CHAPTER 24

Cisco Unified CM Applications

Last revised on: September 18, 2009

Cisco Unified Communications Manager (Unified CM) applications provide numerous operational and functional enhancements to basic IP telephony. External eXtensible Markup Language (XML) productivity applications or IP Phone Services can be run on the web server and/or client on most Cisco Unified IP Phones. For example, the IP phone on a user's desk can be used to get stock quotes, weather information, flight information, and other types of web-based information. In addition, custom IP phone service applications can be written that allow users to track inventory, bill customers for time, or control conference room environments (lights, video screen, temperature, and so forth). Unified CM also has a number of integrated applications that provide additional functionality, including:

- Cisco Extension Mobility (EM)

  The Extension Mobility feature enables mobile users to configure a Cisco Unified IP Phone as their own, on a temporary basis, by logging in to that phone.

- Cisco Unified Communications Manager Assistant (Unified CM Assistant)

  Unified CM Assistant is a Unified CM integrated application that enables assistants to handle one or more managers' incoming phone calls.

- Cisco Unified Communications Manager Attendant Console

  The Unified CM Attendant Console enables one or more receptionists to answer and transfer (or dispatch) calls within an organization.

- Cisco WebDialer

  WebDialer is a click-to-call application for Unified CM that enables users to place calls easily from their PCs using any supported phone device.

In some cases these integrated applications also invoke IP Phone Services to provide additional functionality.

This chapter examines the following Unified CM applications:

What's New in This Chapter

Table 24-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 24-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:
Cisco Unified Communications Manager Attendant Console	Cisco Unified Communications Manager Attendant Console, page 24-34
Cisco Unified Department, Business, and Enterprise Attendant Consoles	Cisco Unified Department, Business, and Enterprise Attendant Consoles, page 24-46
Extension Mobility Redundancy options	EM Redundancy, page 24-14
Extension Mobility security	EM Security, page 24-15
Extension Mobility service parameters	EM Service Parameters, page 24-11
IP Phone Services behavior	Unified CM Services and IP Phone Service Enterprise Parameters, page 24-3
Redirector capacity	WebDialer Performance and Scalability, page 24-60
WebDialer API update	WebDialer Architecture, page 24-56
WebDialer phone support	WebDialer Phone Support, page 24-50
WebDialer redundancy	Device and Reachability Redundancy, page 24-59
WebDialer sizing	WebDialer Performance and Scalability, page 24-60

IP Phone Services

Cisco Unified IP Phone Services are applications that utilize the web client and/or server and XML capabilities of the Cisco Unified IP Phone. The Cisco Unified IP Phone firmware contains a micro-browser that enables limited web browsing capability. These phone service applications provide the potential for value-added services and productivity enhancement by running directly on the user's desktop phone. For purposes of this chapter, the term *phone service* refers to an application that transmits and receives content to and from the Cisco Unified IP Phone.

IP Phone Services Phone Support

The following phones support IP Phone Services:

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified IP Phones 7940G, 7941G, 7941G-GE, 7942G, and 7945G
- Cisco Unified IP Phones 7960G, 7961G, 7961G-GE, 7962G, and 7965G
- Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G

IP Phone Services can also run on the following IP phones, however these phone models support only text-based XML applications:

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phones 7912G and 7912G-A
- Cisco Unified Wireless IP Phone 7920

All of the IP Phones listed above can process a limited set of Cisco-defined XML objects for enabling the user interface (UI) between the phone and the web server that contains the running phone service.

Note that the phones listed above support phone services for both the Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP).

Unified CM Services and IP Phone Service Enterprise Parameters

To enable IP Phone Services, the system administrator must ensure that the Cisco Unified IP Phone Services network service is enabled under the Cisco Unified Serviceability interface. In addition, there are a number of enterprise parameters that provide configuration and customization options for IP Phone Services, as described in the following sections.

Unified CM Services for IP Phone Services

IP Phone Services rely on the Cisco CallManager Cisco IP Phone Services network service on Unified CM in order to function. This feature is installed and activated by default when Unified CM is installed on a server.

