Unified Communications Operating System IPv6 GUI Changes

If you want to configure the Cisco Unified Communications Operating System instead of running CLI command, you can enable IPv6 in the Cisco Unified Communications Operating System, enable the DHCPv6 client in Cisco Unified Communications Manager to request an IPv6 address from the DHCPv6 server, or assign a static address to the server in the Cisco Unified Communications Operating System. Use the following procedure to enable and configure IPv6 on the server.

Note All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Settings > IP > Ethernet IPv6**.

The Ethernet IPv6 Configuration window displays.

Step 2 To modify the Ethernet settings, enter the new values in the appropriate fields. For a description of the fields on the Ethernet IPv6 Configuration window, see Table 7.

Step 3 To preserve your changes, click **Save**.

Note If you check the Update with Reboot check box, the system reboots after you click Save. For the IPv6 settings to take effect, you must reboot the system.

Table 7 Ethernet IPv6 Configuration Fields and Descriptions

Field	Description
Enable IPv6	Check this check box to enable IPv6 on the server.
Address Source	Choose one of the following IP address source: • Router Advertisement • DHCP • Manual Entry/Mask The three IP address sources are mutually exclusive. **Note** Unless you specify Manual Entry, the IP Address and Mask fields are read only.
IPv6 Address	If you chose Manual Entry, enter the IPv6 address of the server; for example: fd6:2:6:96:21e:bff:fecc:2e3a
IPv6 Mask	If you chose Manual Entry, enter the IPv6 mask; for example: 64
Update with Reboot	If you want the system to reboot immediately after you click Save, check this check box. If you want to reboot later, leave the check box blank. **Note** For the IPv6 settings to take effect, you must reboot the system.

Cisco Unified Communications Manager Administration IPv6 GUI Changes

Table 8 describes the IPv6 and IPv4 settings that are in Cisco Unified Communications Manager Administration. For some IPv6 settings in Table 8, equivalent settings for IPv4 display in Cisco Unified Communications Manager Administration; for example, in the SIP Trunk Configuration window, you can configure either the Destination Address IPv6 setting or the Destination Address setting, or both settings, depending on the IP support in your network.

For related configuration procedures, refer to the following sections:

- Service Parameter and Enterprise Parameter Changes for IPv6, page 45
- Configuring a Server, *Cisco Unified Communications Manager Administration Guide*
- Configuring a SIP Route Pattern, *Cisco Unified Communications Manager Administration Guide*
- Configuring a Common Device Configuration, *Cisco Unified Communications Manager Administration Guide*
- Configuring a Trunk, *Cisco Unified Communications Manager Administration Guide*

Table 8 IPv6 Settings in Cisco Unified Communications Manager Administration

Configuration Setting	Description
System > Server	
IPv6 Name	This field supports IPv6. If your network uses DNS that can map to IPv6 addresses, you can enter the host name of the Cisco Unified Communications Manager server. Otherwise, enter the non-link-local IP address of the Cisco Unified Communications Manager server; for information on how to obtain the non-link local IP address, run the CLI command, **show network ipv6 settings**. This field, which gets included in the TFTP configuration file, gets used by phones that run SCCP to retrieve the IPv6 address of the Cisco Unified Communications Manager server so that phone registration occurs. **Tip** Remember to update the DNS server with the appropriate Cisco Unified Communications Manager name and address information. You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot. **Tip** In addition to configuring the IPv6 Name field, you must configure the Host Name/IP Address field in the Server Configuration window, so Cisco Unified Communications Manager can support features/devices that use IPv4 (or IPv4 and IPv6).
Call Routing > SIP Route Patterns	
IPv6 Pattern	Cisco Unified Communications Manager uses SIP route patterns to route or block both internal and external calls. The IPv6 address in this field provides the basis for routing internal and external calls to SIP trunks that support IPv6. **Tip** If the SIP trunk supports both IPv4 and IPv6, configure the IPv4 Pattern field in addition to the IPv6 Pattern.

Table 8 IPv6 Settings in Cisco Unified Communications Manager Administration (continued)

Configuration Setting	Description
Device > Device Settings > Common Device Configuration	
IP Addressing Mode	Choose the version of IP address that the device (SIP trunk or phone that runs SCCP) uses to connect to Cisco Unified Communications Manager. From the drop-down list box, choose one of the following options: • IPv4 Only—For both media and signaling events, the device uses an IPv4 address to connect to Cisco Unified Communications Manager. If an IPv4 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv6 address. • IPv6 Only—For both media and signaling events, the device uses an IPv6 address to connect to Cisco Unified Communications Manager. If an IPv6 address is not available for the device, the call fails. If you choose this option, the phone releases an IPv4 address. Phones that run SIP do not support IPv6, so do not choose this option for these phones. If you configure IPv6 Only as the IP Addressing Mode for phones that run SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file. • IPv4 and IPv6 (Default)—Choose this option for dual-stack devices, which can have both an IPv4 and IPv6 address. For both media and signaling events, the dual-stack device uses either an IPv4 or an IPv6 address to connect to Cisco Unified Communications Manager. If only an IPv4 or IPv6 is available for a device (not both types of IP addresses), the device uses the available IP address to negotiate the call. If the device has both IP address types for both signaling and media events, Cisco Unified Communications Manager uses the configuration for IP Addressing Mode Preference for Signaling setting for signaling events and the IP Addressing Mode Preference for Media enterprise parameter for media events.
IP Addressing Mode Preference for Signaling	For dual-stack phones, which support both IPv4 and IPv6 addresses, choose the version of IP address that the phone prefers to establish a connection to Cisco Unified Communications Manager during a signaling event. For dual-stack SIP trunks, choose the version of IP address that the SIP trunk uses to connect to the peer device for signaling events. From the drop-down list box, choose one of the following options: • IPv4—The dual-stack device prefers to establish a connection via an IPv4 address during a signaling event. • IPv6—The dual-stack device prefers to establish a connection via an IPv6 address during a signaling event. • Use System Default—The configuration for the enterprise parameter, IP Addressing Mode Preference for Signaling, applies.

Table 8 IPv6 Settings in Cisco Unified Communications Manager Administration (continued)

Configuration Setting	Description
Allow Auto-Configuration for Phones	The options in this drop-down list box apply to IPv6 for dual-stack Cisco Unified IP Phones that run SCCP. From the drop-down list box, choose one of the following options: • On—The phone uses the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address. Phones also require a TFTP server address to register with Cisco Unified Communications Manager. It is recommended that you obtain the TFTP server address from a DHCPv6 server, although you can manually configure the TFTP server address via the interface on the phone. To indicate to the phone that it needs to use the DHCPv6 server to obtain other information, ensure that the O (Other information) bit /flag is set in the Router Assignments that is sent by the link local router. • Off—The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server. **Tip** Ensure that the M (Managed address configuration) bit/ flag is set in the Router Advertisements that is sent by the link local router, which indicates that the phone should use DHCP for all addressing information. • Default—To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option.
Device > SIP Trunk	
Destination Address IPv6	The Destination IPv6 Address represents the remote SIP peer with which this trunk will communicate. The allowed values for this field specify a valid IPv6 address (global unicast, unique local, link local, mapped IPv4, or a host name), a fully qualified domain name (FQDN), or a DNS SRV record only if the Destination Address is an SRV field is checked. SIP trunks only accept incoming requests from the configured Destination IPv6 Address and the specified incoming port that is specified in the SIP Trunk Security Profile that is associated with this trunk. If the remote end is a Cisco Unified Communications Manager cluster, consider entering the DNS SRV record in this field. The DNS SRV record should include all Cisco Unified Communications Managers within the cluster. **Tip** For SIP trunks that run in dual-stack mode or that support an IP Addressing Mode of IPv6 Only, configure this field. If the SIP trunk runs in dual-stack mode, you must also configure the Destination Address field.

Table 8 IPv6 Settings in Cisco Unified Communications Manager Administration (continued)

Configuration Setting	Description
Device > Device Settings > SIP Profile	
Enable ANAT	This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. When you check both the Enable ANAT and the Media Termination Point Required check boxes, Cisco Unified Communications Manager inserts a dual-stack MTP and sends out an offer with two m-lines, one for IPv4 and another for IPv6. If a dual- stack MTP cannot be allocated, Cisco Unified Communications Manager sends an INVITE without SDP. When you check the Enable ANAT check box and the Media Termination Point Required check box is unchecked, Cisco Unified Communications Manager sends an INVITE without SDP. When both the Enable ANAT and Media Termination Point Required check boxes display as unchecked (or when an MTP cannot be allocated), Cisco Unified Communications Manager sends an INVITE without SDP. When you uncheck the Enable ANAT check box but you check the Media Termination Point Required check box, consider the information, which assumes that an MTP can be allocated: • Cisco Unified Communications Manager sends an IPv4 address in the SDP for SIP trunks with an IP Addressing Mode of IPv4 Only. • Cisco Unified Communications Manager sends an IPv6 address in the SDP for SIP trunks with an IP Addressing Mode of IPv6 Only. • For dual-stack SIP trunks, Cisco Unified Communications Manager determines which IP address type to send in the SDP based on the configuration for the IP Addressing Mode Preference for Media enterprise parameter.

Service Parameter and Enterprise Parameter Changes for IPv6

Table 9 describes the enterprise and service parameters that you can configure for IPv6. To configure enterprise parameters in Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**. To configure service parameters in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**.

Tip For a step-by-step procedure on how to configure enterprise parameters, refer to the "Enterprise Parameters Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*. For a step-by-step procedure on how to configure service parameters, refer to the "Service Parameters Configuration" in the *Cisco Unified Communications Manager Administration Guide*.

Table 9 Enterprise and Service Parameters for IPv6

Parameter	Description
Enable IPv6	This enterprise parameter specifies whether Cisco Unified Communications Manager can negotiate calls by using IPv6 and whether phone can advertise an IPv6 address. Before you set this parameter to True, make sure that you issued the CLI command, set network ipv6 service enable, on all servers in the cluster. Setting this parameter to True causes the Cisco CallManager service to run in dual-stack mode, which is required for interacting with devices that support IPv6. The default value equals False, which means that Cisco Unified Communications Manager cannot negotiate calls by using IPv6 and phones cannot advertise an IPv6 address. After you update this enterprise parameter, restart the Cisco CallManager, CTIManager, and the Certificate Authority Proxy Function services in Cisco Unified Serviceability.
IP Addressing Mode Preference for Media	This enterprise parameter, which applies only to dual-stack devices, specifies the addressing mode that Cisco Unified Communications Manager uses for media events when both IPv4 and IPv6 addresses are available from each device on the call. The default value equals Prefer IPv4.
IP Addressing Mode Preference for Signaling	This enterprise parameter, which applies only to dual-stack devices, specifies how the dual-stack phone connects to Cisco Unified Communications Manager for signaling events and how the dual-stack SIP trunk connects to the peer device for signaling events. The default value equals Prefer IPv4.
Allow Auto-Configuration for Phones	This parameter determines whether the phone is allowed to obtain an address through stateless autoconfiguration. Valid values specify On (the phone obtains its address as specified by the router advertisements, which may be stateless or stateful, depending on the router configuration) or Off (the phone always uses DHCPv6 to obtain its IPv6 address).
Call Counting CAC Enabled	This service parameter, which supports the Cisco CallManager service, determines whether Cisco Unified Communications Manager uses call counting as part of the locations-based call admission control (CAC) feature. Call counting uses a fixed bandwidth value to reserve and adjust bandwidth per call, regardless of the codec or media payload or the Internet Protocol Version (IPv6 or IPv4) used for each call. Call counting may potentially over-subscribe or under-subscribe bandwidth because a fixed-value bandwidth gets reserved per call no matter what the actual bandwidth is for the call. Cisco recommends you leave this parameter set to the default value of False (disabled) unless your network requires the call counting feature. To enable call counting for CAC, choose True for the parameter; to disable call counting for CAC, choose False. This service parameter applies to IPv4 and IPv6 calls.
Audio Bandwidth For Call Counting CAC	This service parameter, which supports the Cisco CallManager service, specifies the amount of bandwidth to deduct from the available bandwidth for audio calls after you set the Call Counting CAC Enabled parameter to True. For each audio call, the amount of bandwidth that you enter in this field gets deducted, regardless if more or less bandwidth is actually used for the call. This service parameter applies to IPv4 and IPv6 calls.

Table 9 Enterprise and Service Parameters for IPv6 (continued)

Parameter	Description
Video Bandwidth For Call Counting CAC	This service parameter, which supports the Cisco CallManager service, specifies the units of bandwidth to deduct from the available bandwidth for video calls after you set the Call Counting CAC Enabled parameter to True. For each video call, the available bandwidth gets reduced by the number of units that is required to account for the actual bandwidth usage. For example, if you specify 512 kbps as the bandwidth unit in this parameter, and a video call utilizes 384 kbps, then one unit, 512 kbps, will be deducted from available bandwidth. Likewise, if you specify 512 kbps in this parameter and a video call negotiated 768 kbps, then 2 units of bandwidth (1064 kbps) will be deducted from the available bandwidth. This service parameter applies to IPv4 and IPv6 calls.
TFTP IPv6 Address	This service parameter, which supports the Cisco TFTP service, specifies the IPv6 address of the NIC card to use for serving files via TFTP to the phone. If your TFTP server has multiple IPv6 addresses, use this parameter in combination with the Server IP Track parameter; that is, in this field, enter the IPv6 address of the NIC card to use for serving files via TFTP and then set the Server IP Track to False. In addition, the you must set the Enable IPV6 enterprise parameter must be True; otherwise, TFTP ignores this parameter. Enter only one IP address in this field. To want the TFTP server to listen to requests from devices that use different types of IPv6 address, leave this field blank. **Tip** To access this parameter in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**; after you choose the server and service in the Service Parameter Configuration window and click **Advanced**, the service parameter displays.

Table 9 Enterprise and Service Parameters for IPv6 (continued)

Parameter	Description
Server IP Track	This service parameter, which supports the Cisco TFTP service, determines whether the TFTP server listens to file requests from any IP address or the specific IP address that is configured for either the TFTP IPv4 Address or TFTP IPv6 Address service parameters. If you want to the TFTP server to listen for file requests from any IP address in both IPv4 or IPv6 networks, choose True; if you want to use the IP address that the TFTP IPv6 Address or TFTP IPv4 Address parameter specifies, choose False. Use this parameter and the TFTP IPv6 Address service parameter together if the TFTP server has multiple NIC cards. In this case, set this parameter to False and set the TFTP IPv6 Address parameter to the IP address of the NIC card to use for serving files via TFTP. If you configure any of the addresses to loopback or leave blank, the TFTP server listens for file requests from any IP address. **Tip** To access this parameter in Cisco Unified Communications Manager Administration, choose **System > Service Parameters**; after you choose the server and service in the Service Parameter Configuration window and click **Advanced**, the service parameter displays.
Alternate Cisco File Server(s)	These service parameters, which support the Cisco TFTP service, allow you to configure alternate Cisco file servers, which are TFTP servers that are on a different cluster. These parameters, which support either IPv4 or IPv6 addresses or host names that resolve to an IP address, determine the IP stack that the TFTP uses to communicate between primary and alternate file servers. If an alternate file server supports dual-stack mode and you want to set both IPv4 and IPv6 addresses for the same server in these parameter fields, you must add both IP addresses, one per field, and the TFTP server tries each address in the order that you configure.

Installation/Upgrade (Migration) Considerations for IPv6

Cisco Unified Communications Manager supports IPv6 after you install 7.1(1) or upgrade to 7.1(1).

Caution You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

For additional considerations, see Table 6 on page 36.

Serviceability and RTMT Considerations for IPv6

Alarms that report IPv4 addresses may also report IPv6 addresses, depending on the configuration in your network. For information on how to configure alarms and view alarm definitions in Cisco Unified Serviceability, refer to the *Cisco Unified Serviceability Administration Guide*.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

IPv6 impacts the Cisco CallManager, CTIManager, and Certificate Authority Proxy Function services in Cisco Unified Serviceability. Depending on the configuration tasks that you perform in Cisco Unified Communications Manager Administration, you may need to restart these services after you configure IPv6. (For example, you must restart these services after you set the Enable IPv6 enterprise parameter to True.)

In RTMT, you can monitor CTI applications, CTI devices, and CTI lines that use IPv6 addresses. When you search for the application, device, or line, enter the IPv6 address. and check the AppIpv6Addr check box in the attribute window.

In addition, you can perform a device search on phones or SIP trunks that use IPv6 addresses. When you choose CallManager > Device Search > Open Device Search > Phones (or SIP Trunks), make sure that you specify an IPv6 address and check the Ipv6Address check box in the attributes window.

Log files may display IPv4 and IPv6 addresses, depending on the configuration in your network.

In RTMT, the performance monitoring counters in Table 10 display for the IP6 object, which provide IPv6-related statistics for your system.

Table 10 IP6

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated as a result of fragmentation at this entity.
Frag Fails	This counter represents the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not, for example because their Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that have been successfully fragmented at this entity.
In Delivers	This counter represents the total number of input datagrams successfully delivered to IP user-protocols (including Internet Control Message Protocol [ICMP]).
In Discards	This counter represents the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams discarded due to errors in their IP header, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
In Receives	This counter represents the number of input datagrams received from all network interfaces, including those received with errors.
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the total number of IP datagrams received and the number of IP datagrams sent.
Out Discards	This counter represents the number of output IP datagrams that was not transmitted and was discarded. One reason may be a lack of buffer space.

Table 10 IP6 (continued)

Counters	Counter Descriptions
Out Requests	This counter represents the total number of IP datagrams which local IP user-protocols (including Internet Control Message Protocol [ICMP]) supply to IP in requests transmission. This counter does not include any datagrams counted in ForwDatagrams.
Reasm Fails	This counter represents the number of failures detected by the IP reassembly algorithm (for various reasons, for example timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that have been successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments received which needed to be reassembled at this entity.

CAR/CDR Considerations for IPv6

Table 11 provides descriptions for the new CDR fields that support IPv6.

Table 11 IPv6 CDR Field Descriptions

Field Name	Range of Values	Description
origIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that originates the call signalling. The field can be either IPv4 or IPv6 format depending on the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field is the address of the Cisco Unified IP Phone. For PSTN calls, this field is the address of the gateway. For intercluster calls, this field is the address of the remote Cisco Unified Communications Manager. The IP address is either in dotted decimal format or in colon separated hexadecimal format. Default - The IP address of the originating device as reported by the device or used for the call after media negotiation.

Table 11 IPv6 CDR Field Descriptions (continued)

Field Name	Range of Values	Description
destIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that terminates the call signalling. The field can be either in IPv4 or IPv6 format depending upon the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field is the address of the Cisco Unified IP Phone. For PSTN calls, this field is the address of the gateway. For intercluster calls, this field is the address of the remote Cisco Unified Communications Manager. The IP address is either in dotted decimal format or in colon separated hexadecimal format. Default - Empty String "" or null. If the destination does not get reached, this field stays empty.

Security Considerations for IPv6

CAPF can issue and upgrade certificates to a phone that uses an IPv4, an IPv6, or both types of addresses. Table 12 describes how a phone that has an IPv4, IPv6, or both types of addresses connects to CAPF.

When the phone connects to CAPF to get a certificate, CAPF uses the configuration from the Enable IPv6 enterprise parameter to determine whether to issue or upgrade the certificate to the phone. If the enterprise parameter is set to False, CAPF ignores/rejects connections from phones that use IPv6 addresses, and the phone does not receive the certificate.

Table 12 How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF; if the phone cannot connect via an IPv6 address, it attempts to connect by using an IPv4 address.
Dual-stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.

Table 12 How IPv6 or IPv4 Phone Connects to CAPF (continued)

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv6	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv4	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
IPv6	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4	IPv4	IPv6	Phone cannot connect to CAPF.
IPv6	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6	IPv6	IPv4	Phone cannot connect to CAPF.

Supported Phone Models for IPv6

The following Cisco Unified IP Phones that run SCCP support IPv6:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G

Phone Considerations

The Cisco Unified IP Phone uses the internet protocol to provide voice communication over the network. Previous to Cisco Unified Communications Manager release 7.1, only the internet protocol version 4 (IPv4) was supported. Because it uses a 32-bit address, IPv4 cannot meet the increased demands for unique IP addresses for all devices that can connect to the internet. Internet Protocol version 6 (IPv6) is an updated version of the current Internet Protocol, IPv4. IPv6 uses a 128-bit address and provides end-to-end security capabilities, enhanced Quality of Service (QoS), and increased number of available IP addresses.

The Cisco Unified IP Phone supports IPv4 only addressing mode, IPv6 only addressing mode, as well as an IPv4/IPv6 dual stack addressing mode. In IPv4, you can enter each octet of the IP address on the phone in dotted decimal notation; for example, 192.240.22.5. In IPv6, you can enter each octet of the IP address in hexadecimal notation with each octet separated by a colon; for example, 2005:db8:0:1:ef8:9876:ba72:dc9a. The phone truncates and removes leading zeros when it displays the IPv6 address.

Cisco Unified IP Phones support both IPv4 and an IPv6 address transparently, so users can handle all calls on the phone to which they are accustomed. Cisco Unified IP Phones support the use of IPv6 only with Cisco Unified Communications Manager release 7.1 and only with the Skinny Call Control Protocol (SCCP).