IP Phone Service Enterprise Parameters

There are a number of pertinent enterprise parameters that relate to IP Phone Services. In Cisco Unified CM 7.*x*, the Services Provisioning enterprise parameter is a new parameter that affects the behavior of how services are provisioned with IP phones. The following options can be configured:

- Internal

  Phone Services are provisioned by the administrator, and the IP phone receives its list of configured services from its configuration file that is downloaded through TFTP during the registration cycle. The Services, Messages, and Directories URLs specified in the phone URL enterprise parameters are not used. Any valid Java MIDlet services that are provisioned will be installed and available to run. This is the default setting. With this setting, IP phones no longer need to contact the IP Phone Service first to receive their list of configured services. Instead they can directly proceed to access the desired service.

- External URL

  Phone Services are not provisioned in the configuration file obtained via TFTP. The phone uses only the Phone Services URLs specified in the Phone URL enterprise parameters. Java MIDlets will not run because they must be provisioned internally to install and execute. This behavior is identical to pre-7.0 releases of Unified CM.

- Both

  Any Phone Services provisioned in the configuration file will appear first, followed by any services dynamically retrieved via the corresponding URL when the Services, Messages, or Directories button is pressed on the IP phone. Any Java MIDlets provisioned in the configuration file will be installed and available to run.

Note The Services Provisioning enterprise parameter can be overwritten with the setting in the Common Phone Profile configuration, or in the actual phone's configuration (which takes precedence over both).

This parameter is configured hierarchically with three levels: Enterprise Parameters, Common Phone Configuration, and Phone Config. So the Enterprise Parameter will have the three enumerated values above, and the Common Phone Config and Phone Config fields will have an additional Default value, which defers the setting to the level above.

The following items represent a partial list of configuration parameters under the Phone URL Parameters section of the Unified CM Enterprise Parameters configuration page, which relate to IP Phone Services and XML operation of IP Phones:

- URL Authentication (Default value = http://<*CM_IP_address*>:8080/ccmcip/authenticate.jsp)

  This URL points to the authenticate.jsp service on Unified CM, which provides an authentication proxy service between Cisco Unified IP Phones and Unified CM. The URL is used to validate "push" requests made directly to the phone by the phone services. It is automatically configured at installation time. If no value is specified for this parameter, phone services will not be able to push content to the phone.

- URL Directories (Default value = http://<*CM_IP_address*>:8080/ccmcip/xmldirectory.jsp)

  This URL points to the xmldirectory.jsp service on Unified CM, which generates and returns the directory menu presented when the user pushes the Directories (or book icon) button on the phone. The URL is automatically configured at installation time. If no value is specified for this parameter, the directory menu will not be available when the user pushes the Directories button.

- URL Idle (Default value = <*blank*>)

  This URL, if specified, points to a service that provides text or images to be displayed on the phone screen when the phone is idle. This parameter is closely coupled with the URL Idle Time parameter, which indicates how long the phone must be idle before initiating the service. By default this parameter is left blank (not configured) at installation time.

- URL Idle Time (Default value = 0)

  This parameter setting indicates the time in seconds that a phone will wait before initiating the URL Idle service. By default the parameter is set to 0 (zero) at installation time, indicating that the phone will never become idle.

- URL Information (Default value = http://<*CM_IP_address*>:8080/ccmcip/GetTelecasterHelpText.jsp)

  This URL points to the GetTelecasterHelpText.jsp service on Unified CM, which generates and returns on-screen phone help for the phone keys and call statistics when the user presses the Help ("i" or "?") button located to the right of the keypad. The URL is automatically configured at installation time. If no value is specified for this parameter, no help information will be displayed when the user pushes the Help button.

- URL Services (Default value = http://<*CM_IP_address*>:8080/ccmcip/getservicesmenu.jsp)

  This URL points to the getservicesmenu.jsp service on Unified CM, which provides a list of user-subscribed phone services for the phone when the user presses the Services (or globe icon) button. It is automatically configured at installation time. If no value is specified for this parameter, a list of subscribed services will not be provided when the user pushes the Services button.

IP Phone Services Architecture

An IP Phone service can be initiated in several ways:

- User-initiated (pull)

  An IP Phone user presses the Services button, which sends an HTTP GET message to Unified CM for displaying a list of user-subscribed phone services. Figure 24-1 illustrates this functionality.

- Phone-initiated (pull)

  An idle time value can be set within the IP Phone firmware, as indicated by the URL Idle Time parameter. When this timeout value is exceeded, the IP Phone firmware itself initiates an HTTP GET to the idle URL location specified by the URL Idle parameter.