Cisco Unified IP Phones do not support URLs with IPv6 addresses in the URL. This affects all IP Phone Service URLs, including services, directories, messages, help, and any restricted web services that require the phone to use the HTTP protocol to validate the credentials with the Authentication URL. If you configure Cisco Unified IP Phone services for Cisco Unified IP Phones, you must configure the phone and the servers that support the phone service with IPv4 addresses.

If you configure IPv6 Only as the IP Addressing Mode for phones that are running SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

Table 13 describes the networking protocols on the Cisco Unified IP Phone and whether the protocols support IPv6.

Table 13 Supported Networking Protocols on the Cisco Unified IP Phone

Networking Protocol	Purpose	Usage Notes
Hypertext Transfer Protocol (HTTP)	HTTP is the standard way of transferring information and moving documents across the Internet and the web.	Cisco Unified IP Phones use HTTP for the XML services and for troubleshooting purposes. Cisco Unified IP Phones do not support the use of IPv6 addresses in the URL. You cannot use a literal IPv6 address in the URL or a hostname that maps to an IPv6 address.
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	To communicate using IP, network devices must have an assigned IP address, subnet, and gateway. IP addresses, subnets, and gateways identifications are automatically assigned if you are using the Cisco Unified IP Phone with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each phone locally. The Cisco Unified IP Phone supports concurrent IPv4 and IPv6 addresses. Configure the IP addressing mode (IPv4 only, IPv6 only, and both IPv4 and IPv6) in Cisco Unified Communications Manager Administration. For more information, refer to the "Understanding IPv6" chapter in the *Cisco Unified Communications Manager System Guide*.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* provides the ability to control the attributes of an end-to-end call. You can configure the Cisco Unified IP Phone to use either SIP or Skinny Client Control Protocol (SCCP). Cisco Unified IP Phones do not support the SIP protocol when the phones are operating in IPv6 address mode.

The following section provides information on how DHCP and Autoconfiguration affects the network settings on the phone. You can choose to configure the IP address and other network settings, such as the TFTP server, DNS server, domain, name, etc. on an IP phone manually or by using a router and/or a DHCP server to automatically assign the IP address and other network information. For more information on how the Auto IP Configuration and DHCPv6 settings determine where the IP Phone acquires its IPv6 address and other network settings, see Table 14.

Tip If you are not using DHCP in your network, you must configure these network settings on the Cisco Unified IP Phone after installing the phone on the network:

IP address

IP subnet information (subnet mask for IPv4 and subnet prefix length for IPv6)

Table 14 Determining Where a Phone Acquires its Network Settings

DHCPv6	Auto IP Configuration	How the Phone Acquires its IP address and Network Settings
Disabled	Disabled	You must manually configure an IP address and the other network settings. **Note** When DHCPv6 is disabled, the Auto IP Configuration setting is ignored.
Disabled	Enabled	You must manually configure an IP address and the other network settings. **Note** When DHCPv6 is disabled, the Auto IP Configuration setting is ignored.
Enabled	Disabled	The DHCP server assigns the IP address and the other network settings to the phone.
Enabled	Enabled	When the M-bit is set on the router, the O-bit is ignored. The phone can set its IPv6 address based on an IPv6 address that it received from a DHCPv6 server or the phone can acquire its IPv6 address through stateless address autoconfiguration. When the M-bit is not set, you should set the O-bit is set on the router. The phone will then acquire its IPv6 address through stateless address autoconfiguration. It will not request an IPv6 address from the DHCPv6 server, but it will request other network configuration information.

Table 15 describes the phone menus that relate to IPv4 and IPv6. When you edit the value of an option setting on the phone, follow these guidelines:

- To enter a period (for example, in an IP address under IPv4 Configuration), press the **.** (period) softkey or press ***** on the keypad.
- To enter a colon (for example, in an IP address under IPv6 Configuration), press the : (colon) softkey or press * on the keypad.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus

Configuration Setting	Purpose	Description
Settings > Network Configuration Menu		
IPv4 Configuration	Internet Protocol v4 address menu. In the IPv4 Configuration menu, you can do the following: • Enable or disable the phone to use the IPv4 address that is assigned by the DHCPv4 server. • Manually set the IPv4 Address, Subnet Mask, Default Routers, DNSv4 Server, and Alternate TFTP servers for IPv4. For more information on the IPv4 address fields, refer to the specific field within this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to IPv4 Configuration and press the **Select** softkey.
IPv6 Configuration	Internet Protocol v6 address menu. In the IPv6 Configuration menu, you can do the following: • Enable or disable the phone to use the IPv6 address that is assigned by the DHCPv6 server or to use the IPv6 address that it acquires through Stateless Address Autoconfiguration (SLAAC). • Manually set the IPv6 Address, Subnet Prefix Length, DNSv6 Server, and IPv6 TFTP Servers. For more information on the IPv6 address fields, refer to the specific field within this table. For more information on SLAAC, refer to *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1*.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to IPv6 Configuration and press the **Select** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides. **Note** If the phone receives different domain names from the DHCPv4 and DHCPv6 servers, the domain name from the DHCPv6 will take precedence.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Disable DHCP. If the IP Addressing mode is configured for IPv4 only, set the DHCP option to **No**. If the IP Addressing mode is configured for IPv6 only, set the DHCPv6 option to **No**. If the IP Addressing mode is configured for both IPv4 and IPv6, set both DHCP option and DHCPv6 to **No**. 3. Scroll to the Domain Name option, press the **Edit** softkey, and then enter a new domain name. 4. Press the **Validate** softkey and then press the **Save** softkey.
Settings > Network Configuration Menu > IPv4 Configuration Menu		
DHCP	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone anIPv4 address. When DHCP is disabled, the administrator must manually assign an IPv4 address to the phone.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCP option and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IP Address	Internet Protocol version 4 (IPv4) address of the phone. If you assign an IPv4 address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
Subnet Mask	Subnet mask used by the phone.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to No. 3. Scroll to the Subnet Mask option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to No. 3. Scroll to the appropriate Default Router option, press the **Edit** softkey, and then enter a new router IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup routers. 6. Press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to No. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup DNS servers. 6. Press the **Save** softkey.
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IPv4 address.	Display only—Cannot configure.
DHCP Address Released	Releases the IPv4 address that was assigned by the DHCP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCP Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Alternate TFTP	Indicates whether the phone is using an alternate TFTP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the Alternate TFTP option and press the **Yes** softkey if the phone should use an alternate TFTP server. 3. Press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone with an IPv4 address. If you are not using DHCPv4 in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes or disable DHCP, you must enter a non-zero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 1 option. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Any manually assigned IPv6 TFTP Servers • Any manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. If DHCP is enabled, set the Alternate TFTP option to Yes. 3. Scroll to the TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
TFTP Server 2	Optional backup TFTP server that the phone with an IPv4 address uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 2 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 2 option. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Manually assigned IPv6 TFTP Servers • Manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—Cannot configure.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Settings > Network Configuration Menu > IPv6 Configuration Menu		
DHCPv6	Indicates whether the phone has DHCPv6 enabled or disabled. When DHCPv6 is enabled, the DHCPv6 server assigns the phone an IPv6 address. When DHCP v6 is disabled, the administrator must manually assign an IPv6 address to the phone. The DHCPv6 setting along with the Auto IP Configuration setting determine how the IP Phone obtains its network settings. For more information on how these two settings affect the network settings on the phone, see Table 14 (Determining Where a Phone Acquires its Network Settings).	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCPv6 option and press the **No** softkey to disable DHCPv6, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.
IPv6 Address	Internet Protocol version 6 (IPv6) address of the phone. The IPv6 address is a 128 bit address. If you assign an IP address with this option, you must also assign the IPv6 prefix length. See the IPv6 Subnet Prefix options in this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
IPv6 Prefix Length	Subnet prefix length that is used by the phone. The subnet prefix length is a decimal value from 1-128, that specifies the portion of the IPv6 address that comprises the subnet.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IPv6 Prefix Length option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Default Router 1	Default router used by the phone (Default Router 1). **Note** The phone obtains information on the default router from IPv6 Router Advertisements.	Display only—Cannot configure.
IPv6 DNS Server 1 IPv6 DNS Server 2	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2) used by the phone. If your configuration includes both DNSv6 and DNSv4 servers, the phone will look for its DNS server in the following order: • IPv6 DNS Server 1 • IPv6 DNS Server 2 • DNS Server 1-5 for IPv4 (respectively)	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to No. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign the backup DNS server. 6. Press the **Save** softkey.
IPv6 Address Released	Releases the IPv6 address that the phone has acquired from the DHCPv6 server or by stateless address autoconfiguration. **Note** This field is only editable when the DHCPv6 option is enabled.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCPv6 Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Alternate TFTP	Indicates whether the phone is using the IPv6 Alternate TFTP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the IPv6 Alternate TFTP option and press the **Yes** softkey if the phone should use an alternate TFTP server. 3. Press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 TFTP Server 1 (SCCP phones only)	Primary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCPv6 in your network and you want to change this server, you must use the IPv6 TFTP Server 1 option. If you set the IPv6 Alternate TFTP option to yes or you disable DHCPv6, you must enter a non-zero value for the IPv6 TFTP Server 1 option. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Manually assigned IPv6 TFTP Servers • Manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. If DHCPv6 is enabled, set the IPv6 Alternate TFTP option to **Yes**. 3. Scroll to the IPv6 TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 TFTP Server 2 (for SCCP phones only)	Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Manually assigned IPv6 TFTP Servers • Manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the IPv6 TFTP Server 1 option. 4. Scroll to the IPv6 TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey.
Settings > Device Configuration > Network Configuration Menu		
IP Addressing Mode	Displays whether the IP addressing mode that is available on the phone—IPv4 only, IPv6 only, or Both (IPv4 and IPv6).	Display only—Cannot configure.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IP Preference Mode Control	Indicates the IP address version that the phone uses during signaling with Cisco Unified Communications Manager when both IPv4 and IPv6 are both available on the phone. The IP addressing mode preference is configured on Cisco Unified Communications Manager Administration.	Display only—Cannot configure. Displays one of the following options: • IPv4—The dual-stack phone prefers to establish a connection via an IPv4 address during a signaling event • IPv6—The dual-stack phone prefers to establish a connection via an IPv6 address during a signaling event.
Auto IP Configuration	Displays whether the auto configurations is enabled or disabled on the phone. The Auto IP Configuration setting along with the DHCPv6 setting determine how the IP Phone obtains its IPv6 address and other network settings. For more information on how these two settings affect the network settings on the phone, see Table 14 (Determining Where a Phone Acquires its Network Settings). **Note** To see the Auto IP Configuration on the phone, configure the Allow Auto-Configuration for Phones setting in Cisco Unified Communications Manager Administration.	Display only—Cannot configure.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Load Server	Used to optimize installation time for phone firmware upgrades and off load the WAN by storing images locally, negating the need to traverse the WAN link for each phone's upgrade. You can set the Load Server to another TFTP server IP address or name (other than the IPv6 TFTP Server 1 or IPv6 TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use IPv6 TFTP Server 1 or IPv6 TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion. **Note** When you configure both an IPv6 Load Server and a Load Server (for IPv4), the IPv6 Load server takes precedence.	Display only—Cannot configure.
IPv6 Log Server	Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help in debugging the peer to peer image distribution feature. **Note** The remote logging setting does not affect the sharing log messages sent to the phone log.	Display only—Cannot configure.
Settings > Security Configuration Menu		
CAPF Server	Displays the IP address and the port of the IPv4 CAPF server that the phone uses.	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.

Table 15 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 CAPF Server	Displays the IP address and the port of the IPv6 CAPF server that the phone uses.This menu setting is disabled in this release. If your configuration includes both IPv6 CAPF Server and IPv4 CAPF server, the phone will look for its CAPF server in the following order: • IPv6 CAPF Server • IPv4 CAPF Server	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.
Settings > Status > Network Statistics		
IPv6		Displays information on the DHCPv6 status.

For More Information

- *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1*
- *Cisco IOS IPv6 Configuration Library*
- *Implementing VoIP for IPv6*
- "Internet Protocol Version (IPv6)" chapter, *Cisco Unified Communications Manager Features and Services Guide*
- Updates for the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager (SCCP and SIP), page 156 (documentation updates)

Licensing Enhancements

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3) identify the state of a license; that is, if it is missing, if it is a demo license, or if it is an uploaded license. In addition, Cisco Unified Communications Manager Administration warns you whether Cisco Unified Communications Manager currently operates with demo licenses, with an insufficient number of licenses, or with an incorrect software feature license.

Cisco Unified Communications Manager Administration Configuration Tips

For information on how to configure licensing, refer to the licensing chapters in the *Cisco Unified Communications Manager Administration Guide* and *Cisco Unified Communications Manager Security Guide*.

GUI Changes

The following windows display the state of licenses in Cisco Unified Communications Manager Administration:

- Main Window—After you log in to Cisco Unified Communications Manager Administration, messages may display that indicate the current state of licenses for Cisco Unified Communications Manager. For example, Cisco Unified Communications Manager may identify the following situations:
  - Cisco Unified Communications Manager currently operates with demo licenses, so upload the appropriate license files.
  - Cisco Unified Communications Manager currently operates with an insufficient number of licenses, so upload additional license files.
  - Cisco Unified Communications Manager does not currently use the correct software feature license. In this case, the Cisco CallManager service stops and does not start until you upload the appropriate software version license and restart the Cisco CallManager service.
- License File Upload (System > Licensing > License File Upload)—This window displays a message that uploading the license file removes the demo licenses for the feature.
- License Unit Report (System > Licensing > License Unit Report)—This window displays the status of a license file. For example, the Status column for each license type may display Demo, Missing, or Uploaded.

Service Parameter and Enterprise Parameter Changes

No service parameters or enterprise parameters considerations exist for these licensing enhancements.

Installation/Upgrade (Migration) Considerations

After you upgrade to Cisco Unified Communications Manager 7.1(1) from a compatible Cisco Unified CM 5.X or 6.X release, the Cisco CallManager service does not automatically run, even though Cisco Unified Serviceability shows that the Cisco CallManager service is activated.

Immediately after you complete the upgrade to Cisco Unified Communications Manager 7.1(1), upload the software feature license that is required for Cisco Unified Communications Manager 7.1(1) in Cisco Unified Communications Manager Administration and restart the Cisco CallManager service in Cisco Unified Serviceability. Until you perform these tasks, devices fail to register with Cisco Unified Communications Manager 7.1(1).

Serviceability Considerations

After you upload a license file, you must restart the Cisco CallManager service for the changes to take effect.

BAT Considerations

No BAT considerations exist for these licensing enhancements.

CAR/CDR Considerations

No CAR or CDR considerations exist for these licensing enhancements.

Security Considerations

No security considerations exist for these licensing enhancements.

AXL and CTI Considerations

No AXL or CTI considerations exist for these licensing enhancements.

User Tips

This feature does not impact the end user.

For More Information

- Licensing chapter, *Cisco Unified Communications Manager System Guide*

Location-Based Call Admission Control Over Intercluster Trunk

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

When a call is made across cluster through an intercluster trunk (ICT) and gets hairpinned back to the same location or site of the same cluster, although the media is exchanged between two endpoints in the same site or location, the current design of Cisco Unified Communications Manager location call admission control (CAC) deducts location bandwidth twice, once for the outbound call and again for the inbound call. The result does not correctly reflect the bandwidth consumption, which eventually causes denial of a new call to or from the site or location.

In order to resolve the bandwidth calculation problem, this feature enables Cisco Unified Communications Manager to pass location information, the primary key ID (PKID) of location record and location name, as a proprietary information element (IE) between the calling and called parties through an ICT, either in the H.323 or SIP protocol. Thus, either endpoint knows the true location information of the party/endpoint, not the location information of the ICT.

Currently Cisco Unified Communications Manager has Hub_None as the default location that has unlimited bandwidth, plus any user-created location to which the user can assign a device and for which the user can configure bandwidth.

A new type of Cisco Unified Communications Manager location gets created specifically for the ICT for this type application. This new type of location, designated as the Phantom location, also has unlimited bandwidth. The locations server does not deduct bandwidth for a device that is assigned to the Phantom location. A device, such as the ICT, that is assigned to the Phantom location can use its own location or the true location of the connected device. Likewise, the outbound ICT can use its own location or the callee location, and the inbound ICT can use its own location or the caller location to deduct or adjust the bandwidth.

When the media connects, Cisco Unified Communications Manager adjusts the allocated location bandwidth according to the negotiated media codec. Cisco Unified Communications Manager can correctly readjust the location bandwidth based on received callee location information for the outbound call. This enhancement helps the outbound call, which has reserved bandwidth during call setup time, to adjust the bandwidth back to 0 if the call is hairpinned back to the same site or location.

Some supplementary services, such as transfer, can also hairpin the call back to the same site or location after the initial call setup process. Passing the location information of the final destination through the Notify signals (H.323) and re-INVITE signals (SIP) back to the calling cluster so that bandwidth can be adjusted to the right value is also required.

Because location record PKID is uniquely defined within the Cisco Unified Communications Manager enterprise environment, Cisco Unified Communications Manager uses location record PKID to identify whether the call over ICT has been looped back to the same cluster for the location-based CAC purpose. If other applications, like Cisco Voice Proxy (CVP), that do not have access to the Cisco Unified Communications Manager database for location record PKID information and also because PKID is a string of characters and digits, applications may need to rely on the location name information being

passed around for the purpose of CAC. The same location name may exist for different locations with different location PKIDs in two different Cisco Unified Communications Manager clusters, which may cause confusion to the applications.

Cisco Unified Communications Manager Administration Configuration Tips

The Location Configuration window specifies the Phantom location as a location, besides the Hub_None location, that can be selected. Administrators cannot delete the Phantom location.

Administrators can create a new default location page for the new Phantom location, similar to the Hub_None location. The Phantom location has unlimited audio and video bandwidth value and the administrator cannot modify the audio and video bandwidth values. The user can assign a location-pair RSVP policy between this new location and other existing locations.

Tip If the intercluster trunk or H.323 gateways gets configured in any other location besides the Phantom location, this feature does not work. In addition, if the intercluster trunk is connected to a third-party system that does not recognize and pass the Cisco-specific location information in the SIP or H.323 signals, this feature does not work.

GUI Changes

This feature does not entail any new menu options or new fields in Cisco Unified Communications Manager Administration. The Phantom value is added for all entities that specify a location in the Location drop-down list box. The Location field is found on the Device Pool Configuration, Annunciator Configuration, Music On Hold (MOH) Server Configuration, Conference Bridge Configuration, Voice Mail Port Configuration, Voice Mail Port Wizard Configuration, CTI Route Point Configuration, Gateway Configuration, Phone Configuration, Trunk Configuration, Pilot Point Configuration windows.

Service Parameter and Enterprise Parameter Changes

No service parameter nor enterprise parameter changes apply to this feature.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager maintains the RSVP policy for the Phantom location during migration.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR nor CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL nor CTI considerations exist for this feature.

User Tips

This feature does not entail user interaction.

For More Information

- Call Admission Control, *Cisco Unified Communications Manager System Guide*
- Resource Reservation Protocol, *Cisco Unified Communications Manager System Guide*
- Understanding Cisco Unified Communications Manager Trunk Types, *Cisco Unified Communications Manager System Guide*
- Location Configuration, *Cisco Unified Communications Manager Administration Guide*

Logging Missed Calls For Shared Lines

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

With the missed call logging for shared lines feature, the administrator can configure Cisco Unified Communications Manager Administration or the phone user can configure Cisco Unified CM User Options, so Cisco Unified Communications Manager logs missed calls in the call history to a specified shared line appearance on a phone.

Tip If configured correctly, this feature works if a phone user logs in to a phone via Cisco Extension Mobility.

The examples in Table 16, which use the following phones, describe how the missed call logging feature works for shared lines:

- Phone A, which has directory number 1000 configured for the first line and directory number 2000 for the second line, which is shared with phone B.
- Phone B, which has directory number 2000 configured as the first line, which is shared with phone A, and directory number 3000 configured as the second line.
- Phone C, which places the calls.

Table 16 Example of How Logging Works for Missed Calls With Shared Lines

Phone A	Phone B
• Phone C calls directory number (DN) 1000. • The Logged Missed Calls check box is checked for DN 1000. • Missed calls get logged to DN 1000. If the Logged Missed Calls check box is not checked, missed calls are not logged to DN 1000.	Not applicable
• Phone C calls directory number (DN) 2000. • The Logged Missed Calls check box is checked for DN 2000. • Missed calls get logged to DN 2000. If the Logged Missed Calls check box is not checked, missed calls are not logged to DN 2000.	• Phone C calls DN 2000, which is a shared line appearance. • Logging displays for the shared line appearance on Phone B because the Logged Missed Calls check box is checked for DN 2000.

Cisco Unified Communications Manager Administration Configuration Tips

If this feature is not configured, the call history on the phone does not display missed calls for the specified line appearance.

GUI Changes

If the phone supports this feature, the Directory Number Configuration window in Cisco Unified Communications Manager Administration displays the Log Missed Calls check box, which allows you turn on or off this feature. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone. To access the Directory Number Configuration window, choose **Call Routing > Directory Number**.

The Directory Number Configuration window in Cisco Unified Communications Manager Administration displays the Logged Missed Calls check box, which turns on or off this feature. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone. To access the check box, choose **Call Routing > Directory Number**. In the Directory Number Configuration window, highlight the associated device in the Associated Devices pane; then, click the **Edit Line Appearance** button.

In the Line Settings Configuration window in the Cisco Unified CM User Options, the phone user can check and uncheck the Log Missed Calls check box.

Service Parameter and Enterprise Parameter Changes

No new or updated parameters exist for this feature.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(1) or upgrade to 7.1(1), you can configure this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

The Bulk Administration GUI has the following updates to support the Log Missed Calls feature:

- Log Missed Calls Check Box— This check box allows you to turn this feature on or off. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone.

Note The Log Missed Calls Check Box is present on the Phone Line Template, UDP Line Template, Phone Update Line, and UDP Update Line pages.

- Insert, Export, and Validate Details support for the log missed calls feature—the following insert, export, and validate details features have support for the log missed calls feature:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
- File Formats—the following file formats support the Log Missed Calls feature:
  - Phone File Format—Log Missed Calls field is a part of the Line Fields section.
  - UDP File Format—Log Missed Calls field is a part of the Line Fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration page lists the Log Missed Calls field in the Line Fields section.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

Tip If configured correctly, this feature works when a Cisco Extension Mobility user logs in to a phone via Cisco Extension Mobility.

For a list of phone models that support this feature, see the "Missed Calls" section on page 145.

For More Information

- Missed Calls, page 145

Logical Partitioning

Description

Regulations of the Telecom Regulatory Authority of India (TRAI) require that voice traffic over the enterprise data network and the Public Switched Telephone Network (PSTN) must be strictly separated and no mixing of calls between the two networks can occur for the purpose of toll bypass.

Originally, Indian regulations required that Voice over IP (VoIP) systems be physically separate from PSTN interconnect systems. Users used phones on a VoIP system strictly for interoffice phone calls, but any calls that needed to go to or come from the PSTN had to be made using the PSTN system. Recent changes to the law permit a single system to support both types of calls, as long as the system can be configured so that forbidden calls cannot complete. In a Cisco Unified Communications Manager system, the term *logical partitioning* specifies this capability.

The following basic scenarios are restricted (that is, not allowed):

- The call that passes through a PSTN gateway must never connect directly using WAN to a VoIP phone or VoIP PSTN gateway in a different geographic location.
- If PSTN gateway is located in India, this is strictly restricted. If the PSTN is in another country and a VoIP phone is in India and if connection results in revenue loss to Indian telecom service providers, the connection is considered restricted.

The following are basic scenarios are permitted:

- Call directly between two VoIP phones in different geographic locations
- Call from a VoIP phone to a PSTN gateway in the same geographic location

The current Enterprise VoIP implementations that use Cisco Unified Communications Manager in India use the same Cisco Unified IP Phone for both the VoIP and PSTN connectivity. Cisco Unified Communications Manager does not support specific configurations for controlling the mixing of VoIP and PSTN traffic when supplementary features are invoked from a single line with participants in VoIP or PSTN domains.

To comply with regulations, previous VoIP implementations in India used separate lines on VoIP phones for PSTN and VoIP calls.

Cisco Unified Communications Manager uses the concept of partitions and calling search spaces (CSS) for configuration of the respective lines. Thus, control is separate for the VoIP and PSTN domains and features like Transfer from a single line are not available, because invoking such features could result in joining the VoIP with the PSTN network.

With this limitation, enterprise VoIP deployments in India that use Cisco equipment are limited to using phones with minimum of two lines, which is not a cost-effective solution for most customers. This limitation also prevents solutions that use low-cost analog phones that are single-line by design and use VG224/VG248 gateways.

To overcome the limitations, a Cisco Unified Communications Manager solution allows logical partitioning of a single line on Cisco Unified IP Phones through administrator policies. Control of call joining or call redirection is required, based on an attribute tag or the geolocation of the parties.

The Logical Partitioning feature specifies the capability of a telephony system to control calls and features based on specific allowed or forbidden configurations. The common telephony system can provide access to Voice over Internet Protocol (VoIP) and Public Switched Telephone Network (PSTN) networks, and configuration can control access.

A calls that passes through a PSTN gateway must never connect directly to a VoIP phone or VoIP PSTN gateway in a different site or geographic location (geolocation) through use of IP telephony.

Internally, the device layer of Cisco Unified Communications Manager associates with a geolocation values that call processing uses. No communication of geolocation from Cisco Unified Communications Manager to a phone takes place.

To support logical partitioning for participants that belong to different clusters, the following support, which is termed *location conveyance*, is required from SIP trunks and intercluster trunks (ICTs):

- The geolocation information and device type information must be sent from one cluster to another cluster.
- Geolocation and device type information is sent both at call establishment as well as during midcall joins and redirects.
- The geolocation filter is configured for the trunk. Such configuration allows construction of geolocation identifier values for logical partitioning policy checks.

The setting of the Send Geolocation Information check box on the configuration window of a SIP trunk or ICT determines whether the geolocation information gets sent across clusters for the trunk.

The location conveyance is independent of any logical partitioning configuration.

If a device has a configured geolocation, interactions of the device with a SIP trunk or ICT cause the geolocation information to be sent in call signaling across the trunk.

The SIP trunk supports the location conveyance of PIDF-LO as described in RFC 4119, which is an encapsulation of location information within a presence document.

- INVITE and UPDATE requests carry the PIDF-LO XML.
- Support exists for ASCII and Unicode characters in the geolocation fields.

ICTs also support location conveyance using PIDF-LO XML with reduction in some of the XML elements.

- Support exists for Setup, Alert, Progress, Connect Notify requests.
- Support exists for ASCII characters supported in the geolocation fields.

Cisco Unified Communications Manager Administration Configuration Tips

Table 17 displays the configuration checklist for logical partitioning, which is documented in the "Logical Partitioning" chapter in the *Cisco Unified Communications Manager Features and Services Guide*. Before you configure logical partitioning in your network, review Table 17.

Table 17 Logical Partitioning Configuration Checklist

Configuration Steps		Procedures and Related Topics
Step 1	Define a set of geolocations on a new Geolocation Configuration window.	Geolocation Configuration, *Cisco Unified Communications Manager Features and Services Guide*
Step 2	Assign geolocations to device pools, devices, trunks, gateways, or MGCP ports.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Phone Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*
Step 3	Assign geolocations to a default geolocation as determined by the geolocation-related enterprise parameter.	Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*
Step 4	Determine the policy for devices for which no geolocation is configured.	
Step 5	Determine the policy for devices for which the Unspecified geolocation is configured.	
Step 6	Define a filter rule for geolocation string creation through an enterprise parameter.	Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*
Step 7	Define a separator character for geolocation string creation through an enterprise parameter.	Enterprise Parameters Configuration, *Cisco Unified Communications Manager Administration Guide*
Step 8	Define a filter rule for geolocation string creation on a device pool, trunk, intercluster trunk, H.323 gateway, or MGCP port.	Device Pool Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Gateway Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Phone Configuration Settings, *Cisco Unified Communications Manager Administration Guide* Trunk Configuration Settings, *Cisco Unified Communications Manager Administration Guide*

The Logical Partitioning solution comprises provisioning the following elements:

- Identifiers—Develop a framework to associate a unique identifier with every device.
- Policies—Allow administrator the ability to define rules or policies that determine the interconnection between any two devices (a VoIP phone and a gateway) in the Cisco Unified Communications Manager system.
- Checking Policies—Call processing and features such as transfer, pickup, ad hoc conference check the defined policies before allowing the calls or features between participants.

Cisco Unified Communications Manager administrators must define the following:

- A geolocation for every device that uses logical partitioning. Geolocations are based on the RFC 4119 standard. Geolocations use the civic location format that specifies the following fields: country, A1, A2, A3, A4, A5, A6, PRD, POD, STS, HNO, HNS, LMK, LOC, FLR, NAM, and PC. Geolocations get configured manually.
- A geolocation filter for every device. Filters allow selection of specific fields from the 17 geolocation fields for the purpose of creating an identifier from the selected fields. Geolocation filters get configured manually.

Cisco Unified Communications Manager administrators then assign geolocation values to devices.

The standard record for a geolocation specifies *Unspecified*. Use this value when no geolocation needs to associate with a device. If the geolocation of a device is unspecified, no identifier gets created and the device does not participate in logical partitioning policy checks.

The Default Geolocation service parameter can be configured with a geolocation value.

The following entities in a Cisco Unified Communications Manager cluster can have geolocation values assigned:

- Device pools
- CTI route points
- Phones (optional)
- SIP trunks
- Intercluster trunks (ICT)
- H.323 gateways
- MGCP ports of the following types: T1, E1, PRI, FXO

Media devices, such as media termination points (MTP), conference bridges (CFB), annunciators, and music on hold (MOH) servers, do not need to associate with geolocation values.

Beyond the configuration of geolocations, geolocation filters, and logical partitioning policies, logical partitioning requires special configuration when an allowed call changes due to the following features:

- Call forwarding
- Call transfer
- Ad hoc conference, Join, JAL
- Meet-me conference
- Call Pickup
- Park
- Directed Call Park
- Cisco Extension Mobility

- Mobile Connect
- Shared line, Barge, cBarge, Remote Resume
- Redirection (3xx)
- All features that perform Join (SsJoinReq primitive) or Redirects (SsRedirectCallReq primitive)

The following restrictions apply to logical partitioning:

- SIP Trunk UAS location conveyance in UPDATE

  The UAS uses UPDATE request to communicate geolocation of the called party to the UAC. This normally happens after 180 Ringing.

  The LP Policy checks in LP-aware cluster that receives this geolocation may CANCEL the call if policy is denied. The end user experience may not be convenient.

- The LP checks are not supported for participants across conferences in Conference chaining.

  For example, meet-me and ad hoc chained conferences can have participants that are LP denied.

- Limitation with QSIG intercluster trunk (ICT)

  The ICT with Q.SIG protocol is not allowed to communicate geolocation info for the caller or callee device. The ICT configuration for “Send Geolocation Information” gets disabled when the Q.SIG tunneled protocol gets selected.

- Shared Line Active Call Info

  For LP restricted scenario, the shared line drops the active call information for the duration of the call, even if some feature moves the shared line call to allowed.

- cBarge/Barge

  The Barge/cBarge are prevented by not allowing shared lines to attempt these features based on LP deny policy with the connected party (the call instance gets dropped).

  When the connected party invokes a feature like Conference or Meet-Me, the shared line shows call instance info and cBarge/Barge feature-based LP policy checking does not get performed.

- CUCM shall not communicate geolocation info to H.323 or MGCP gateway.

  Communication to a SIP gateway can be disabled from a SIP trunk check box.

- Scenario: Cisco Unified Communications Manager 1 is LP enabled but Cisco Unified Communications Manager 2 is LP disabled.

  Phone A on CCM1 calls Phone B on CCM2 (using ICT or SIP Trunk).

  Phone B presses conference and invites PSTN to conference.

  Limitation: The conference gets established.

  Once phone B goes on hook, the call between phone A and the PSTN on Cisco Unified Communications Manager 2 gets cleared with a reorder tone.

- Mobility Cell Pickup: LP Deny handling after call gets answered on the mobile phone.

  The LP policy check does not happen before the call gets placed to the mobile phone (as it happens for a basic SNR call). The current design checks LP policy only after SsJoinReq processing, which takes place after the mobile phone answers the call.

- Cisco Extension Mobility login to a phone in a different geolocation

  Outgoing PSTN calls are possible when Local Route Groups are configured.

  Incoming PSTN calls are not placed to the phone, but are given a reorder tone.

- BLF SD or BLF Pickup Presence notifications are not checked for LP policy.

Currently no LP infrastructure gets added for notifications.

GUI Changes

Use the following new menu options in Cisco Unified Communications Manager Administration to configure the logical partitioning feature:

- System > Geolocation Configuration
- System > Geolocation Filter
- Call Routing > Logical Partitioning Policy

The following existing Cisco Unified Communications Manager Administration windows contain new fields for configuring logical partitioning:

- Device Pool Configuration—pane: Geolocation Configuration, fields: Geolocation, Geolocation Filter
- CTI Route Point Configuration—field: Geolocation
- Gateway Configuration—pane: Geolocation Configuration; fields: Geolocation, Geolocation Filter
- Cisco Unified IP Phone Configuration— field: Geolocation
- Trunk Configuration—pane: Geolocation Configuration, fields: Geolocation, Geolocation Filter, Send Geolocation Information

Service Parameter and Enterprise Parameter Changes

The following new enterprise parameters affect the configuration of the logical partitioning feature:

- Enable Logical Partitioning
- Default Geolocation
- Logical Partitioning Default Policy
- Logical Partitioning Default Filter

Installation/Upgrade (Migration) Considerations

The following migration considerations that affect the dial plan exist for the logical partitioning feature when migrating from releases of Cisco Unified Communications Manager earlier than Release 7.1(1):

- If the Enable Logical Partitioning enterprise parameter is set to *True*, geolocations and geolocation filters must be configured for the following entities:
  - Device pools for all phones
  - MGCP ports that access the PSTN
  - H.323 gateways that access the PSTN
  - Intercluster trunks (ICTs, either gatekeeper-controlled or non-gatekeeper-controlled) to remote clusters
  - SIP trunks that access the PSTN or remote clusters
- The location conveyance must be turned on in all clusters to allow end-to-end communication of geolocation information.

  To do so, check the Send Geolocation check box on intercluster trunks (ICTs) and SIP trunks.
- Logical partitioning policies must be configured for all entities for which geolocations and geolocation filters are configured.

Serviceability Considerations

The following consideration exists for the logical partitioning feature:

- The Cisco Call Restriction counters specify a new group of performance monitoring counters that log the number of failures that result because of logical partitioning policy restrictions. The Cisco Call Restriction counters include the following performance monitoring counters:
  - AdHocConferenceFailures
  - BasicCallFailures
  - ForwardingFailures
  - LogicalPartitionFailuresTotal
  - MeetMeConferenceFailures
  - MidCallFailures
  - ParkRetrievalFailures
  - PickUpFailures
  - SharedLineFailures
  - TransferFailures

  See the "Performance Objects and Counters for Cisco Unified Communications Manager" appendix of the *Real-Time Monitoring Tool Administration Guide* for details.

BAT Considerations

The Cisco Bulk Administration Tool specifies several new menu items to support logical partitioning. See the "Support for Logical Partitioning" section on page 113 for details.

CAR/CDR Considerations

The following CAR and CDR considerations exist for the logical partitioning feature:

- To support the logical partitioning feature, call termination cause codes are added. See the "Cisco Call Detail Records Codes" chapter of the *Cisco Unified Communications Manager Call Detail Records Administration Guide* for details.
- The "CDR Examples" chapter of the *Cisco Unified Communications Manager Call Detail Records Administration Guide* provides examples of CDRs that are added to support the logical partitioning feature.

Security Considerations

No security considerations exist for the logical partitioning feature.

AXL and CTI Considerations

AXL supports all geolocation-related database changes in Cisco Unified Communications Manager. The AXL SOAP interface is modified to accommodate all new configuration that the logical partitioning feature requires.

The following CTI considerations exist for the logical partitioning feature:

- CTI handles the new error tags that the logical partitioning feature reports and maps those tags to new CTI error codes.
- When the logical partitioning policy failures result in clearing of the calls, CTI handles the new cause code sent from Unified CM, CCM_SIP_503_SERVICE_UNAVAIL_SER_OPTION_NOAVAIL, maps it to the CTI cause code, CtiCcmSip503ServiceNotavailable, and sends it to the application. No new cause code gets added to support the logical partitioning feature.

- For logical partitioning policy failures, the call control sends an SsRedirectCallErr message with a new error code, REDIRECT_CALL_PARTITIONING_POLICY. CTI adds a corresponding CTI error code for these SsRedirectCallErr messages.

User Tips

No user tips exist for the logical partitioning feature.

For More Information

- Logical Partitioning, *Cisco Unified Communications Manager Features and Services Guide*
- Device Pool Configuration, *Cisco Unified Communications Manager Administration Guide*
- CTI Route Point Configuration, *Cisco Unified Communications Manager Administration Guide*
- Cisco Unified IP Phone Configuration, *Cisco Unified Communications Manager Administration Guide*
- Trunk Configuration, *Cisco Unified Communications Manager Administration Guide*
- Gateway Configuration, *Cisco Unified Communications Manager Administration Guide*
- Performance Objects and Counters for Cisco Unified Communications Manager, *Real-Time Monitoring Tool Administration Guide*
- Cisco Call Details Records Codes, *Cisco Unified Communications Manager Call Detail Records Administration Guide*
- CDR Examples, *Cisco Unified Communications Manager Call Detail Records Administration Guide*

Multicast Music On Hold Over H.323 Intercluster Trunks

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

The Multicast Music on Hold (MOH) over H.323 Trunk feature allows multicast MOH to work over H.323 intercluster trunks (ICTs). Prior to the implementation of this feature, multicast MOH used bandwidth for each unicast MOH over the same ICT, which wasted bandwidth.

Prior to the implementation of this feature in 6.1(3) and 7.1(1), the H.323 Open Logical Channel (OLC) ACK message carried the IP address and port for multicast MOH. With the implementation of this feature, the H.323 OLC message now carries the IP address and port for multicast MOH, and Cisco Unified Communications Manager adds the mechanism to handle the information in the H.323 OLC message.

The new service parameter, Send Multicast MOH in H.245 OLC Message, controls the Multicast Music On Hold Over H.323 Intercluster Trunk feature. Both Cisco Unified Communications Manager nodes that are involved in the call must support single-transmitter multicast for the setting of this parameter to have any effect. This service parameter affects only the side of the party that places the call on hold and does not affect how the far end carries the multicast transport address. Even if this parameter is turned off, multicast MOH applies for the held-party side of the call as long as the held party has the capability to support single-transmitter multicast.

When a call connects over an intercluster trunk and one of the parties presses the Hold key, MOH will stream over the intercluster trunk. If multicast MOH is turned on and the holding party and trunk are configured to use the multicast MOH server, MOH streams with multicast. Only one multicast MOH stream streams over the trunk no matter how many calls are put on hold on this trunk.

Cisco Unified Communications Manager Administration Configuration Tips

Calls that connect over Cisco Unified Communications Manager intercluster trunks use this feature for multicast MOH. This feature does not work if any middle box between Cisco Unified Communications Managers does not pass the new fields in Terminal Capability Set (TCS) and OLC message.

No additional configuration exists for this new feature in addition to the normal configuration for setting up multicast MOH. This new feature only applies between Cisco Unified Communications Managers that support single-transmitter multicast.

You can turn this feature off by changing the default True value of the new Send Multicast MOH in H.245 OLC Message service parameter to False. You may need to do so if an interoperability issue arises.

GUI Changes

This feature does not entail any GUI changes to Cisco Unified Communications Manager Administration.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature via the clusterwide service parameter, Send Multicast MOH in H.245 OLC Message, which supports the Cisco CallManager service, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration. Then, choose the server and the Cisco CallManager service. From the Send Multicast OH in H.245 OLC Message drop-down list box, choose **True**.

The new feature is active by default. To turn off the feature, set the value of the Send Multicast MOH in H.245 OLC Message service parameter to **False**. Do so to resolve interoperability issues that the feature may cause.

The new service parameter governs the multicast MOH behavior on H.323 trunks and devices. The new service parameter does not control multicast MOH over SIP trunks, because multicast MOH over SIP trunks does not constitute a new behavior.

Installation/Upgrade (Migration) Considerations

No installation nor upgrade considerations exist for this feature. You may, however, turn off the feature if interoperability issues arise as a result of the feature. To do so, set the value of the Send Multicast MOH in H.245 OLC Message service parameter to **False**.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR nor CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL considerations exist for this feature.

CTI-controlled phones work as before for multicast MOH. CTI-controlled applications such as CTI ports and CTI route points do not perform multicast MOH, which is the same behavior as prior to the implementation of this feature.

User Tips

When multicast MOH gets turned on in Cisco Unified Communications Manager Administration, phone users hear MOH if the call connects through an intercluster trunk.

For More Information

- Music on Hold, *Cisco Unified Communications Manager Features and Services Guide*

Off-Hook Abbreviated Dial

Description

Cisco Unified Communications Manager release 7.1 introduces an enhancement to the existing Abbreviated Dial feature to allow Abbreviated Dialing while off-hook. The user can initiate Off-Hook Abbreviated Dialing while placing a basic call, while conferencing a call, while transferring a call, or while a call is on hold.

To enable Off-Hook Abbreviated Dialing, assign the softkey Abbreviated Dial (AbbrDial) to a softkey template, and assign the template to the IP Phone. The Abbreviated Dial (AbbrDial) softkey can be included in the Off Hook, Off Hook With Feature, or Digits After First states of a Softkey Layout Configuration.

Cisco Unified Communications Manager Administration Configuration Tips

Step 1 Find the softkey template:

a. Choose **Device > Device Settings > Softkey Template.**

The Find and List Softkey Templates window displays. Records from an active (prior) query may also display in the window.

b. To find all records in the database, ensure the dialog box is empty; go to step c.

To filter or search records

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.
- From the third drop-down list box, select whether to search for standard, non-standard, or both types of softkey templates.

c. Click **Find**.

All matching records display.

Step 2 Add the Abbreviated Dial (AbbrDial) softkey to the off-hook call states:

a. From the list of matching records, choose the softkey template in which you want to configure softkey positions. The Softkey Template Configuration window displays.

Note You can modify only softkey templates that display a check box in the left column. All other softkey templates are standard, read-only templates.

b. Choose **Configure Softkey Layout** from the Related Links drop-down list box; then, click **Go**.