- Phone service-initiated (push)

  A phone service application can push content to the IP Phone by sending an HTTP POST message to the phone.

Note Unlike with the user-initiated and phone-initiated pull functionality, whereby the phone's web client is used to invoke phone services, the phone service-initiated push functionality invokes action on the phone by posting content (via an HTTP POST) to the phone's web server (not to its client).

Figure 24-1 shows a detailed illustration of the user-initiated IP Phone service operation. With Services Provisioning set to External URL when a user presses the Services button, an HTTP GET message is sent from the IP Phone to the Unified CM getservicesmenu.jsp script by default (step 1). You can specify a different script by changing the Phone URL enterprise parameter (see IP Phone Service Enterprise Parameters, page 24-3). The getservicesmenu.jsp script returns the list of phone service URL locations to which the individual user has subscribed (step 2). The HTTP response returns this list to the IP Phone (step 3). Any further phone service menu options chosen by the user continue the HTTP messaging between the user and the web server containing the selected phone service application (step 4).

Note If the Service Provisioning enterprise parameter is set to Internal, steps 1 through 3 are bypassed and the operation of phone services begins with step 4.

Figure 24-1 User-Initiated IP Phone Service Architecture

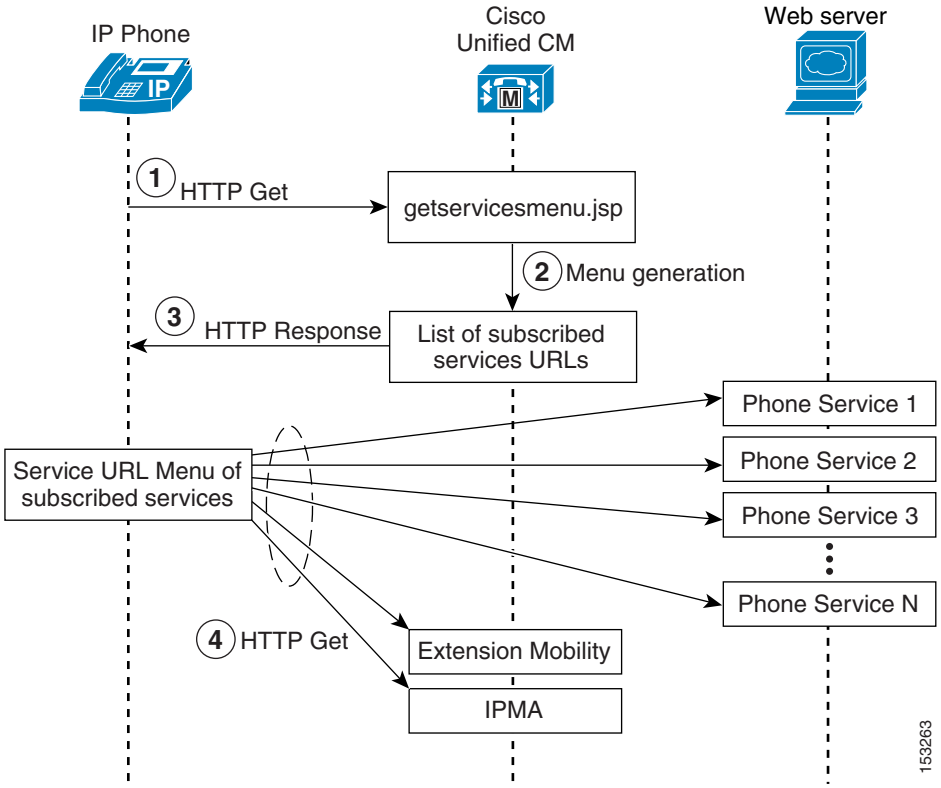
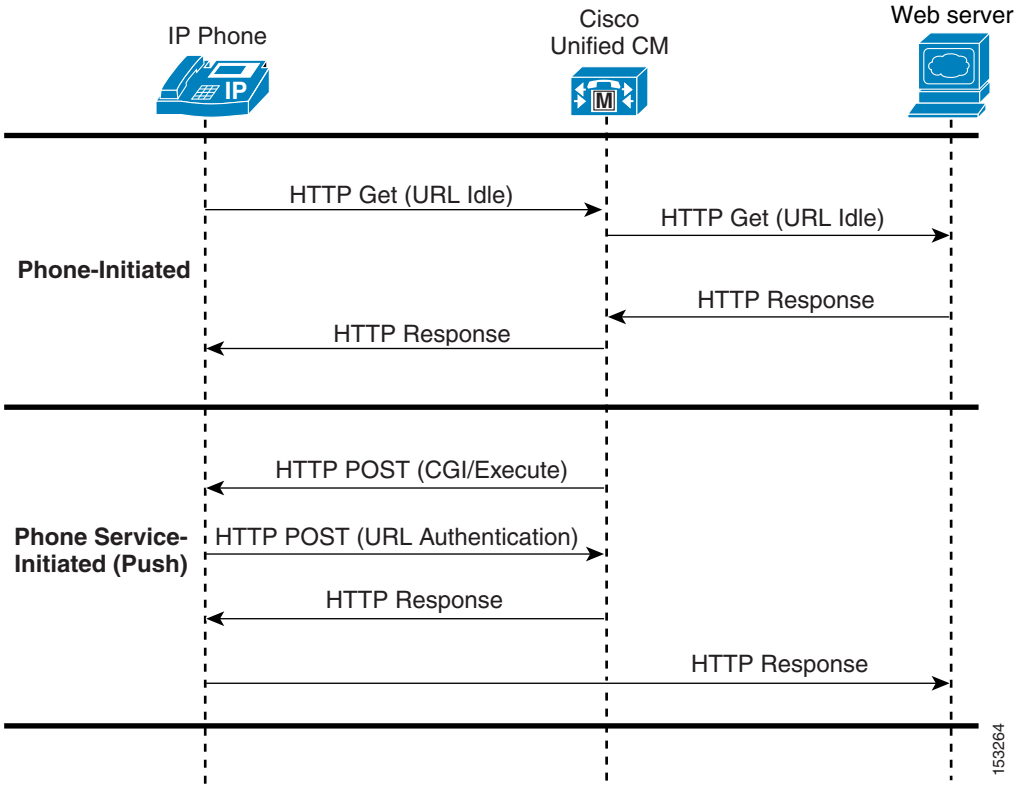