The Softkey Layout Configuration window displays. The Select a call state to configure drop-down list box lists each Cisco Unified Communications Manager call state for an IP phone.

c. Change the off-hook call states to include the Abbreviated Dial (AbbrDial) softkey. The off-hook call states include Off Hook, Off Hook With Feature, and Digits After First. You must add the Abbreviated Dial (AbbrDial) softkey to each of these call states.

- From the Select a call state to configure drop-down list box, select Off-hook. The Softkey Layout Configuration window redisplays, and the Unselected Softkeys pane and Selected Softkeys pane display the softkeys that are applicable to the call state.
- Move the Abbreviated Dial (AbbrDial) softkey to the Selected Softkeys list using the arrows between the panes.
- To rearrange the positions of the Selected Softkeys, use the up and down arrows to the right of the Selected Softkeys pane.
- Click **Save** to save your softkey layout configuration.
- Repeat these steps for the call states Off Hook With Feature and Digits After First. You must add the Abbreviated Dial (AbbrDial) softkey to all three off-hook call states include Off Hook, Off Hook With Feature, and Digits After First.

d. To return to the Softkey Template Configuration window, choose the Softkey Template Configuration link from the Related Links drop-down list box in the top, right-hand corner; then, click **Go**.

e. To save your configuration, click **Save**.

f. To make the updates of the softkey template take effect on the phone, click **Reset**. To assign a template to a phone, see "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide.*

GUI Changes

No GUI changes were made to support this feature.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes were made to support this feature.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager 7.1(1) introduces this feature. After you install or upgrade to 7.1(1), you can configure this feature.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that you activated the Cisco CallManager service in the Service Activation window in Cisco Unified Serviceability.

BAT Considerations

The Bulk Administration Tool (BAT) supports the import and export of the AbbrDial softkey configuration.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security consideration exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For information on user tips and phone support for this feature, see "Off-Hook Abbreviated Dialing" section on page 146.

For More Information

- "Softkey Template Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phones," *Cisco Unified Communications Manager System Guide*

Party Entrance Tone

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

Tip To configure the party entrance tone in previous releases of Cisco Unified Communications Manager (except for 6.1(3)), you configured the party entrance tone service parameter for the Cisco CallManager service, which applied to the entire cluster. In Cisco Unified Communications Manager 7.1(1) and 6.1(3), you can configure the party entrance tone for directory numbers on a phone.

With the party entrance tone feature, a tone plays on the phone when a basic call changes to a multi-party call; that is, when a basic call changes to a barged call, cBarged call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call.

If the controlling device, that is, the originator of the multi-party call has a built-in bridge, the tone gets played to all parties if you configured party tone entrance for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.

When a joined call or ad hoc conference begins, Cisco Unified Communications Manager uses the party entrance tone configuration from the conference controller. Cisco Unified Communications Manager uses this configuration until the conference ends.

If two ad hoc conferences are chained together and the controlling device for one conference has the party entrance tone set to True while the other controlling device for the other conference has a party entrance tone of False, Cisco Unified Communications Manager determines whether to plan the tone based on which conference the new party is added.

When a barge call gets created, the party entrance tone configuration of the barge target that shares the line with the barge initiator determines whether Cisco Unified Communications Manager plays the party entrance tone.

When a cBarge call gets created, the party entrance tone configuration of the cBarge target that shares the line with the cBarge initiator determines whether Cisco Unified Communications Manager plays the party entrance tone. However, if the call for the target is an existing ad hoc conference that is in the same cluster, the party entrance tone configuration for the ad hoc conference controller determines whether Cisco Unified Communications Manager plays the tone.

When a meet-me conference gets created, the party entrance tone configuration for the first party to enter the conference determines whether Cisco Unified Communications Manager plays the tone. Cisco Unified Communications Manager uses the configuration for the first party until the conference ends.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

To use the party entrance feature, ensure that you turned the privacy feature off for the devices and ensure that the controlling device for the multi-party call has a built-in bridge.

To configure the party entrance tone for a specific directory number, choose **Call Routing > Directory Number** in Cisco Unified Communications Manager Administration. From the Party Entrance Tone drop-down list box, choose one of the following options:

- **Default**—Use the value that you configured in the Party Entrance Tone service parameter.
- **On**—A tone plays on the phone when a basic call changes to a multi-party call; that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call. If the controlling device, that is, the originator of the multi-party call has a built-in bridge, the tone gets played to all parties if you choose On for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.
- **Off**—A tone does not play on the phone when a basic call changes to a multi-party call.

Service Parameter and Enterprise Parameter Changes

If you want to configure this feature for the entire cluster instead of per line, configure the Party Entrance Tone service parameter, which supports the Cisco CallManager service. To access this parameter, choose **System > Service Parameters** in Cisco Unified Communications Manager Administration; choose the server and the **Cisco CallManager** service. When the parameters display, locate the Party Entrance Tone service parameter. For more information on this parameter, click the name of the service parameter or the question-mark button in the Service Parameter Configuration window.

Installation/Upgrade (Migration) Considerations

Cisco Unified Communications Manager 7.1(1) introduces this feature.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that the service is activated in Cisco Unified Serviceability.

BAT Considerations

The Bulk Administration GUI has the following updates to support the party entrance tone feature:

- Party Entrance Tone drop-down list box—choose one of the following options:
  - **Default**—Use the value that you configured in the Party Entrance Tone service parameter.
  - **On**—A tone plays on the phone when a basic call changes to a multi-party call; that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call. If the controlling device, that is, the originator of the multi-party call has a built-in bridge, the tone gets played to all parties if you choose On for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.
  - **Off**—A tone does not play on the phone when a basic call changes to a multi-party call.

Note The Party Entrance Tone drop-down list box is present on the Phone Line Template, UDP Line Template, UDP Update Line, RDP Line Template, Phone Update Line, and UDP Update Line pages.

- Insert, Export, and Validate Details support for party entrance tone—the following insert, export, and validate details features have support for the party entrance tone:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
  - Insert Gateways
  - Insert Remote Destination Profiles
  - Export Remote Destination Profiles
- File Formats—the following file formats support the party entrance tone feature:
  - Phone File Format—Party Entrance Tone field is a part of the Line Fields section.
  - UDP File Format—Party Entrance Tone field is a part of the Line Fields section.

– Remote Destination Profile File Format—Party Entrance Tone field is a part of the Line Fields section.

Note For more information on BAT, refer to the Bulk Administration Tool section of this document.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For information on the phones that support this feature, see the "Barge Tone Enhancements" section on page 127.

For More Information

- Barge Tone Enhancements, page 127

Phone Migration in Cisco Unified Communications Manager Administration

Description

The Phone Migration window in Cisco Unified Communications Manager Administration allows you to migrate feature, user, and line configuration for a phone to a different phone; that is, you can migrate data to a different phone model or to the same phone model that runs a different protocol. For example, you can migrate data from a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975; or, you can migrate data from a phone model that runs SCCP, for example, the Cisco Unified IP Phone 7965 (SCCP), and move it to the same phone model that runs SIP, for example, the Cisco Unified IP Phone 7965 (SIP).

Tip Phone migration allows you to port existing phone configuration to a new phone without needing to add a phone, lines, speed dials, and so on.

Cisco Unified Communications Manager Administration Configuration Tips

Before you can migrate phone configuration to a new phone, consider the following information:

- If the phone models do not support the same functionality, be aware that you may lose functionality on the new phone. Before you save the migration configuration in the Phone Migration window, Cisco Unified Communications Manager Administration displays a warning that you may lose feature functionality.
- Some phone models do not support phone migration; for example, CTI port, H.323 client, Cisco Unified Mobile Communicator, and Cisco IP Softphone.

- Before you can migrate the phone configuration in Cisco Unified Communications Manager Administration, you must create a phone template for the phone model to which you want to migrate in BAT (Bulk Administration > Phones > Phone Template). For example, if you want to migrate the configuration for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.
- The new phone uses the same PKID and existing phone record as the original phone, so migrating the phone configuration to the new phone removes the configuration for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database; that is, you cannot view or access the configuration for the original phone after the migration.

  Migrating to a phone that uses fewer speed dials or lines does not remove the speed dials or lines for the original phone from Cisco Unified Communications Manager Administration/the Cisco Unified Communications Manager database, although some of the speed dials/lines do not display on the new phone. After you migrate the configuration, you can see all speed dials and lines for the original phone in the Phone Configuration window for the new phone.
- Before you migrate the phone configuration to a new phone, ensure that the phones are unplugged from the network. After you perform the migration tasks, you can plug the new phone into the network.
- Before you migrate the phone configuration to a new phone, ensure that you have the appropriate device licenses for the new phone.

GUI Changes

Table 18 describes the configuration settings that display in the Phone Migration Configuration window.

Table 18 Phone Migration Configuration Settings

Field	Description
Phone Template	From the drop-down list box, choose the phone template for the phone model to which you want to migrate the phone configuration. Only the phone templates that you configured in the Phone Template window in Bulk Administration display (Bulk Administration > Phones > Phone Template).
MAC Address	Enter the Media Access Control (MAC) address that identifies Cisco Unified IP Phones (hardware phones only). Make sure that the value comprises 12 hexadecimal characters. For information on how to access the MAC address for your phone, refer to the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager that supports your phone model.
Description	If you want to do so, enter a description for the new phone.

Service Parameter and Enterprise Parameter Changes

No service or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No special installation or upgrade considerations exist for this feature. After you install or upgrade to Cisco Unified Communications Manager 7.1(1), you can use this feature.

Serviceability Considerations

No special serviceability considerations exist for this feature.

BAT Considerations

Before you can migrate the phone configuration in Cisco Unified Communications Manager Administration, you must create a phone template for the phone model to which you want to migrate in BAT (Bulk Administration > Phones > Phone Template). For example, if you want to migrate the configuration for a Cisco Unified IP Phone 7965 to a Cisco Unified IP Phone 7975, you create the phone template for the Cisco Unified IP Phone 7975.

If you want to migrate several phones at the same time, consider using BAT, as described in the "Phone Migration in BAT" section on page 112.

CAR/CDR Considerations

No CDR or CAR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

User Tips

No end user tips exist for this feature.

For More Information

- Phone Migration in BAT, page 112

QSIG Variant Configuration for a Gateway or Trunk

Description

The QSIG variant specifies how to encode the Invoke Object ID (OID) for remote operations service element (ROSE) operations, as well as how to code the protocol profile for out bound facility Information elements.

Cisco Unified Communications Manager release 7.1 introduces an enhancement to the existing QSIG variant feature to allow CCM administrators to configure QSIG variants for s specific trunk or gateway. In previous releases, the QSIG variant was configurable for cluster service configurations only.

Cisco Unified Communications Manager release 7.1 also introduces support using Annex M.1 to tunnel QSIG over intercluster trunks with the QSIG Variant ECMA.

Cisco Unified Communications Manager Administration Configuration Tips

To create Cisco Unified Communications Manager compatibility with your version of the QSIG protocol, configure the ASN.1 ROSE OID Encoding and QSIG Variant in the service parameters, for a gateway, or for a trunk.

Tip For more information on these parameters, click the **?** that displays in the upper corner of the Service Parameter window.

If you choose ECMA for the QSIG Variant parameter, you must choose the Use Global Value (ECMA) setting for the ASN.1 ROSE OID Encoding service parameter.

If you choose ISO for the QSIG Variant parameter, you normally choose the Use Local Value setting for the ASN.1 ROSE OID Encoding service parameter. You may need other configurations in unusual situations.

Tip To display the options in the QSIG Variant drop-down list box, choose QSIG from the Tunneled Protocol drop-down list box. Keep the QSIG Variant and ASN.1 ROSE OID Encoding parameters set to the default value unless a Cisco support engineer instructs otherwise.

Cisco Unified Communications Manager supports using Annex M.1 to tunnel QSIG over intercluster trunks. To configure Annex M.1, do one of the following:

- Set the ASN.1 ROSE OID Encoding to Use Local Value and the QSIG Variant to ISO (Protocol Profile 0x9F).
- Set the ASN.1 ROSE OID Encoding to Use Global Value (ECMA) and the QSIG Variant to ECMA.

Serviceability Considerations

This feature relies on the Cisco CallManager service, so make sure that you activated the Cisco CallManager service in the Service Activation window in Cisco Unified Serviceability.

BAT Considerations

The Bulk Administration Tool (BAT) supports the import and export of the QSIG variant configuration.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security consideration exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

End users are not impacted by this feature change.

For More Information

- "Gateway Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Trunk Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Service Parameters Configuration," *Cisco Unified Communications Manager Administration Guide.*
- "Understanding IP Telephony Protocols," *Cisco Unified Communications Manager System Guide*

Standard Audit Log Administration Role

The Standard Audit Log role allows you to configure the following Resource Access Information. For each item, you can choose Read access, Update access, or both.

- Alarm Configuration web page
- Alarm Definition web page

- Audit Configuration
- Audit Trace
- CDR Management
- Control Center - Feature Services web page
- Control Center - Network Services web page
- Log Partition Monitoring->Configuration web page
- RTMT->Alert Config
- RTMT->Profile Saving
- Real Time Monitoring Tool
- SNMP->V1/V2c->Configuration->Community String web page
- SNMP->V1/V2c->Configuration->Notification Destination web page
- SNMP->V3 Configuration->Notification Destination web page
- SNMP->V3 Configuration->User web page
- SNMP->system Group Configuration->MIB2 System Group Configuration web page
- SOAP Backup and Restore APIs
- SOAP CDR on Demand APIs
- SOAP Control Center APIs
- SOAP Log Collection APIs
- SOAP Performance Informations APIs
- SOAP Realtime Informations and Control Center APIs
- SOAP SNMP Config API
- Service Activation web page
- Serviceability Report Archive
- Trace Collection Tool
- Trace Configuration web page
- Troubleshoot Trace Settings web page

Service Parameter and Enterprise Parameter Changes

This feature requires no configuration to work.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(1) or upgrade to 7.1(1), you can use this feature.

Serviceability Considerations

For more information, refer to the Cisco Unified Serviceability section of this document.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

This feature does not affect the end user.

Standard Audit Users User Group

Only a user or application assigned to the Standard Audit Users user group can change audit log settings. By default, the CCMAdministrator application user gets assigned to the Standard Audit Users user group and can add or delete users from the Standard Audit Users user group.

You can configure the audit log settings that can be changed by a Standard Audit Log user through the Standard Audit Log Administration role. See the "Standard Audit Log Administration Role" section on page 94.

Service Parameter and Enterprise Parameter Changes

This feature requires no configuration to work.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(1) or upgrade to 7.1(1), you can use this feature.

Serviceability Considerations

For more information, refer to the Cisco Unified Serviceability section of this document.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

This feature does not affect the end user.

Synchronization of Configuration Settings

Description

Cisco Unified Communications Manager Release 7.1(1) allows you to use a single button in Cisco Unified Communications Manager Administration pages to synchronize various devices with the most recent configuration changes. This button is called “Apply Config” when it is located on a configuration window, and is called “Apply Config to Selected” when it is located in a “Find and List” window.

Cisco Unified Communications Manager Administration Configuration Tips

To synchronize a device with the most recent configuration changes, perform the following procedure.

Procedure

Step 1 Navigate to one of the windows shown in Table 19. Table 19 lists all the windows in Cisco Unified Communications Manager Administration, organized by menu, that provide the configuration synchronization function.

The Find and List window for the applicable items displays.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.

Step 4 The window displays a list of items that match the search criteria.

a. If the window shows a button called **Apply Config to Selected**, perform the following (otherwise proceed to b.)

- Check the check boxes next to the items that you want to synchronize. To choose all items in the window, check the check box in the matching records title bar.
- Click **Apply Config to Selected.**
- Proceed to Step 5.

b. If the window *does not* show a button called **Apply Config to Selected**, perform the following:

- Click the item that you want to synchronize.
- The configuration window for the item you clicked displays.

  Click **Apply Config**.

  Proceed to Step 5.

Step 5 The **Apply Configuration Information** dialog displays.

Note The device(s) may need to restart for configuration changes to take effect.

Click **OK**.

Table 19 Windows for Synchronizing Configuration Settings

Navigation Path to Window	Window Name
System Menu	
System > Cisco Unified CM	Cisco Unified CM Configuration

Table 19 Windows for Synchronizing Configuration Settings (continued)

Navigation Path to Window	Window Name
System > Cisco Unified CM Group	Cisco Unified CM Group Configuration
System > Date/Time Group	Date/Time Group Configuration
System > Region	Region Configuration
System > Device Pool	Device Pool Configuration
System > Enterprise Parameters	Enterprise Parameters Configuration
System > Security > Phone Security Profile	Phone Security Profile Configuration
System > Security > SIP Trunk Security Profile	SIP Trunk Security Profile Configuration
Call Routing Menu	
Call Routing > Dial Rules > SIP Dial Rules	SIP Dial Rule Configuration
Call Routing > Route Filter	Route Filter Configuration
Call Routing > Route Hunt > Route List	Find and List Route Lists
Call Routing > Route Hunt > Hunt List	Find and List Hunt Lists
Call Routing > Class of Control > Partition	Partition Configuration
Call Routing > Intercom > Intercom Route Partition	Intercom Partition Configuration
Call Routing > Intercom > Intercom Directory Number	Intercom Directory Number Configuration
Call Routing > Directed Call Park	Directed Call Park Configuration
Call Routing > Directory Number	Directory Number Configuration
Media Resources Menu	
Media Resources > Annunciator	Find and List Annunciators
Media Resources > Conference Bridge	Find and List Conference Bridges
Media Resources > Media Termination Point	Find and List Media Termination Points
Media Resources > Music On Hold Server	Find and List Music On Hold Servers
Media Resources > Transcoder	Find and List Transcoders
Voice Mail Menu	
Voice Mail > Cisco Voice Mail Port	Find and List Cisco Voice Mail Ports
Voice Mail > Voice Mail Profile	Voice Mail Profile Configuration
Device Menu	
Device > CTI Route Point	Find and List CTI Route Points
Device > Gatekeeper	CTI Route Point Gatekeepers
Device > Gateway	Find and List Gateway
Device > Phone	Find and List Phones
Device > Trunk	Find and List Trunks
Device > Device Settings > Softkey Template	Softkey Template Configuration
Device > Device Settings > SIP Profile	SIP Profile Configuration
Device > Device Settings > Common Device Configuration	Common Device Configuration
Device > Device Settings > Common Phone Profile	Common Phone Profile Configuration

Table 19 Windows for Synchronizing Configuration Settings (continued)

Navigation Path to Window	Window Name
Application Menu	
Application > Cisco Unified CM Attendant Console > Pilot Point	Find and List Pilot Points

GUI Changes

The Cisco Unified Communications Manager Administration pages added the "Apply Config" or "Apply Config to Selected" buttons to the windows listed in Table 19.

Service Parameter and Enterprise Parameter Changes

The Enterprise Parameters Configuration window (**System > Enterprise Parameters**) contains the "Apply Config" button.

Installation/Upgrade (Migration) Considerations

No specific installation or upgrade considerations exist for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

BAT support this feature by enabling the "Apply Config" button on the following pages:

- Bulk Administration > Phones > Update Phones—The **Apply Config** button allows you to reset only the settings that have changed since the last reset.
- Bulk Administration > Phones > Reset/Restart Phones—The **Apply Config** button allows you to reset only the settings that have changed since the last reset.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

This feature does not affect the end user.

For More Information

Refer to configuration information as it pertains to the windows listed in Table 19 in the following manuals:

- *Cisco Unified Communications Manager Administration Guide*
- *Cisco Unified Communications Manager Features and Services Guide*
- *Cisco Unified Communications Manager System Guide*

Table Out of Sync Detection

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

When the Table Out Of Sync parameter is turned on, the Database Replication Status summary gets collected every day during the maintenance window. The system compares the output of three consecutive days to determine if tables have been out of sync for all three days. If so, it triggers an alert.

This parameter, by default, is set to Off and is run at the time specified in Maintenance Time parameter.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

To use the database table out of sync feature, ensure that you turn the parameter on.

To enable the database table out of sync feature, perform the following procedure:

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Service Parameter.**

Step 2 From the Server drop-down list, select the server.

Step 3 From the Service drop-down list, select **Cisco Database Layer Monitor.**

Step 4 Set the Maintenance Time parameter value.

Step 5 Set the Maintenance Window parameter value.

Step 6 From the Table Out of Sync Detection drop-down list, choose **On**.

Step 7 From the MaintenanceTaskTrace drop-down list, choose **On**.

Step 8 Click **Save**.

Steps to Ensure That You are Notified of Inconsistencies

To ensure that you will be notified if the databases on the publisher server and the subscriber servers are inconsistent, you should perform the following tasks:

- Complete the steps described in "Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes" section on page 100.
- Enable the alert.
- Configure the Alert in RTMT.

Enable the Alert

To enable Cisco Unified CM to alert you in case of out of sync conditions, perform the following steps from Cisco Unified Serviceability:

Step 1 From the Alarm menu, choose **Configuration**.

Step 2 From the server drop-down list, choose your server.

Step 3 From from the Service Group drop-down list, choose **Database and Admin Services** and click **Go**.

Step 4 From the Service drop-down list, choose **Cisco Database Monitor Layer Monitor** and click **Go**.

Step 5 In the SDI Trace field, click **Enable Alarm** and set the Alarm Event Level to.....

Step 6 Click **Save**.