Figure 24-2 shows examples of both phone-initiated and phone service-initiated push functionality. In the phone-initiated example, the phone automatically sends an HTTP GET to the location specified under the URL Idle parameter (see IP Phone Service Enterprise Parameters, page 24-3) when the URL Idle Time is reached. The HTTP GET is forwarded via Unified CM to the external web server. The web server sends back an HTTP Response, which is relayed by Unified CM back to the phone, and the phone displays the text and/or image on the screen.

In the phone service-initiated push example, the phone service on the external web server sends an HTTP POST with a Common Gateway Interface (CGI) or Execute call to the phone's web server. Before performing the CGI or Execute call, the phone authenticates the request using the proxy authentication service specified by the URL Authentication parameter (see IP Phone Service Enterprise Parameters, page 24-3). This proxy authentication service provides an interface between the phone and the Unified CM directory in order to validate requests made directly to the phone. If the request is authenticated, Unified CM forwards an HTTP Response to the phone. The phone's web server then performs the requested action, and the phone returns an HTTP response back to the external web server. If authentication fails, Unified CM forwards a negative HTTP Response, and the phone does not perform the requested CGI or Execute action but in turn forwards a negative HTTP Response to the external web server.

Figure 24-2 Phone-Initiated and Phone Service-Initiated IP Phone Service Architecture



In addition to XML Services, a new service can be created with a Service Category of Java MIDlet. When a Java MIDlet-type service is invoked, the configured Service URL contains the URL from which the MIDlet JAD file can be retrieved. When the application server receives the JAD file request, the server should return the appropriate JAR file for that device, which the phone's MIDlet-installer will download and process.

For more information on Java MIDlet support on Cisco IP Phones, refer to the Cisco IP Phone data sheets at http://www.cisco.com.

Note After a phone has downloaded its configuration file via TFTP, the phone parses the services configuration to determine whether or not the list of services has changed, and if so, it updates its local (persisted) services configuration. If any of the changed services were Java MIDlets (which are explicitly provisioned and stored on the phone), then the phone sequentially walks through the necessary install, upgrade, downgrade, and uninstall operations to comply with what was provisioned in the configuration file. If a MIDlet install fails, it will re-attempt the install the next time the phone checks its configuration file (during boot, reset, or restart).