Configure the Alert in RTMT

To configure the alert in RTMT, see the Setting Alert Properties in the *Cisco Unified Real-time Monitoring Tool Guide*.

Note You can configure RTMT to make you aware of this alarm via email.

Note Cisco recommends that you call TAC if this alert gets generated.

For More Information

- *Cisco Unified Real-time Monitoring Tool Guide*

Unconfigured Device Registration Attempts Restricted

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Prior to Cisco Unified Communications Manager 6.1(3) or 7.1(1) (not 7.0(1)), if a Cisco Unified IP Phone had not been added to the Cisco Unified Communications Manager database and did not have auto-registration enabled, the phone would repeatedly attempt to register (unsuccessfully) with Cisco Unified Communications Manager, thus wasting Cisco Unified Communications Manager with these repeated registration requests.

However, in Cisco Unified Communications Manager 6.1(3) or 7.1(1), if auto-registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone will not attempt to register with Cisco Unified Communications Manager. The phone continues to display the Configuring IP message until auto-registration gets enabled or until the phone gets added to the Cisco Unified Communications Manager database.

Supported Devices

The following devices support this changed registration behavior:

- IP Phone 7906G
- IP Phone 7911G
- IP Phone 7931G
- IP Phone 7941G
- IP Phone 7942G
- IP Phone 7945G
- IP Phone 7961G
- IP Phone 7962G
- IP Phone 7965G
- IP Phone 7970G

- IP Phone 7971G
- IP Phone 7975G
- Cisco Analog Telephone Adapter
- VG248 Gateways

Cisco Unified Communications Manager Administration Configuration Tips

For information on configuring autoregistration, refer to the "Autoregistration" chapter in the *Cisco Unified Communications Manager System Guide*. For information on configuring a phone, refer to the "Phone Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Before you configure a phone, consider the following information:

- If the Cisco Unified Communications Manager database contains a real MAC address for a phone, not the dummy MAC address that is created via the Bulk Administration Tool (BAT), licensing immediately consumes device license units for the phone after the phone gets added to the database.
  - If the number of used device license units and number of pending device licensing units do not exceed the total number of device license units that are available for use, the phone with the real MAC address gets added to the database.
  - If the number of used device license units and number of pending device licensing units exceed the total number of device license units that are available for use, the phone with the real MAC address does not get added to the database.
- Licensing uses the Is Active check box in the Phone Configuration window in Cisco Unified Communications Manager Administration to determine whether to consume device license units for the phone. In addition, Cisco Unified Communications Manager uses this check box to determine whether a phone should register with Cisco Unified Communications Manager.

  For a phone that uses a real MAC address, not the dummy MAC address that is created via BAT, the check box displays as checked and disabled, which indicates that the phone uses device license units and can register with Cisco Unified Communications Manager.

  For a phone that uses the dummy MAC address that is created via BAT, the Is Active check box displays as unchecked and enabled. If you manually convert the dummy MAC address to a real MAC address in the Phone Configuration window, check the Is Active check box, which ensures that the phone can register with Cisco Unified Communications Manager and that licensing consumes device license units for the phone.
- Cisco Unified Communications Manager allows you to provision phones with dummy MAC addresses via BAT as long as the number of used device license units and the number of pending device license units do not exceed the total number of device license units that are available for use.
- If you use the Cisco Unified Communications Manager Auto-Register Phone Tool (TAPS) to associate an auto-registered phone with the BAT dummy settings, the Cisco Unified Communications Manager Auto-Register Phone Tool deletes the auto-registered phone from the database, and licensing gives you credits for the device license units for the deleted phone. After the Cisco Unified Communications Manager Auto-Register Phone Tool applies the device name to the phone that uses the dummy MAC address, the Cisco Unified Communications Manager Auto-Register Phone Tool updates the Is Active check box to display as checked and disabled. Licensing consumes device license units for the phone, and the phone can register with Cisco Unified Communications Manager, unless the number of used device license units exceeds the total number of device license units that are available for use.
- When a phone auto-registers for use with the Cisco Unified Communications Manager Auto-Register Phone Tool, it gets inserted into the database as long as the number of used device license units is less than the number of device license units that are available for use.

- You can view the number of pending, used, and available device license units in the License Unit Report and the License Unit Calculator in Cisco Unified Communications Manager Administration.

GUI Changes

No new fields display in Cisco Unified Communications Manager Administration for this feature.

Service Parameter and Enterprise Parameter Changes

No parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(1), if auto-registration is not enabled and the phone has not been added to the Cisco Unified Communications Manager database, the phone does not attempt to register with Cisco Unified Communications Manager.

Serviceability Considerations

The Real-Time Monitoring Tool and Cisco Unified Reporting can display information on registered and unregistered devices. For more information, refer to the *Real-Time Monitoring Tool Administration Guide* and the *Cisco Unified Reporting Administration Guide*.

BAT Considerations

For information on adding devices through BAT, refer to the *Cisco Unified Communications Manager Bulk Administration Guide*.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

If the Configuring IP message displays on the phone, the phone user should contact the phone administrator.

Viewing Held Calls on Shared Lines

Tip This feature is supported in Cisco Unified Communications Manager Releases 7.1(1) and 6.1(3).

Description

With the held calls on shared lines feature, a phone user can determine whether the call was put on hold by the phone user locally at the primary device or by another party remotely on a shared device. How the held call displays on the devices depends on whether the primary device or shared device puts the call on hold. For information on how the held call displays on the devices, see the "Hold Status" section on page 128.

Cisco Unified Communications Manager Administration Configuration Tips and GUI Changes

This feature requires no configuration to work.

Service Parameter and Enterprise Parameter Changes

This feature requires no configuration to work.

Installation/Upgrade (Migration) Considerations

After you install Cisco Unified Communications Manager 7.1(1) or upgrade to 7.1(1), you can use this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR or CDR considerations exist for this feature.

Security Considerations

No security considerations exist for this feature.

AXL and CTI Considerations

No AXL or CTI considerations exist for this feature.

User Tips

For a list of phones that support this feature, see the "Hold Status" section on page 128.

For More Information

- Hold Status, page 128

Security

This section contains information on the following Cisco Unified Communications Manager Administration security features and applications:

- CAPF Interaction with IPv6 Addressing, page 104
- Security Icons, page 105
- Cisco Security Agent Version, page 107
- Accessing Cisco Security Agent Logs, page 107

CAPF Interaction with IPv6 Addressing

Description

CAPF can issue and upgrade certificates to a phone that uses an IPv4, an IPv6, or both types of addresses. Table 20 describes how a phone that has an IPv4, IPv6, or both types of addresses connects to CAPF.

Table 20 How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF; if the phone cannot connect via an IPv6 address, it attempts to connect by using an IPv4 address.
Dual-stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Dual-stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Dual-stack	IPv4	IPv6	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv4	Phone cannot connect to CAPF.
Dual-stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
IPv6	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4	IPv4	IPv6	Phone cannot connect to CAPF.
IPv6	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6	IPv6	IPv4	Phone cannot connect to CAPF.

Cisco Unified Communications Manager Administration Configuration Tips

To issue or upgrade certificates for SCCP phones that use an IPv6 address, you must set the Enable IPv6 service parameter to True in Cisco Unified Communications Manager Administration.

For More Information

- Internet Protocol Version 6 (IPv6), page 32
- *Cisco Unified Communications Manager Security Guide*

Security Icons

Description

Cisco Unified Communications Manager provides security status for a call, according to security levels that are configured for the Cisco Unified Communications Manager server(s) and devices participating in the call.

Phones that support security icons display the call security level.

- The phone displays a shield icon for calls with a signaling security level of authenticated. A shield identifies a secured connection between Cisco IP devices, which means that the devices have authenticated or encrypted signaling.
- The phone displays a lock icon for calls with encrypted media, which means that the devices are using encrypted signaling and encrypted media.

Note Some phone models display only the lock icon.

The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signaling support notification of call security status changes to participating endpoints. If a SIP trunk is involved in a call path, the call session status specifies nonsecure. Refer to *Cisco Unified Communications Manager Security Guide* for restrictions that are associated with security icons.

The call security status is based on the audio and video portions of the call. The call is considered secure only if both the audio and video portions are secure. Table 21 describes the rules that determine whether a security icon displays, and which icon appears.

Table 21 Security Icon Display Rules

Media and Device Types In the Call	Phones That Display Both Shield and Lock Icons	Phones That Display Only the Lock Icon
Secure audio only	Lock	Lock
Secure audio with unsecure video	Shield	None
Secure audio with secure video	Lock	Lock
Authenticated device with nonsecure audio only	Shield	None
Authenticated device with nonsecure audio and video	Shield	None
Unauthenticated device with nonsecure audio only	None	None
Unauthenticated device with nonsecure audio and video	None	None

For conference and barge calls, the security icon displays the security status for the conference.

Cisco Unified Communications Manager Administration Configuration Tips

No configuration is required for this feature.

GUI Changes

No GUI changes exist for this feature.

Service Parameter and Enterprise Parameter Changes

No service parameter or enterprise parameter changes exist for this feature.

Installation/Upgrade (Migration) Considerations

No installation or upgrade considerations exist for this feature.

Serviceability Considerations

No serviceability considerations exist for this feature.

BAT Considerations

No BAT considerations exist for this feature.

CAR/CDR Considerations

No CAR/CDR considerations exist for this feature.

Security Considerations

This feature changes the rules that determine the display of secure icons on secure phones.

AXL and CTI Considerations

No CAR/CDR considerations exist for this feature.

User Tips

None

For More Information

- *Cisco Unified Communications Manager Security Guide*

Cisco Security Agent Version

Cisco Security Agent version 5.2 is included with this release of Cisco Unified Communications Manager.

Accessing Cisco Security Agent Logs

The CLI command that accesses the log for Cisco Security Agent is changed to **utils create report csa**. Refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions* for more information about starting a CLI session and using CLI commands.

Bulk Administration Tool

This section contains information on the following topics:

- Support for Party Entrance Tone, page 108
- Support for Log Missed Calls, page 109
- Support for Always Use Prime Line, page 110
- Support for VG202 and VG204 Gateways, page 111
- Phone Migration in BAT, page 112

- Support for Logical Partitioning, page 113
- New fields supported for Export by Import/Export, page 113
- Support for Park Monitoring, page 113
- Support for Seamless Integration (Apply Config), page 114

Support for Party Entrance Tone

The Bulk Administration GUI has the following updates to support the party entrance tone feature:

- Party Entrance Tone drop-down list box—choose one of the following options:
  - **Default**—Use the value that you configured in the Party Entrance Tone service parameter.
  - **On**—A tone plays on the phone when a basic call changes to a multi-party call; that is, a barge call, cBarge call, ad hoc conference, meet-me conference, or a joined call. In addition, a different tone plays when a party leaves the multi-party call. If the controlling device, that is, the originator of the multi-party call has a built-in bridge, the tone gets played to all parties if you choose On for the controlling device. When the controlling device leaves the call, Cisco Unified Communications Manager identifies whether another device on the call can play the tone; if another device on the call can play the tone, Cisco Unified Communications Manager plays the tone. If the controlling device cannot play the tone, Cisco Unified Communications Manager does not play the tone even if you enable the party entrance tone feature.
  - **Off**—A tone does not play on the phone when a basic call changes to a multi-party call.

Note The Party Entrance Tone drop-down list box displays in the Phone Line Template, UDP Line Template, gateway Line Template, UDP Update Line, RDP Line Template, and Phone Update Line windows.

- Insert, Export, and Validate Details support for party entrance tone—the following insert, export, and validate details features have support for the party entrance tone:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
  - Insert Gateways

  - Insert Remote Destination Profiles
  - Export Remote Destination Profiles
  - Phone Add lines
  - UDP Add Lines
  - Phone Update Lines
  - UDP Update Lines
  - Generate Phone Report
  - Generate UDP Report
- File Formats—the following file formats support the party entrance tone feature:
  - Phone File Format—Party Entrance Tone field is a part of the Line Fields section.
  - UDP File Format—Party Entrance Tone field is a part of the Line Fields section.
  - Remote Destination Profile File Format—Party Entrance Tone field is a part of the Line Fields section.
- Generate Phone Report—The Generate Phone Report Configuration page lists the Party Entrance Tone field in the Line Fields section.

Support for Log Missed Calls

The Bulk Administration GUI has the following updates to support the Log Missed Calls feature:

- Log Missed Calls Check Box— This check box allows you to turn this feature on or off. If the check box displays as checked (turned on), which is the default for this setting, Cisco Unified Communications Manager logs missed calls in the call history for that shared line appearance on the phone.

Note The Log Missed Calls Check Box displays in the Phone Line Template, UDP Line Template, Phone Update Line, and UDP Update Line windows.

- Insert, Export, and Validate Details support for the log missed calls feature—the following insert, export, and validate details features have support for the log missed calls feature:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details
  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details

  - Insert Phones/Users
  - Validate Phones/Users
  - Phone Add lines
  - UDP Add Lines
  - Phone Update Lines
  - UDP Update Lines
  - Generate Phone Report
  - Generate UDP Report
- File Formats—the following file formats support the missed logged calls feature:
  - Phone File Format—Missed logged calls field is a part of the Line Fields section.
  - UDP File Format—Missed logged calls field is a part of the Line Fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration page lists the Log Missed Calls field in the Line Fields section.
- Generate Phone Report—The Generate Phone Report Configuration page lists the Log Missed Calls field in the Line Fields section.

Support for Always Use Prime Line

The Bulk Administration GUI has the following updates to support the Always Use Prime Line feature:

- Always Use Prime Line drop-down list box—choose one of the following options:
  - Off
  - On
  - Default
- Always Use Prime Line for Voice Message drop-down list box—choose one of the following options:
  - Off
  - On
  - Default

Note For details of configuration options for the Always Use Prime Line feature, refer to Table 2 and Table 3.

Note The Always Use Prime Line, and Always Use Prime Line for Voice Message drop-down list boxes are present on the Phone Template, UDP Template, and Update Phone pages.

- Insert, Export, and Validate Details support for always use prime line—the following insert, export, and validate details features have support for the always use prime line feature:
  - Insert Phones Specific Details
  - Insert Phones All Details
  - Export Phones Specific Details

  - Export Phones All Details
  - Validate Phones All Details
  - Validate Phones Specific Details
  - Insert UDP All Details
  - Insert UDP Specific Details
  - Export UDP All Details
  - Export UDP Specific Details
  - Validate UDP All Details
  - Validate UDP Specific Details
  - Insert Phones/Users
  - Validate Phones/Users
  - Generate Phone Report
  - Generate UDP Report
- Phone File Format—Phone File Format Configuration page lists the Always Use Prime Line, and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- UDP File Format—UDP File Format Configuration page lists the Always Use Prime Line, and Always Use Prime Line for Voice Message drop-down list boxes in the device fields section.
- Generate User Device Profile Report—The Generate User Device Profile Report Configuration page lists the Always Use Prime Line, and Always Use Prime Line for Voice Message fields in the Device Fields section.
- Generate Phone Report—The Generate Phone Report Configuration page lists the Always Use Prime Line, and Always Use Prime Line for Voice Message fields in the Line Fields section.

Support for VG202 and VG204 Gateways

BAT now supports VG202 and VG204 gateways. The Bulk Administration Tool has the following updates to support VG202 and VG204 gateways:

- Bulk Administration >Gateways >Gateway Template—VG202 and VG204 gateways now display in the Gateway Type drop-down list box.
- Bulk Administration >Gateways >Insert Gateways—VG202 and VG204 gateways now display in the Gateway Type drop-down list box.
- Bulk Administration >Gateways >Insert Gateways. Select Gateway type as VG202 or VG204 and click next. The second Insert Gateways Configuration page displays—The View Sample File link displays VG202 and VG204 sample files.
- File Formats—the Create File Format and Add File Format gateway pages now support VG202 and VG204 gateways.
- Generate Gateway Report—The Generate Gateway Report Configuration page now lists all supported gateways including VG202 and VG204.
- Delete Gateway Support—Delete Gateways Configuration page now lists all BAT supported gateways including VG202 and VG204.
- BAT.XLT Support—VG202 and VG204 gateways are supported by BAT.xlt.

Phone Migration in BAT

You can use the Phone Migration feature in Cisco Unified Communications Manager Bulk Administration Tool to migrate phones from one type to another in bulk. You can access the Phone Migration submenu from the Bulk Administration menu of Cisco Unified Communications Manager.

Some limitations to keep in mind while migrating phones are:

- Migrating to a phone with fewer speed dials or lines will not remove lines or speed dials. However, some of the lines/speed dials will no longer show up on the phone. You can still find all of the original lines/speed dials on the phone configuration page.
- Even migrating to a newer phone can cause loss of features like in the case of moving from SIP to SCCP or vice versa.
- Only existing phones can be migrated. If you enter a non-existing device in the CSV file, the system displays an error message.
- If the phone gets migrated successfully, the old phone will be updated with the new phone settings.
- If you select the reset or restart option, the new phone would be reset.

You can create a CSV file for phone migration by using one of the following options:

- Using the BAT Spreadsheet to create CSV Data Files for phone migration
- Using a text editor to create a text-based CSV File for phone migration

Migrating Phones

To migrate phones in bulk with the Phone Migration feature in BAT, use the following procedure:

Before You Begin

- You must have a data file in comma separated value (CSV) format that contains device name of the phone that you wish to migrate, the MAC address for the new phone, and the description for the new phone.
- You must have a phone template of a specific type, and the protocol you wish to use for migration configured and ready.
- Upload the data files by choosing the relevant target and function for the transaction using the procedure that is mentioned in “Uploading a File” section in the *Cisco Unified Communications Manager Bulk Administration Guide*.

Procedure

Step 1 Choose **Bulk Administration > Phone Migration**. The Phone Migration Configuration window displays.

Step 2 You can choose to reset or restart phones by selecting the appropriate radio button from the Reset/Restart Information section. ‘Don’t Reset/Restart phones’ is the default setting.

Step 3 In the Phone Migration Information section, from the File Name drop-down list box, choose the file that you uploaded.

Step 4 From the Phone Template Name drop-down list box, choose the phone template that you wish to use for migration.

Step 5 In the Job Information section, enter a description for the job. The default description specifies Phone Migration.

Step 6 You can choose to run the job immediately or later by selecting the corresponding radio button.

Step 7 To create a job for migrating phones, click **Submit**.

Step 8 A warning message informing you of a possible loss of features/data displays.

Click **Cancel** to return to the Phone Migration Configuration window without submitting the job;

OR

Click **OK**, to continue with submitting the job.

A message in the Status section lets you know that the job was submitted successfully.

Step 9 To schedule and/or activate this job, use the Job Scheduler option in the Bulk Administration main menu.

Support for Logical Partitioning

BAT supports the logical partitioning feature by enabling GeoLocation configuration in bulk. The following BAT pages include the GeoLocation field:

- Bulk Administration > Phones > Phone Template—The GeoLocation drop-down list box displays on the Phone Template Configuration page.
- Bulk Administration > Gateways > Gateway Templates > Select VG224 Gateway, Module: Analog, Subunit0: 24FXS-SCCP, Product Type: Analog—The GeoLocation drop-down list box displays on the Phone Template Configuration page.

New fields supported for Export by Import/Export

Bulk Administration > Import/Export > Export. The flowering new fields are supported for export by the Import/Export tool:

System Data

- Geo Location
- Geo Location Filter
- Enterprise Phone Configuration

Call Routing Data

- Logical Partition Policy

Support for Park Monitoring

The Bulk Administration GUI has the following updates to support the Park Monitoring feature:

- Bulk Administration > Phones > Add/Update Lines > Update Lines—The following Park Monitoring fields display:
  - Park Monitoring Forward No Retrieve Destination External—Cisco Unified Communications Manager Release 7.1(1) does not support this setting.
  - Park Monitoring Forward No Retrieve Destination Internal—Cisco Unified Communications Manager Release 7.1(1) does not support this setting.
  - Park Monitoring Reversion Timer—Cisco Unified Communications Manager Release 7.1(1) does not support this setting.

- Bulk Administration > Phones > Phone Template; click Add a new DN in the Associated Information area. The Line template Configuration Page displays—The following Park Monitoring fields display on this page:
  - Park Monitoring Forward No Retrieve Destination External—Cisco Unified Communications Manager Release 7.1(1) does not support this setting.
  - Park Monitoring Forward No Retrieve Destination Internal—Cisco Unified Communications Manager Release 7.1(1) does not support this setting.
  - Park Monitoring Reversion Timers—Cisco Unified Communications Manager Release 7.1(1) does not support this setting.

Note You can access the Line Template Configuration page though the UDP line template, gateway Line template. Phone Update Line, and UDP Update Line pages.

Support for Seamless Integration (Apply Config)

BAT support the seamless integration feature by enabling the Apply Config button on the following pages:

- Bulk Administration > Phones > Update Phones—The **Apply Config** button allows you to reset only the settings that have changed since the last reset.
- Bulk Administration > Phones > Reset/Restart Phones—The **Apply Config** button allows you to reset only the settings that have changed since the last reset.

Cisco Unified Serviceability

This section contains these subsections:

- IPv6 and Serviceability, page 114
- Service Manager Enhancements, page 114
- Information Assurance and Audit Logging, page 116
- Cisco Audit Event Service, page 116
- Audit Role and Permissions, page 116
- DBReplicationTableOutOfSync Alarm, page 117

IPv6 and Serviceability

Alarms that report IPv4 addresses may also report IPv6 addresses, depending on the configuration in your network. For information on how to configure alarms and view alarm definitions in Cisco Unified Serviceability, refer to the *Cisco Unified Serviceability Administration Guide*.

SNMP supports IPv4, although the CISCO-CCM-MIB includes columns and storage for IPv6 addresses, preferences, and so on.

Service Manager Enhancements

The following information describes enhancements for Service Manager.

Starting and Stopping Service States

This release includes two new service states: Starting and Stopping.

When the service state is stopping, a service cannot start. When a service state is starting, a service cannot stop. These states display in the Service Activation window in Cisco Unified Serviceability and in the command line interface (CLI).

Performance Improvements for Service Manager

This release includes the following performance enhancements to Service Manager:

- ServM can respond to 60 requests per minutes.
- Blocking mode does not block a ServM scrip.
- ServM responds within tens of milliseconds to any request to handle a single service.
- ServM responds within hundreds of milliseconds to any request to handle all services.
- ServM writes fewer logs per day. In idle state, it writes approximately 37 logs per day.
- ServM maintains a single session with the Tomcat manager webapp.
- ServM sends three requests to the Tomcat server under idle conditions.

Disaster Recovery Framework Enhancements for Service Manager

The Disaster Recovery Framework (DRF) backs up the services.conf and servM.conf files. The restore process restores all services to their original forms.

Single Tomcat Session

Instead of creating a new session on the Tomcat manager webapp for every tomcat request, ServM now creates a single session on the Tomcat manager webapp.

Request Processor Thread

ServM is a multi-threaded application. In this release, ServM handles blocking in the request processing thread, which makes ServM available to most clients that request the service.

Common Webapp Timers

This release implements a common webapp health timer, which helps to improve system performance and allows reducing the number of requests that are sent to ServM.

Security Enhancements

This release implements the following security enhancements:

- Service Manager listens to port 8889 at the local host
- Service Manager does not accept raw XML data
- ServM resists to DOS attacks.

Service Manager Return Codes

Table 22 describes the Service Manager return codes that this release implements.

Table 22 New Service Manager Return Codes

Code	Meaning
1078	Service start pending
1079	Service stop pending
1080	HTTP timed out
1081	Tomcat webapp deploy failed
1082	Invalid Tomcat application URL
1083	No such Tomcat command specified
1084	Tomcat webapp undeploy failed
1085	No such Tomcat manager user failed
1086	Tomcat manager failed to reload
1087	Tomcat manager failed
1088	Webapp start failed
1089	Unknown Tomcat command
1090	Connection refused

Information Assurance and Audit Logging

Centralized audit logging is part of the Cisco Unified Communications Manager Information Assurance for Linux feature. Any configuration change to the Cisco Unified Communications Manager system gets logged in separate log files for auditing. In addition to centralized audit logging, there are security features that also comprise Information Assurance. Information Assurance is primarily administered through Cisco Unified Serviceability.

Cisco Unified Serviceability logs the following events:

- Activation, deactivation, start, or stop of a service from any Serviceability window.
- Changes in trace configurations and alarm configurations.
- Changes in SNMP configurations.
- Changes in CDR Management.
- Review of any report in the Serviceability Reports Archive. This log gets viewed on the reporter node.

Cisco Audit Event Service

The Cisco Audit Event Service was added to the Control Center Network GUI in Cisco Unified Serviceability to start or stop the Audit Log service. You may stop or restart this service by going to **Serviceability > Tools > Control Center - Network Services**.

Audit Role and Permissions

Only a user with an audit role has permission to change the Audit Log settings. By default, the CCMAdministrator has the audit role after fresh installs and upgrades. The CCMAdministrator can assign the “standard audit users” group to any new user that the CCMAdministrator specifically creates

for audit purposes. The CCMAdministrator can then be removed from the audit user group. The "standard audit log configuration" role provides the ability to delete audit logs, read/update access to Real-Time Monitoring Tool, Trace Collection Tool, RTMT Alert Configuration, the Control Center - Network Services window, RTMT Profile Saving, the Audit Configuration window, and a new resource called Audit Traces.

DBReplicationTableOutOfSync Alarm

In Cisco Unified Serviceability, you can configure the DBReplicationTableOutOfSync alarm, as described in the "New Preconfigured Alert - DBReplicationTableOutOfSync" section on page 119.

Cisco Unified Real-Time Monitoring Tool

This section contains these subsections:

- IPv6 and RTMT, page 117
- Audit Events Get Logged, page 118
- Viewing and Deleting Audit Logs, page 119
- Alert When Audit Logs Are Full, page 119
- Quality Report Tool Reports, page 119
- New Preconfigured Alert - DBReplicationTableOutOfSync, page 119
- System History Log Displays in RTMT, page 119

IPv6 and RTMT

In RTMT, you can monitor CTI applications, CTI devices, and CTI lines that use IPv6 addresses. When you search for the application, device, or line, enter the IPv6 address. and check the AppIpv6Addr check box in the attribute window.

In addition, you can perform a device search on phones or SIP trunks that use IPv6 addresses. When you choose CallManager > Device Search > Open Device Search > Phones (or SIP Trunks), make sure that you specify an IPv6 address and check the Ipv6Address check box in the attributes window.

Log files may display IPv4 and IPv6 addresses, depending on the configuration in your network.

In RTMT, the performance monitoring counters in Table 23 display for the IP6 object, which provide IPv6-related statistics for your system.

Table 23 IP6

Counters	Counter Descriptions
Frag Creates	This counter represents the number of IP datagrams fragments that have been generated as a result of fragmentation at this entity.
Frag Fails	This counter represents the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not, for example because their Do not Fragment flag was set.
Frag OKs	This counter represents the number of IP datagrams that have been successfully fragmented at this entity.

Table 23 IP6 (continued)

Counters	Counter Descriptions
In Delivers	This counter represents the total number of input datagrams successfully delivered to IP user-protocols (including Internet Control Message Protocol [ICMP]).
In Discards	This counter represents the number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams that were discarded while awaiting reassembly.
In HdrErrors	This counter represents the number of input datagrams discarded due to errors in their IP header, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
In Receives	This counter represents the number of input datagrams received from all network interfaces, including those received with errors.
In UnknownProtos	This counter represents the number of locally addressed datagrams that were received successfully but discarded because of an unknown or unsupported protocol.
InOut Requests	This counter represents the total number of IP datagrams received and the number of IP datagrams sent.
Out Discards	This counter represents the number of output IP datagrams that was not transmitted and was discarded. One reason may be a lack of buffer space.
Out Requests	This counter represents the total number of IP datagrams which local IP user-protocols (including Internet Control Message Protocol [ICMP]) supply to IP in requests transmission. This counter does not include any datagrams counted in ForwDatagrams.
Reasm Fails	This counter represents the number of failures detected by the IP reassembly algorithm (for various reasons, for example timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms, notably the algorithm in RFC 815, can lose track of the number of fragments by combining them as they are received.
Reasm OKs	This counter represents the number of IP datagrams that have been successfully reassembled.
Reasm Reqds	This counter represents the number of IP fragments received which needed to be reassembled at this entity.

Audit Events Get Logged

Centralized audit logging is part of the Cisco Unified Communications Manager Information Assurance for Linux feature. Any configuration change to the Cisco Unified Communications Manager system gets logged in separate log files for auditing. An audit event is any event that is required to be logged.

Real-Time Monitoring Tool logs the following events with an audit event alarm:

- Alert configuration.
- Alert suspension.
- E-mail configuration.
- Set node alert status.
- Alert addition.
- Add alert action.
- Clear alert.
- Enable alert.
- Remove alert action.
- Remove alert.

Viewing and Deleting Audit Logs

All audit logs are collected, viewed and deleted from Trace and Log Central in the Real-Time Monitoring Tool.

Alert When Audit Logs Are Full

Audit logs get written in the common partition. The Log Partition Monitor (LPM) manages the purging of these audit logs as needed, similar to trace files. By default, the LPM purges the audit logs, but the audit user can change this setting from the Audit User Configuration page in Cisco Unified Serviceability. The LPM sends an alert whenever the common partition disk usage exceeds the threshold; however, the alert does not have the information about whether the disk is full because of audit logs or trace files.

Quality Report Tool Reports

There is a change in the Call State information collected from Cisco Unified Communications Manager/CTIManager and displayed in the Quality Report Tool (QRT) reports. Previously the information included Connected, Connected Conference, Connected Transfer, and On Hook call state information. Now the report only includes Connected and On Hook call state information.

- New Preconfigured Alert - DBReplicationTableOutOfSync, page 119
- System History Log Displays in RTMT, page 119

New Preconfigured Alert - DBReplicationTableOutOfSync

For information on the DBReplicationTableOutofSync alert, see the "Table Out of Sync Detection" section on page 100.

System History Log Displays in RTMT

To access the system history log in RTMT, navigate to RTMT Trace Collection:

RTMT > Trace Log Collection

For more information on the system history log, see the "System History Log for Cisco Unified Communications Manager" section on page 2.

Cisco Unified Communications Manager CDR Analysis and Reporting

This section contains these subsections:

- Audit Events Get Logged, page 120
- Customized Log-on Message, page 120
- Upgrade of CAR Data, page 120
- Backup of CAR Data, page 121
- FTP/SFTP Billing Servers, page 122
- Ensure CAR Administrator Privileges Are Restored After Upgrade, page 122

Audit Events Get Logged

Centralized audit logging is part of the Cisco Unified Communications Manager Information Assurance feature. Any configuration change to the Cisco Unified Communications Manager system gets logged in separate log files for auditing.

An audit event is any event that is required to be logged. Cisco Unified CDR Analysis and Reporting creates audit logs for these events:

- Scheduling the CDR Loader.
- Scheduling the daily, weekly, and monthly user reports, system reports, and device reports.
- Mail parameters configurations.
- Dial plan configurations.
- Gateway configurations.
- System preferences configurations.
- Autopurge configurations.
- Rating engine configurations for duration, time of day, and voice quality.
- QoS configurations.
- Automatic generation/alert of pregenerated reports configurations.
- Notification limits configurations.

Customized Log-on Message

You can upload a text file that contains a customized log-on message that appears on the initial Cisco Unified Communications Manager CDR Analysis and Reporting window.

Upgrade of CAR Data

When you upgrade from an earlier version of Cisco Unified Communications Manager to a later version of Cisco Unified Communications Manager, you may not be able to upgrade all your CDR data.

The Cisco Unified Communications Manager installation program limits the time period for the migration of the CAR records from the CSV files in the Data Migration Assistant (DMA) TAR file to the CAR database on the upgraded system. The migration time period is 60 minutes. To allow the migration of the highest number of CSV files in the allotted time period, CAR record migration uses the following steps:

- Data migration begins with the migration of the billing records from the tbl_billing_data CSV file to the tbl_billing_data table of the CAR database. Data migration begins with the youngest record and proceeds toward the oldest record in the CSV file. The billing data migration stops when there are no more billing records to migrate or the migration time period reaches 60 minutes.
- If time remains after the billing data gets migrated, data migration proceeds with the migration of error records from the tbl_billing_error CSV file to the tbl_billing_error table of the CAR database. Data migration begins with the youngest record and proceeds toward the oldest record in the CSV file. For each error record that gets migrated, CAR migrates the data that corresponds to the error_record_id that is present in the tbl_error_id_map CSV file into the tbl_error_id_map table of the CAR database. This action ensures that error record data migration stays consistent with data in the tbl_error_id_map. The error record data migration stops when there are no more error records to migrate or the migration period reaches 60 minutes.

If the 60 minute migration time limit occurs at any point in the migration process, CAR data migration ceases and the tbl_system_preferences of the CAR database gets updated to reflect the data present in the upgraded system database.

Backup of CAR Data

The CAR and CDR Disaster Recovery Service (DRS) now integrates into the Cisco Unified Communications Manager DRS. The DRS includes the backup of the CAR database, pregenerated reports, and the CDR preserved flat files.

The CAR Web Service and CAR Scheduler automatically stop before the backup and restore process begin, and automatically restart after the backup and restore process is complete.

Table 1-24 displays the features and components that the Disaster Recovery System can back up and restore. For each feature that you choose, the system backs up all its components automatically.

Table 1-24 Cisco Unified CM Features and Components

Feature	Components
CCM—Cisco Unified Communications Manager	Cisco Unified Communications Manager database
	Platform
	Serviceability
	Music On Hold (MOH)
	Cisco Emergency Responder
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tct (trace collection tool)
	Call Detail Records (CDRs)
	CDR Reporting and Analysis (CAR)

FTP/SFTP Billing Servers

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner (CTDP) program. CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to http://www.cisco.com/pcgi-bin/ctdp/search.pl. For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to http://www.globalscape.com/gsftps/cisco.aspx. Cisco uses the following servers for internal testing. You may use one of these servers, but you must contact the vendor for support:

- Open SSH (for Unix systems).
- Cygwin (refer to http://sshwindows.sourceforge.net/).
- Titan (refer to http://www.titanftp.com/).

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support

Cisco has tested and will support the following versions of FTP or SFTP for CAR billing servers:

- Linux/Unix
  - FTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)
  - SFTP: Unix (SunOS 5.6 Generic_105181-10) and Linux server (2.4.21-47.ELsmp and 2.6.9-42.7.ELsmp)
- Windows
  - FTP: Microsoft FTP service (Windows 2000 5.00.2195 sp4, IIS 5.0), WAR FTP Daemon (1.82.0.10), and FreeFTPd (1.0.10 and 1.0.11). FreeFTPd can be used only for files that are less than 1 GB in size.
  - SFTP: FreeFTPd (1.0.10 and 1.0.11). Free FTPd can be used only for files that are less than 1 GB in size.

Ensure CAR Administrator Privileges Are Restored After Upgrade

When you use DMA to upgrade Cisco Unified Communications Manager, CAR users no longer have CAR administrator privileges after the upgrade and become standard end users. You must reset the CAR administrator privileges after the upgrade. Refer to the “Configuring CAR Administrators, Managers, and Users” section in the *CDR Analysis and Reporting Administration Guide* for more information on how to configure CAR administrators.

Cisco Unified Communications Manager Call Detail Records

This section contains these subsections:

- IPv6 and CDRs, page 123
- Logical Partitioning, page 124
- New Call Termination Cause Codes, page 124
- SIP Calls with URL in callingPartyNumber Field, page 124

- GlobalCallId Survives Over Cisco Unified Communications Manager Restarts, page 125

IPv6 and CDRs

Cisco Unified Communications Manager supports IPv6 in this release. There are two new CDR fields as part of this feature.

Table 25 IPv6 CDR Field Descriptions

Field Name	Range of Values	Description
origIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that originates the call signalling. The field can be either IPv4 or IPv6 format depending on the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field is the address of the Cisco Unified IP Phone. For PSTN calls, this field is the address of the gateway. For intercluster calls, this field is the address of the remote Cisco Unified Communications Manager. The IP address is either in dotted decimal format or in colon separated hexadecimal format. Default - The IP address of the originating device as reported by the device or used for the call after media negotiation.

Table 25 IPv6 CDR Field Descriptions (continued)

Field Name	Range of Values	Description
destIpv4v6Addr	Text string	This field comprises an alphanumeric string of up to 64 characters. This field identifies the IP address of the device that terminates the call signalling. The field can be either in IPv4 or IPv6 format depending upon the type of IP address that gets used for the call. For Cisco Unified IP Phones, this field is the address of the Cisco Unified IP Phone. For PSTN calls, this field is the address of the gateway. For intercluster calls, this field is the address of the remote Cisco Unified Communications Manager. The IP address is either in dotted decimal format or in colon separated hexadecimal format. Default - Empty String "" or null. If the destination does not get reached, this field stays empty.

Logical Partitioning

Logical partitioning is supported in this release of Cisco Unified Communications Manager. CDR examples that use logical partitioning are provided for call termination cause code 424 and cause code 503.

New Call Termination Cause Codes

New Cisco-specific call termination cause codes have been introduced to support logical partitioning.

Table 26 Cisco-Specific Call Termination Cause Codes

Decimal Value Code	Hex Value Code	Description
419430421	0x19000015	CCM_SIP_424_BAD_LOCATION_INFO
-1493172161	0xA700003F	CCM_SIP_503_SERVICE_UNAVAILABLE_SER_OPTION_NOAVAIL

SIP Calls with URL in callingPartyNumber Field

A new CDR example is provided for this situation: an incoming call is received through a SIP trunk by the Cisco Unified Communications Manager. The call contains a SIP URL for the callingPartyNumber CDR field.

GlobalCallId Survives Over Cisco Unified Communications Manager Restarts

For Cisco Unified Communications Manager Release 5.x and later releases, the value in the GlobalCallId CDR field survives over Cisco Unified Communications Manager restarts. In Release 4.x and earlier releases, even though the GlobalCallId field is time-based, the field gets reused under conditions of heavy traffic. Because of this behavior, problems can occur with customer billing applications and the ability of CAR to correlate CMRs with CDRs and to correlate conference call CDRs. For Release 5.x and later releases, GlobalCallId redesign ensures the field retains a unique value, at least for a certain number of days. Now, the last used globalCallId_callId value gets written to disk periodically (for every x number of calls). The value gets retrieved after a Cisco Unified Communications Manager restart, and the new globalCallId_callId value begins with this number plus x.

Cisco Unified Reporting

For a complete description of reports that are available on your system and the data that gets captured in a report, access the **Report Descriptions** report, as described in the *Cisco Unified Reporting Administration Guide*.

Table 27 describes the standard reports that display in *Cisco Unified Reporting Administration Guide*.

Table 27 Standard Reports That Display in Cisco Unified Reporting

Report	Description
Unified CM Cluster Overview	Provides an overview of the Cisco Unified Communications Manager cluster; for example, this report provides the Cisco Unified Communications Manager version that is installed in the cluster, the host name or IP address of all servers in the cluster, a summary of hardware details, and so on.
Unified CM Data Summary	Provides a summary of data that exists in the Cisco Unified Communications Manager database, according to the structure of the menus in Cisco Unified Communications Manager Administration. For example, if you configure 3 credential policies, 5 conference bridges, and 10 shared line appearances, you can see that type of information in this report.
Unified CM Database Replication Debug	Provides debugging information for database replication. **Tip** For this report, generation takes up to 10 seconds per server in the cluster and may spike CPU.
Unified CM Database Status	Provides a snapshot of the health of the Cisco Unified Communications Manager database. Generate this report before an upgrade to ensure that the database is healthy.
Unified CM Device Counts Summary	Provides the number of devices by model and protocol that exist in the Cisco Unified Communications Manager database.
Unified CM Extension Mobility	Provides a summary of Cisco Extension Mobility usage; for example, the number of phones that have a Cisco Extension Mobility user logged in to them, the users that are associated with Cisco Extension Mobility, and so on.
Unified CM GeoLocation Policy (new for 7.1)	Provides a list of records from the GeoLocation Logical Partitioning Policy Matrix.

Table 27 Standard Reports That Display in Cisco Unified Reporting (continued)

Report	Description
Unified CM GeoLocation Policy with Filter (new for 7.1)	Provides a list of records from the GeoLocation Logical Partitioning Policy Matrix for the selected GeoLocation policy.
Unified CM Lines Without Phones	Provides a list of lines that are not associated with a phone.
Unified CM Multi-Line Devices	Provides a list of phones with multiple line appearances.
Unified CM Phone Feature List (new for 7.1)	Provides a list of supported features for each device type in Cisco Unified Communications Manager Administration.
Unified CM Phones With Mismatched Load (new for 7.1)	Provides a list of all phones that have mismatched firmware load.
Unified CM Phones Without Lines	Provides a list of all phones in the Cisco Unified Communications Manager database that do not have lines associated with them.
Unified CM Shared Lines	Provides a list of all phones in the Cisco Unified Communications Manager with at least one shared line appearance.
Unified CM Table Count Summary	Provides a database centric view of data. This report proves useful for administrators or AXL API developers that understand database schema.
Unified CM User Device Count	Provides information about associated devices; for example, this report lists the number of phones with no users, the number of users with 1 phone, and the number of users with more than 1 phone.
Unified CM Voice Mail	Provides a summary of voice-messaging related configuration in the Cisco Unified Communications Manager Administration; for example, this report lists the number of configured voice mail ports, the number of message waiting indicators, the number of configured voice messaging profiles, the number of directory numbers that are associated with voice message profiles, and so on.
Unified CM Device Distribution Summary	Provides a summary of how devices are distributed throughout the cluster; for example, this report shows which devices are associated with the primary, secondary, tertiary servers and so on.

Cisco Unified IP Phones

The Cisco Unified IP Phone user guides were not updated for Cisco Unified Communications Manager Release 7.1. For more information on the Cisco Unified IP Phone user guides for Cisco Unified Communications Manager Release 6.1(3) and Cisco Unified Communications Manager Release 7.0(1), go to the following URL:

http://www.cisco.com/en/US/products/hw/phones/ps379/products_user_guide_list.html

This section provides descriptions and configuration information for the following features:

- Barge Tone Enhancements, page 127
- Cisco Unified IP Phone Support HTTPS, page 127
- Hold Status, page 128
- Internet Protocol Version 6 on the Cisco Unified IP Phone, page 129

- Line Select, page 145
- Missed Calls, page 145
- Off-Hook Abbreviated Dialing, page 146
- Restrict Unconfigured Phone Registration, page 148
- Secure Icon, page 148
- WebDialer Enhancements, page 149

Barge Tone Enhancements

The Party Entrance Tone configuration is available as a per-line setting, in *addition* to a service parameter setting for Cisco Unified CM administrators. The default value for the line setting specifies the service parameter setting. The Party Entrance Tone setting gets applied to Barge, cBarge, Join, Ad-hoc, and Meet Me conferences. For more information, see the "Party Entrance Tone" section on page 88.

Barge and cBarge supports the interaction with Private Line Automatic Ringdown (PLAR). When a shared line has PLAR configured, a user can Barge or cBarge into a call connected on the shared PLAR line.

These Barge Tone enhancements are supported on the following SIP and SCCP phones:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G

Where to Find More Information

- *Cisco Unified IP Phone Guide*

Cisco Unified IP Phone Support HTTPS

Cisco Unified IP Phones can securely access the web with the use of a phone trust store called "phone-trust." Administrators can upload certificates to a phone-trust store by using the Cisco Unified Communications Manager Operating System GUI. The Cisco Unified IP Phone will display a menu option called "Application Server" for each phone-trust store whose certificates have been uploaded into Cisco Unified OS Administration and later downloaded into the Cisco Unified IP Phone CTL file.

The phone-trust certificates and secure HTTPS web access are supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Administration Guide*
- *Cisco Unified Communications Operating System Administration Guide*
- *Cisco Unified Communication Manager Security Guide*

Hold Status

Cisco Unified Communications Manager 6.1(3) and 7.1(1) introduced the following enhancements to hold status:

- The Hold Status feature allows phones with a shared line to distinguish whether the local user placed the call on hold, or a remote (shared line) user placed the call on hold.
- If two phone users share a line and one user places a call on hold, that user's phone displays the local hold icon while the other user's phone displays the remote hold icon. In addition, on the Cisco Unified IP Phone 7906G and 7911G, the hold button is solid red on the local and remote phone. On all other supported phones, the local phone LED flashes green and the remote phone user's LED flashes green.

The hold status enhancement is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G

- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*

Internet Protocol Version 6 on the Cisco Unified IP Phone

The Cisco Unified IP Phone uses the internet protocol to provide voice communication over the network. Previous to Cisco Unified Communications Manager release 7.1, only the internet protocol version 4 (IPv4) was supported. Because it uses a 32-bit address, IPv4 cannot meet the increased demands for unique IP addresses for all devices that can connect to the internet. Internet Protocol version 6 (IPv6) is an updated version of the current Internet Protocol, IPv4. IPv6 uses a 128-bit address and provides end-to-end security capabilities, enhanced Quality of Service (QoS), and increased number of available IP addresses.

The Cisco Unified IP Phone supports IPv4 only addressing mode, IPv6 only addressing mode, as well as an IPv4/IPv6 dual stack addressing mode. In IPv4, you can enter each octet of the IP address on the phone in dotted decimal notation; for example, 192.240.22.5. In IPv6, you can enter each octet of the IP address in hexadecimal notation with each octet separated by a colon; for example, 2005:db8:0:1:ef8:9876:ba72:dc9a. The phone truncates and removes leading zeros when it displays the IPv6 address.

Cisco Unified IP Phones support both IPv4 and an IPv6 address transparently, so users can handle all calls on the phone to which they are accustomed. Cisco Unified IP Phones support the use of IPv6 only with Cisco Unified Communications Manager release 7.1 and only with the Skinny Call Control Protocol (SCCP).

Cisco Unified IP Phones do not support URLs with IPv6 addresses in the URL. This affects all IP Phone Service URLs, including services, directories, messages, help, and any restricted web services that require the phone to use the HTTP protocol to validate the credentials with the Authentication URL. If you configure Cisco Unified IP Phone services for Cisco IP Phones, you must configure the phone and the servers that support the phone service with IPv4 addresses.

If you configure IPv6 Only as the IP Addressing Mode for phones that are running SIP, the Cisco TFTP service overrides the IP Addressing Mode configuration and uses IPv4 Only in the configuration file.

For more information on deploying IPv6 in your Cisco Unified Communications network, refer to the "Internet Protocol Version 6 (IPv6)" chapter in *Cisco Unified Communications Manager Features and Services Guide* and *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1*.

Accessing IPv6 and IPv4 Configuration Settings in Cisco Unified IP Phone Menus

Table 28 describes the IPv6 and IPv4 settings that are in Cisco Unified IP Phone menus.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus

Configuration Setting	Purpose	Description
Settings > Network Configuration Menu		
IPv4 Configuration	Internet Protocol v4 address menu. In the IPv4 Configuration menu, you can do the following: • Enable or disable the phone to use the IPv4 address that is assigned by the DHCPv4 server. • Manually set the IPv4 Address, Subnet Mask, Default Routers, DNSv4 Server, and Alternate TFTP servers for IPv4. For more information on the IPv4 address fields, refer to the specific field within this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to IPv4 Configuration and press the **Select** softkey.
IPv6 Configuration	Internet Protocol v6 address menu. In the IPv6 Configuration menu, you can do the following: • Enable or disable the phone to use the IPv6 address that is assigned by the DHCPv6 server or to use the IPv6 address that it acquires through Stateless Address Autoconfiguration (SLAAC). • Manually set the IPv6 Address, Subnet Prefix Length, DNSv6 Server, and IPv6 TFTP Servers. For more information on the IPv6 address fields, refer to the specific field within this table. For more information on SLAAC, refer to *Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager 7.1*.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to IPv6 Configuration and press the **Select** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides. **Note** If the phone receives different domain names from the DHCPv4 and DHCPv6 servers, the domain name from the DHCPv6 will take precedence.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Disable DHCP. If the IP Addressing mode is configured for IPv4 only, set the DHCP option to **No**. If the IP Addressing mode is configured for IPv6 only, set the DHCPv6 option to **No**. If the IP Addressing mode is configured for both IPv4 and IPv6, set both DHCP option and DHCPv6 to **No**. 3. Scroll to the Domain Name option, press the **Edit** softkey, and then enter a new domain name. 4. Press the **Validate** softkey and then press the **Save** softkey.
Settings > Network Configuration Menu > IPv4 Configuration Menu		
DHCP	Indicates whether the phone has DHCP enabled or disabled. When DHCP is enabled, the DHCP server assigns the phone anIPv4 address. When DHCP is disabled, the administrator must manually assign an IPv4 address to the phone.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCP option and press the **No** softkey to disable DHCP, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IP Address	Internet Protocol version 4 (IPv4) address of the phone. If you assign an IPv4 address with this option, you must also assign a subnet mask and default router. See the Subnet Mask and Default Router options in this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
Subnet Mask	Subnet mask used by the phone.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to No. 3. Scroll to the Subnet Mask option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.
Default Router 1 Default Router 2 Default Router 3 Default Router 4 Default Router 5	Default router used by the phone (Default Router 1) and optional backup routers (Default Router 2–5).	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to No. 3. Scroll to the appropriate Default Router option, press the **Edit** softkey, and then enter a new router IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup routers. 6. Press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
DNS Server 1 DNS Server 2 DNS Server 3 DNS Server 4 DNS Server 5	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2–5) used by the phone.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCP option to No. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign backup DNS servers. 6. Press the **Save** softkey.
DHCP Server	IP address of the Dynamic Host Configuration Protocol (DHCP) server from which the phone obtains its IPv4 address.	Display only—Cannot configure.
DHCP Address Released	Releases the IPv4 address that was assigned by the DHCP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCP Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Alternate TFTP	Indicates whether the phone is using an alternate TFTP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the Alternate TFTP option and press the **Yes** softkey if the phone should use an alternate TFTP server. 3. Press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
TFTP Server 1	Primary Trivial File Transfer Protocol (TFTP) server used by the phone with an IPv4 address. If you are not using DHCPv4 in your network and you want to change this server, you must use the TFTP Server 1 option. If you set the Alternate TFTP option to yes or disable DHCP, you must enter a non-zero value for the TFTP Server 1 option. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 1 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 1 option. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Any manually assigned IPv6 TFTP Servers • Any manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. If DHCP is enabled, set the Alternate TFTP option to Yes. 3. Scroll to the TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
TFTP Server 2	Optional backup TFTP server that the phone with an IPv4 address uses if the primary TFTP server is unavailable. If neither the primary TFTP server nor the backup TFTP server is listed in the CTL file on the phone, you must unlock the CTL file before you can save changes to the TFTP Server 2 option. In this case, the phone will delete the CTL file when you save changes to the TFTP Server 2 option. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Manually assigned IPv6 TFTP Servers • Manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the TFTP Server 1 option. 4. Scroll to the TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey.
BOOTP Server	Indicates whether the phone obtains its configuration from a Bootstrap Protocol (BootP) server instead of from a DHCP server.	Display only—Cannot configure.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
Settings > Network Configuration Menu > IPv6 Configuration Menu		
DHCPv6	Indicates whether the phone has DHCPv6 enabled or disabled. When DHCPv6 is enabled, the DHCPv6 server assigns the phone an IPv6 address. When DHCP v6 is disabled, the administrator must manually assign an IPv6 address to the phone. The DHCPv6 setting along with the Auto IP Configuration setting determine how the IP Phone obtains its network settings. For more information on how these two settings affect the network settings on the phone, see Table 14 (Determining Where a Phone Acquires its Network Settings).	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCPv6 option and press the **No** softkey to disable DHCPv6, or press the **Yes** softkey to enable DHCP. 3. Press the **Save** softkey.
IPv6 Address	Internet Protocol version 6 (IPv6) address of the phone. The IPv6 address is a 128 bit address. If you assign an IP address with this option, you must also assign the IPv6 prefix length. See the IPv6 Subnet Prefix options in this table.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IP Address option, press the **Edit** softkey, and then enter a new IP Address. 4. Press the **Validate** softkey and then press the **Save** softkey.
IPv6 Prefix Length	Subnet prefix length that is used by the phone. The subnet prefix length is a decimal value from 1-128, that specifies the portion of the IPv6 address that comprises the subnet.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to **No**. 3. Scroll to the IPv6 Prefix Length option, press the **Edit** softkey, and then enter a new subnet mask. 4. Press the **Validate** softkey and then press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Default Router 1	Default router used by the phone (Default Router 1). **Note** The phone obtains information on the default router from IPv6 Router Advertisements.	Display only—Cannot configure.
IPv6 DNS Server 1 IPv6 DNS Server 2	Primary Domain Name System (DNS) server (DNS Server 1) and optional backup DNS servers (DNS Server 2) used by the phone. If your configuration includes both DNSv6 and DNSv4 servers, the phone will look for its DNS server in the following order: • IPv6 DNS Server 1 • IPv6 DNS Server 2 • DNS Server 1-5 for IPv4 (respectively)	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Set the DHCPv6 option to No. 3. Scroll to the appropriate DNS Server option, press the **Edit** softkey, and then enter a new DNS server IP address. 4. Press the **Validate** softkey. 5. Repeat Steps 3 and 4 as needed to assign the backup DNS server. 6. Press the **Save** softkey.
IPv6 Address Released	Releases the IPv6 address that the phone has acquired from the DHCPv6 server or by stateless address autoconfiguration. **Note** This field is only editable when the DHCPv6 option is enabled.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the DHCPv6 Address Released option and press the **Yes** softkey to release the IP address assigned by DHCP, or press the **No** softkey if you do not want to release this IP address. 3. Press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Alternate TFTP	Indicates whether the phone is using the IPv6 Alternate TFTP server.	1. Unlock network configuration options by pressing **#. **Note** Pressing **# either locks or unlocks the options, depending on the previous state. 2. Scroll to the IPv6 Alternate TFTP option and press the **Yes** softkey if the phone should use an alternate TFTP server. 3. Press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 TFTP Server 1 (SCCP phones only)	Primary IPv6 Trivial File Transfer Protocol (TFTP) server used by the phone. If you are not using DHCPv6 in your network and you want to change this server, you must use the IPv6 TFTP Server 1 option. If you set the IPv6 Alternate TFTP option to yes or you disable DHCPv6, you must enter a non-zero value for the IPv6 TFTP Server 1 option. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Manually assigned IPv6 TFTP Servers • Manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. If DHCPv6 is enabled, set the IPv6 Alternate TFTP option to **Yes**. 3. Scroll to the IPv6 TFTP Server 1 option, press the **Edit** softkey, and then enter a new TFTP server IP address. 4. Press the **Validate** softkey, and then press the **Save** softkey.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 TFTP Server 2 (for SCCP phones only)	Optional backup IPv6 TFTP server that the phone uses if the primary IPv6 TFTP server is unavailable. If you make changes to the Alternate TFTP or IPv6 TFTP servers, you must first unlock the CTL file on the phone. When the phone looks for its TFTP server, it gives precedence to manually assigned TFTP servers, regardless of the protocol. If your configuration includes both IPv6 and IPv4 TFTP servers, the phone prioritizes the order that it looks for its TFTP server by giving priority to manually assigned IPv6 TFTP servers and IPv4 TFTP servers. The phone looks for its TFTP server in the following order: • Manually assigned IPv6 TFTP Servers • Manually assigned IPv4 TFTP Servers • DHCPv6 assigned TFTP Servers • DHCP assigned TFTP Servers For information about the CTL file, refer to *Cisco Unified Communications Manager Security Guide*. For information about unlocking the CTL file, refer to the "Security Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.	1. Unlock the CTL file, if necessary. 2. Unlock network configuration options. 3. Enter an IP address for the IPv6 TFTP Server 1 option. 4. Scroll to the IPv6 TFTP Server 2 option, press the **Edit** softkey, and then enter a new backup TFTP server IP address. 5. Press the **Validate** softkey, and then press the **Save** softkey.
Settings > Device Configuration > Network Configuration Menu		
IP Addressing Mode	Displays whether the IP addressing mode that is available on the phone—IPv4 only, IPv6 only, or Both (IPv4 and IPv6).	Display only—Cannot configure.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IP Preference Mode Control	Indicates the IP address version that the phone uses during signaling with Cisco Unified Communications Manager when both IPv4 and IPv6 are both available on the phone. The IP addressing mode preference is configured on Cisco Unified Communications Manager Administration.	Display only—Cannot configure. Displays one of the following options: • IPv4—The dual-stack phone prefers to establish a connection via an IPv4 address during a signaling event • IPv6—The dual-stack phone prefers to establish a connection via an IPv6 address during a signaling event.
Auto IP Configuration	Displays whether the auto configurations is enabled or disabled on the phone. The Auto IP Configuration setting along with the DHCPv6 setting determine how the IP Phone obtains its IPv6 address and other network settings. For more information on how these two settings affect the network settings on the phone, see Table 14 (Determining Where a Phone Acquires its Network Settings). **Note** Use the "Allow Auto-Configuration for Phones" setting in Cisco Unified Communications Manager Administration.	Display only—Cannot configure.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 Load Server	Used to optimize installation time for phone firmware upgrades and off load the WAN by storing images locally, negating the need to traverse the WAN link for each phone's upgrade. You can set the Load Server to another TFTP server IP address or name (other than the IPv6 TFTP Server 1 or IPv6 TFTP Server 2) from which the phone firmware can be retrieved for phone upgrades. When the Load Server option is set, the phone contacts the designated server for the firmware upgrade. **Note** The Load Server option allows you to specify an alternate TFTP server for phone upgrades only. The phone continues to use IPv6 TFTP Server 1 or IPv6 TFTP Server 2 to obtain configuration files. The Load Server option does not provide management of the process and of the files, such as file transfer, compression, or deletion. **Note** When you configure both an IPv6 Load Server and a Load Server (for IPv4), the IPv6 Load server takes precedence.	Display only—Cannot configure.
IPv6 Log Server	Indicates the IP address and port of the remote logging machine to which the phone sends log messages. These log messages help in debugging the peer to peer image distribution feature. **Note** The remote logging setting does not affect the sharing log messages sent to the phone log.	Display only—Cannot configure.
Settings > Security Configuration Menu		
CAPF Server	Displays the IP address and the port of the IPv4 CAPF server that the phone uses.	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.

Table 28 IPv4 and IPv6 Settings in Cisco Unified IP Phone Menus (continued)

Configuration Setting	Purpose	Description
IPv6 CAPF Server	Displays the IP address and the port of the IPv6 CAPF server that the phone uses.This menu setting is disabled in this release. If your configuration includes both IPv6 CAPF Server and IPv4 CAPF server, the phone will look for its CAPF server in the following order: • IPv6 CAPF Server • IPv4 CAPF Server	For more information about this server, refer to the "Using the Certificate Authority Proxy Function" section in *Cisco Unified Communications Manager Security Guide*.
Settings > Status > Network Statistics		
IPv6		Displays information on the DHCPv6 status.

The IPv6 feature is supported on the following Cisco Unified IP Phones (SCCP):

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G

For More Information

- "Internet Protocol Version 6 (IPv6)," *Cisco Unified Communications Manager Features and Services Guide*
- Phone Considerations, page 53
- Updates for the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager (SCCP and SIP), page 156

Line Select

Cisco Unified Communications Manager 6.1(3) and 7.1(1) introduced settings to determine whether the primary line is automatically selected when answering a call, or when the Messages button is pressed. These settings can be made for all phones in the system, or for a single phone.

- **Line Select (Always use Prime line)**—If this feature is disabled (default), then the ringing line is selected. When enabled, the primary line is picked up even if a call is ringing on another line. The User must manually select the other line.
- **Line Select for Voice Messages (Always use Prime line for Voice Message)**—When disabled (default), pressing the Messages button connects to the line that has a voice message. If more than one line has voice mail, then the first available line is selected. When enabled, the primary line is always used to retrieve voice messages.

Note The primary line settings are also available for phones using Extension Mobility.

These enhancements are supported on the following SIP and SCCP phones:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G (SCCP only)

Where to Find More Information

- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*
- *Cisco Unified Communications Manager Administration Guide*

Missed Calls

The missed calls feature allows the phone administrator to specify whether missed calls will be logged in the missed calls directory for a given line appearance. The following properties apply to the missed calls feature:

- The line can be a directory number or shared line. The default behavior is to log all missed calls on all lines.
- Missed call logging operates on a line basis. The line can be a directory number or a shared line.

- If the phone administrator configures a line appearance (share or non-shared), so that missed calls are not logged, then calls to that line are never logged in the missed call log directory, even if the calls were eventually forwarded due to no answer.
- If more than one line key gets configured on a phone, logging missed calls is dependent on the missed call log setting for each line.
- Missed call logging is controlled by an on/off configuration parameter that is sent to the phone in the configuration file.
- The Missed Calls Log configuration does not affect any existing or previous call log items.
- Calls on lines that are not logged do not affect the New Missed Call status message.
- If the phone administrator turns off the missed calls feature on the configured line appearance, the missed calls are not listed in the missed call history on that line appearance.

In addition to these properties, the following properties continue to apply all calls:

- All calls received on a phone appear in the Received Calls log, regardless of the line on which they were received.
- All calls made from a phone appear in the Placed Calls log, regardless of whether they were placed from a shared or primary line.

The missed calls feature is supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Guide*
- *Cisco Unified IP Phone Administration Guide*

Off-Hook Abbreviated Dialing

Cisco Unified Communications Manager release 7.1 introduces Off-Hook Abbreviated Dialing. The user can initiate Off-Hook Abbreviated Dialing while conferencing a call, while transferring a call, or while placing a new call after putting a call on hold.

Cisco Unified Communications Manager Configuration Tips

- Assign the softkey, **AbbrDial**, to the IP Phone by using Softkey Template Configuration. The following phone states apply: Offhook, Offhook with Feature, and Digits After First.

User Tips

Table 29 provides the procedure for using off-hook abbreviated dialing.

Table 29 How to Use Off-hook Abbrievated Dialing

If you want to...	Then...
Use Abbreviated Dialing (Off-hook)	1. Pickup the handset. 2. Press the **AbbrDial** softkey and enter the abbreviated dial code using the keypad. 3. Press the **AbbrDial** softkey again. To use Off-hook Abbreviated Dialing to conference a call: 1. Press the **Confrn** softkey. The user will hear dial tone. 2. Follow steps 2 and 3 above. 3. Press the **Confrn** softkey again. To use Off-hook Abbreviated Dialing to transfer a call: 1. Press the **Transfer** softkey. The user will hear dial tone. 2. Follow steps 2 and 3 above. 3. Press the **Transfer** softkey again. To use Off-hook Abbreviated Dialing while a call is on hold: 1. Press the **NewCall** softkey. 2. Follow steps 2 and 3 above.

The Off-Hook Abbreviated Dialing feature is supported on the following SIP and SCCP phones:

- Cisco Unified IP Phone 7975G
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7906G

For More Information

- "Cisco Unified IP Phone Configuration," *Cisco Unified Communications Manager Administration Guide*

- "Softkey Template Configuration," *Cisco Unified Communications Manager Administration Guide*
- "Cisco Unified IP Phone," *Cisco Unified Communications Manager System Guide*

Restrict Unconfigured Phone Registration

In Cisco Unified Communications Manager releases other than 6.1(3) and 7.1(1), if a Cisco Unified IP Phone had not been added to the Cisco Unified Communications Manager database and did not have auto-registration enabled, the phone would repeatedly attempt to register (unsuccessfully) with Cisco Unified Communications Manager, thus continually notifying Cisco Unified Communications Manager with these repeated registration requests.

With Cisco Unified Communications Manager 6.1(3) and 7.1(1), if auto-registration is not enabled, and the phone has not been added to the Cisco Unified Communications Manager database, the phone will not attempt to register with Cisco Unified Communications Manager. The phone will continue to display the "Configuring IP" message until auto-registration has been enabled, or until the phone has been added to the Cisco Unified Communications Manager database.

The registration behavior is supported on the following SCCP and SIP phones and devices:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)
- Cisco Unified IP Phone 7941G
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G
- Cisco Unified IP Phone 7971G
- Cisco Unified IP Phone 7975G
- Cisco Analog Telephone Adapter
- VG248 Gateways

Where to Find More Information

- *Cisco Unified IP Phone Administration Guide*
- *Cisco Unified Communications Manager Administration Guide*

Secure Icon

Cisco Unified Communications Manager release 7.1 uses a different method to calculate which Security icon to send to Cisco Unified IP Phones. Prior to release 7.1, the type of Security icon that Cisco Unified Communications Manager sent to IP Phones was based solely on the audio stream involved in a call or conference. However, in Cisco Unified Communications Manager Release 7.1, Cisco Unified Communications Manager calculates which Security icon to display based on both audio and video (if applicable) streams, and sends the resulting Security icon to the Cisco Unified IP Phone.

All media involved in the call must be secure in order for the Lock (Encrypted) icon to display on the phone. For example, if the audio is encrypted but the video is not encrypted, the Security icon displayed will not be the Lock (Encrypted) icon because the call as a whole is not encrypted. Instead, the Shield (Authenticated) icon, if one exists for the given phone model, displays on the phone. For phones that do not support Shield icons, these phones will not display any Security icon for an Authenticated call or conference.

For a table which shows which type of security icon to expect for various call scenarios, see the *Cisco Unified Communications Manager Security Guide,* "Security Icons" section.

New Behavior for Secure-Tone Feature

In releases prior to Cisco Unified Communications Manager Release 7.1, a security tone would play to indicate that a call was "protected," which meant that two phones on a call were configured for Protected mode and that the phones were receiving and transmitting encrypted audio. Beginning with Cisco Unified Communications Manager Release 7.1, if a video stream is also involved in the call, the security tone will play only if both phones are receiving and transmitting encrypted video as well as encrypted audio.

For More Information

- *Cisco Unified IP Phone Administration Guide*
- *Cisco Unified Communications Manager Security Guide*

WebDialer Enhancements

Cisco Unified Communications Manager supports the following WebDialer enhancements:

- Changing the WebDialer database location—The list of WebDialers will be moved from the Service Parameter Configuration window in Cisco Unified Communications Manager, to be node-specific on the Application Server Configuration window. The Application Server Configuration window will be updated to enable sorting by application server type and node.

  For more information on this topic, see the "Cisco Web Dialer Configured in Application Server Window" section on page 31.
- Preferred Device menu name change—On the Cisco WebDialer Make Call page, the "Use permanent device" is changed to display "Use preferred device". When there is only one preferred device available, the MAC address will not be displayed in the menu. MAC addresses will only be displayed if there are two or more devices of the same type assigned to the user.
- Merging the Preferences and Make Call pages together—The Cisco WebDialer Preferences page options will now be available from the Cisco WebDialer Make Call page.
- Integration with Extension Mobility—If the user has an Extension Mobility profile, then an option labeled "Use my Extension Mobility logged in device" will be available from the Preferred Device menu.
- Dialog changes for Hang-Up UI—Changes the text on the Hang-Up UI to say:

  Calling <Username if available> at <dial-out number>

  If authorization codes are required, enter them now

The WebDialer enhancements are supported on the following SCCP and SIP phones:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7931G (SCCP only)

- Cisco Unified IP Phone 7941G/GE
- Cisco Unified IP Phone 7942G
- Cisco Unified IP Phone 7945G
- Cisco Unified IP Phone 7961G/GE
- Cisco Unified IP Phone 7962G
- Cisco Unified IP Phone 7965G
- Cisco Unified IP Phone 7970G-GE
- Cisco Unified IP Phone 7971G-GE
- Cisco Unified IP Phone 7975G

Where to Find More Information

- *Cisco Unified IP Phone Guide*

Table 30 lists Cisco Unified IP Phones that support new Cisco Unified Communications Manager features.

Table 30 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Barge Tone Enhancements	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Barge Tone Enhancements, page 127

Table 30 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features (continued)

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Cisco Unified IP Phone Support HTTPS	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Cisco Unified IP Phone Support HTTPS, page 127
Hold Status	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Hold Status, page 128
Internet Protocol Version 6 (IPv6)	SCCP only 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931 7911G 7906G	Internet Protocol Version 6 on the Cisco Unified IP Phone, page 129

Table 30 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features (continued)

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Line Select	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Line Select, page 145
Missed Calls	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Missed Calls, page 145
Off Hook Abbreviated Dialing	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Off-Hook Abbreviated Dialing, page 146

Table 30 Cisco Unified IP Phone Support for Cisco Unified Communications Manager Features (continued)

Cisco Unified Communications Manager Feature	Cisco Unified IP Phone Support	For more information, see
Restrict Unconfigured Phone Registration	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	Restrict Unconfigured Phone Registration, page 148
Secure Icon	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7931G 7911G 7906G	Secure Icon, page 148
WebDialer Enhancements	SCCP and SIP 7975G 7971G-GE 7970G 7965G 7962G 7961G 7961G-GE 7945G 7942G 7941G 7941G-GE 7911G 7906G SCCP only 7931G	WebDialer Enhancements, page 149

Cisco Unified CM User Options

See the following sections for enhancements to the Cisco Unified CM User Options:

- Logging Missed Calls For Shared Lines, page 74
- WebDialer Enhancements, page 149

Documentation Updates

This section contains information on documentation omissions, errors, and updates for the following 7.1(1) documentation:

- Cisco Unified Communications Manager Administration, page 154
- Cisco Unified Communications Manager CDR Analysis and Reporting, page 155
- Cisco Unified IP Phones, page 156
- Cisco Unified Communications Manager Assistant, page 163

Cisco Unified Communications Manager Administration

This section contains documentation updates, errors, and omissions for the *Cisco Unified Communications Manager Administration Guide*, *Cisco Unified Communications Manager System Guide*, and *Cisco Unified Communications Manager Features and Services Guide*.

IPv6 Chapter Contains Incorrect Information

The *Cisco Unified Communications Manager Administration Guide* and "Internet Protocol Version 6 (IPv6)" chapter in the *Cisco Unified Communications Manager Features and Services Guide* contain incorrect information on DNS and the Allow Auto-Configuration of Phones configuration setting. Disregard the incorrect information in the guides and use the corrected information in the following paragraphs.

Incorrect Information on DNS

Configure DNS for IPv6 after the upgrade to Cisco Unified Communications Manager 7.1. Do not configure DNS for IPv6 before the upgrade; otherwise, the upgrade fails.

Correct Information on DNS

You can provision your DNS server for IPv6 prior to upgrading from Cisco Unified Communications Manager Release 7.0(1) to Release 7.1(1). However, do not configure the DNS records for Cisco Unified Communications Manager for IPv6 until after you upgrade to Release 7.1(1). Configuring the DNS records for Cisco Unified Communications Manager for IPv6 prior to upgrading to Release 7.1(1) causes the upgrade to fail and causes your system to become nonfunctional after you reboot.

Incorrect Information on Allow Auto-Configuration of Phones

This drop-down list box supports IPv6 for dual-stack Cisco Unified IP Phones that run SCCP. From the drop-down list box, choose one of the following options:

- On—The phone uses the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address.

Phones also require a TFTP server address to register with Cisco Unified Communications Manager. You can manually configure the TFTP server address via the interface on the phone, or you can obtain it from a DHCPv6 server.

Tip To indicate to the phone that it needs to use the DHCPv6 server to obtain other information, ensure that the O bit is set in the router assignment on the router.

- Off—The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server.

Tip Ensure that the M (Managed address configuration) bit/ flag is also set in the router assignment on the router, which indicates that the phone should use DHCP for all addressing information.

- Default—To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option.

Correct Information on Allow Auto-Configuration of Phones

The options in this drop-down list box apply to IPv6 for dual-stack Cisco Unified IP Phones that run SCCP. From the drop-down list box, choose one of the following options:

- On—The phone uses the IPv6 Network ID that is advertised in the Router Advertisements (RAs) to autoconfigure its IPv6 address.

  Phones also require a TFTP server address to register with Cisco Unified Communications Manager. It is recommended that you obtain the TFTP server address from a DHCPv6 server, although you can manually configure the TFTP server address via the interface on the phone.

  To indicate to the phone that it needs to use the DHCPv6 server to obtain other information, ensure that the O (Other information) bit /flag is set in the Router Assignments that is sent by the link local router.

- Off—The phone obtains its IPv6 address and TFTP server address from the DHCPv6 server.

Tip Ensure that the M (Managed address configuration) bit/ flag is set in the Router Advertisements that is sent by the link local router, which indicates that the phone should use DHCP for all addressing information.

- Default—To use the configuration for the Allow Auto-Configuration for Phones enterprise parameter, choose this option.

Cisco Unified Communications Manager CDR Analysis and Reporting

This section contains information on documentation omissions, errors, and updates for Cisco Unified Communications Manager CDR Analysis and Reporting.

- Configuring Department Bills Users Reports, page 155

Configuring Department Bills Users Reports

The following note has been added to Step 6 of the Configuring Department Bills Reports procedure:

Click the **Down** radio button to view your direct reports. Use the **Up** and **Down** radio buttons to move up and down the report chain.

Cisco Unified IP Phones

This section contains documentation updates, errors, and omissions for Cisco Unified IP Phone documentation.

Updates for the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager (SCCP and SIP)

This section includes the following documentation updates for the Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager (SCCP and SIP):

- Chapter 1, "An Overview of the Cisco Unified IP Phone," Checklist for Configuring the Cisco Unified IP Phones 79XX series for Cisco Unified Communications Manager, page 156
- Chapter 1, "An Overview of the Cisco Unified IP Phone," Checklist for Installing the Cisco Unified IP Phone 797XX Series, page 159

Chapter 1, "An Overview of the Cisco Unified IP Phone," Checklist for Configuring the Cisco Unified IP Phones 79XX series for Cisco Unified Communications Manager

Table 31 replaces Table 1-6, Checklist for Configuring the Cisco Unified IP Phones for Cisco Unified Communications Manager.

C

Table 31 Checklist for Configuring the Cisco Unified IP Phones for Cisco Unified Communications Manager

Task	Purpose	For More Information
1.	Gather the following information about the phone: • Phone Model • MAC address • Physical location of the phone • Name or user ID of phone user • Device pool • Partition, calling search space, and location information • Number of lines and associated directory numbers (DNs) to assign to the phone • Cisco Unified Communications Manager user to associate with the phone • Phone usage information that affects phone button template, softkey template, phone features, IP Phone services, or phone applications Provides list of configuration requirements for setting up phones. Identifies preliminary configuration that you need to perform before configuring individual phones, such as phone button templates or softkey templates.	Refer to *Cisco Unified Communications Manager System Guide,* "Cisco Unified IP Phone" chapter. Refer to the "Telephony Features Available for the Phone" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
2.	Customize phone button templates (if required). Changes the number of line buttons, speed-dial buttons, Service URL buttons or adds a Privacy button to meet user needs. You must specify a service URL with an IPv4 address.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Phone Button Template Configuration" chapter. Refer to the "Modifying Phone Button Templates" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
3.	Add and configure the phone by completing the required fields in the Phone Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, MAC address and device pool. Adds the device with its default settings to the Cisco Unified Communications Manager database.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter. For information about Product Specific Configuration fields, refer to "?" Button Help in the Phone Configuration window.
4.	Add and configure directory numbers (lines) on the phone by completing the required fields in the Directory Number Configuration window. Required fields are indicated by an asterisk (*) next to the field name; for example, directory number and presence group. Adds primary and secondary directory numbers and features associated with directory numbers to the phone.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Directory Number Configuration" chapter, "Creating a Cisco Unity Voice Mailbox" section. Refer to the "Telephony Features Available for the Phone" section in the corresponding *Cisco Unified IP Phone Administration Guide*.

Table 31 Checklist for Configuring the Cisco Unified IP Phones for Cisco Unified Communications Manager

Task	Purpose	For More Information
5.	Customize softkey templates. Adds, deletes, or changes order of softkey features that display on the user's phone to meet feature usage needs.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Softkey Template Configuration" chapter. Refer to the "Configuring Softkey Templates" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
6.	Configure speed-dial buttons and assign speed-dial numbers (optional). Adds speed-dial buttons and numbers. **Note** Users can change speed-dial settings on their phones by using Cisco Unified CM User Options.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Configuring Speed-Dial Buttons" section.
7.	Configure Cisco Unified IP Phone services and assign services (optional). Provides IP Phone services. **Note** Users can add or change services on their phones by using the Cisco Unified CM User Options web pages. **Note** You must specify a service URL with an IPv4 address	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Services Configuration" chapter. Refer to the "Setting Up Services" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
8.	Assign services to phone buttons (optional). Provides single button access to an IP phone service or URL.	Refer to *Cisco Unified Communications Manager Administration Guide*, "Cisco Unified IP Phone Configuration" chapter, "Adding a Cisco Unified IP Phone Service to a Phone Button" section.
9.	Add user information by configuring required fields. Required fields are indicated by an asterisk (*); for example, User ID and last name. **Note** Assign a password (for User Options web pages) and PIN (for Extension Mobility and Personal Directory) Adds user information to the global directory for Cisco Unified Communications Manager.	Refer to *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter. Refer to the "Adding Users to Cisco Unified Communications Manager" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
10.	Associate a user to a user group. Assigns users a common list of roles and permissions that apply to all users in a user group. Administrators can manage user groups, roles, and permissions to control the level of access (and, therefore, the level of security) for system users.	Refer to the *Cisco Unified Communications Manager Administration Guide*: • "End User Configuration" chapter, "End User Configuration settings" section. • "User Group Configuration" chapter, "Adding Users to a User Group" section.
11.	Associate a user with a phone (optional). Provides users with control over their phone such as forwarding calls or adding speed-dial numbers or services. **Note** Some phones, such as those in conference rooms, do not have an associated user.	Refer to *Cisco Unified Communications Manager Administration Guide*, "End User Configuration" chapter, "Associating Devices to a User" section.

Chapter 1, "An Overview of the Cisco Unified IP Phone," Checklist for Installing the Cisco Unified IP Phone 797XX Series

Table 32 replaces Table 1-7, Checklist for Installing the Cisco Unified IP Phones f.

Table 32 Checklist for Installing the Cisco Unified IP Phones

Task	Purpose	For More Information
1.	Choose the power source for the phone: • Power over Ethernet (PoE) • External power supply Determines how the phone receives power.	Refer to the "Providing Power to the Phone" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
2.	Assemble the phone, adjust phone placement, and connect the network cable. Locates and installs the phone in the network.	Refer to the "Installing the Cisco Unified IP Phone" section in the corresponding *Cisco Unified IP Phone Administration Guide*. Refer to the "Adjusting the Placement of the Cisco Unified IP Phone" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
3.	Add a Cisco Unified IP Phone Expansion Module 7914 (optional). Extends functionality to a Cisco Unified IP Phone by adding 14 line appearances or speed dial numbers.	Refer to the "Attaching the Cisco Unified IP Phone Expansion Module 7914" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
4.	Monitor the phone startup process. Verifies that phone is configured properly.	Refer to the "Verifying the Phone Startup Process" section in the corresponding *Cisco Unified IP Phone Administration Guide*.

Table 32 Checklist for Installing the Cisco Unified IP Phones

Task	Purpose	For More Information
5.	If you are configuring the network settings on the phone for an IPv6 network, you can set up an IP address for the phone by either using DHCP or manually entering an IP address. Using DHCP—To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, choose **Settings > Network Configuration> IPv6 Configuration** and: • To enable DHCPv6,set DHCPv6 Enabled to **Yes.** DHCPv6 is enabled by default. • To use an alternate TFTP server, set IPv6 Alternate TFTP Server to **Yes**, and enter the IP address for IPv6 TFTP Server 1. **Note** Consult with the network administrator if you need to assign an alternative TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, subnet mask, TFTP server, and default router locally on the phone, choose **Settings > Network Configuration> IPv6 Configuration**: To disable DHCP and manually set an IP address: **a.** To disable DHCPv6, set DHCPv6 Enabled to **No**. **b.** Enter the static IP address for phone. **c.** Enter the IPv6 prefix length. **d.** Enter the IPv6 default router IP addresses. **e.** Set IPv6 Alternate TFTP Server to **Yes**, and enter IP address for IPv6 TFTP Server 1. You must also enter the domain name where the phone resides by Choosing **Settings > Network Configuration.** **Note** The Cisco Unified IP Phone supports having both IPv4 and an IPv6 address concurrently. You can configure Cisco Unified Communications Manager to support IPv4 addresses only, IPv6 addresses only, or support both IPv4/IPv6 addresses.	See the "Configuring Startup Network Settings" section in the *Cisco Unified IP Phone Administration Guide*. See the "Network Configuration Menu" section in the *Cisco Unified IP Phone Administration Guide*.

Table 32 Checklist for Installing the Cisco Unified IP Phones

Task	Purpose	For More Information
6.	When you are configuring the network settings on the phone, for an IPv4 network you can set up an IP address for the phone by either using DHCP or by manually entering an IP address. Using DHCP—To enable DHCP and allow the DHCP server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, choose **Settings > Network Configuration> IPv4 Configuration** and configure the following: • To enable DHCP, set DHCP to **Yes.** DHCP is enabled by default. • To use an alternate TFTP server, set Alternate TFTP Server to **Yes,** and enter the IP address for the TFTP Server. **Note** Consult with the network administrator if you need to assign an alternate TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, subnet mask, TFTP server, and default router locally on the phone, choose **Settings > Network Configuration> IPv4 Configuration**: To disable DHCP and manually set an IP address: **a.** To disable DHCP, set DHCP to **No**. **b.** Enter the static IP address for phone. **c.** Enter the subnet mask. **d.** Enter the default router IP addresses. **e.** Set Alternate TFTP Server to **Yes, and** enter the IP address for TFTP Server 1. You must also enter the domain name where the phone resides by Choosing **Settings > Network Configuration.** **Note** You can configure Cisco Unified Communications Manager to support IPv4 devices only, IPv6 devices only, or to support both IPv4 and IPv6 devices concurrently.	Refer to the "Configuring Startup Network Settings" section in the corresponding *Cisco Unified IP Phone Administration Guide*. Refer to the "Network Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.

Table 32 Checklist for Installing the Cisco Unified IP Phones

Task	Purpose	For More Information
7.	If you are configuring the network settings on the phone for an IPv6 network, you can set up an IP address for the phone by either using DHCPv6 or by manually entering an IP address. Using DHCPv6—To enable DHCPv6 and allow the DHCPv6 server to automatically assign an IP address to the Cisco Unified IP Phone and direct the phone to a TFTP server, choose **Settings > Network Configuration> IPv6 Configuration** and configure the following: • To enable DHCPv6, set DHCPv6 to **Yes.** DHCPv6 is enabled by default. • To use an alternate TFTP server, set IPv6 Alternate TFTP Server to **Yes**, and enter the IP address for IPv6 TFTP Server 1. **Note** Consult with the network administrator if you need to assign an alternate TFTP server instead of using the TFTP server assigned by DHCP. Without DHCP—You must configure the IP address, subnet mask and TFTP server locally on the phone, choose **Settings > Network Configuration> IPv6 Configuration**: To disable DHCP and manually set an IP address: **a.** To disable DHCPv6, set DHCPv6 to **No**. **b.** Enter the static IP address for phone. **c.** Enter the IPv6 prefix length. **d.** Set IPv6 Alternate TFTP Server to **Yes**, and enter IP address for IPv6 TFTP Server 1. You must also enter the domain name where the phone resides by Choosing **Settings > Network Configuration.** **Note** You can configure Cisco Unified Communications Manager to support IPv4 devices only, IPv6 devices only, or to support both IPv4 and IPv6 devices concurrently.	Refer to the "Configuring Startup Network Settings" section in the corresponding *Cisco Unified IP Phone Administration Guide*. Refer to the "Network Configuration Menu" section in the corresponding *Cisco Unified IP Phone Administration Guide*.
8.	Set up security on the phone. Provides protection against data tampering threats and identity theft of phones.	Refer to the "Configuring Security on the Cisco Unified IP Phone" section in the corresponding *Cisco Unified IP Phone Administration Guide*.

Table 32 Checklist for Installing the Cisco Unified IP Phones

Task	Purpose	For More Information
9.	Make calls with the Cisco Unified IP Phone. Verifies that the phone and features work correctly.	Refer to the corresponding *Cisco Unified IP Phone Guide*.
10.	Provide information to end users about how to use their phones and how to configure their phone options. Ensures that users have adequate information to successfully use their Cisco Unified IP Phones.	Refer to the "Providing Information to Users Via a Website" appendix in the corresponding *Cisco Unified IP Phone Administration Guide*.

Cisco Unified Communications Manager Assistant

This section contains documentation errors, omissions, and updates for the *Cisco Unified Communications Manager Assistant User Guide*.

Cisco Unified Communications Manager Assistant User Guide for Cisco Unified Communications Manager 6.0

Consider the following note.

If the Assistant is configured with the Unified CM Intercom line, the speed dial on that line will initially point to the first Manager and then eventually to the last Manager that was called from the Intercom line.