The administrator has the added ability to specify the Service Type of configured services to be one of the following: IP Phone Services, Directories, or Messages. This gives the administrator the flexibility to control which button users must press on the IP phone to access new services. New services can optionally be configured as Enterprise Subscriptions, which forces them to appear automatically on all IP phones without the need to update subscriptions for each individual phone. In addition, services can be enabled or disabled without the need to delete the service from the Unified CM database.

Note Default services such as Missed Calls, Placed Calls, and Corporate Directory can also be disabled. This allows the administrator to create a custom service with a Service URL matching that of the corresponding default service, thus allowing phones to subscribe to these default services on an as-needed basis.

IP Phone Services Redundancy

To ensure reliable services for phone users, you must maintain a high level of system availability, with a seamless transition to redundant systems during a system failure.

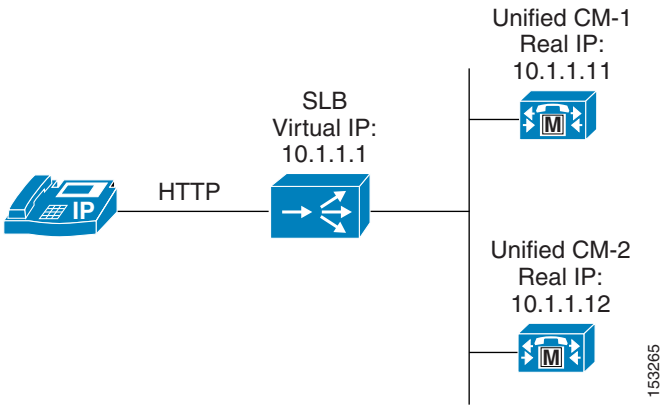
With Services Provisioning set to Internal, the phone will receive its subscribed phone services from the phone's configuration file and store these (and their corresponding service URLs) in flash. This allows the phone to access the service URLs directly on a web server without first querying the Cisco CallManager IP Phone Service. With Services Provisioning set to Internal, the Corporate and Personal Directories default services also have an extra level of redundancy built into the phones. When these services are selected, the phone will attempt to send an HTTP message with the proper URL string to the Unified CM with which it is currently registered. Therefore, the Unified CM Group configuration of the phone's device pool provides redundancy for these services.

If Services Provisioning is set to External URL or both, while most of the back-end processing of a phone service occurs on a web server, the phones still depend upon Unified CM to inform them of the service URLs for their subscribed phone services. Given the architecture of IP phone service functionality and the message flows shown in Figure 24-1 and Figure 24-2, the following two main failure scenarios should be considered.

Failure Scenario 1: Server with Cisco CallManager Cisco IP Phone Services Fails

Redundancy in this case depends upon some type of server load balancing (SLB), as illustrated in Figure 24-3, where a virtual IP address is used to point to one or more Unified CM servers. This virtual IP address is used when configuring the URL Services parameter. Thus, a Unified CM server failure does not prevent the IP Phone Services subscription list from being returned to the phone when the phone's Services button is pushed. In addition, phone services such as Extension Mobility and Unified CM Assistant that run on a Unified CM server are also potentially made redundant via this method. (See EM Redundancy, page 24-14, and Unified CM Assistant Redundancy, page 24-28.)

Figure 24-3 Method for Providing Redundancy for Phone Services



Failure Scenario 2: External Web Server Hosting a Particular IP Phone Service Fails

In this scenario, the connection to the Unified CM server is preserved, but the link fails to the web server hosting the user-subscribed phone service. This is an easier scenario to provision for redundancy because the IP phone is still able to access the Unified CM server when the Services button is pressed. In this case, the IP phone is similar to any other HTTP client accessing a web server. As a result, you can again use some type of SLB functionality (similar to the one indicated in Figure 24-3) to redirect the HTTP request from the phone to one or more redundant web servers hosting the user-subscribed phone service.

IP Phone Services Scalability

Cisco Unified IP Phone Services act, for the most part, as an HTTP client. In most cases it uses Unified CM only as a redirect server to the location of the subscribed service. Because Unified CM acts as a redirect server to the phone service, there is minimal performance impact on Unified CM when a user initiates a phone service request by pressing the Services key.

Note In the case of Extension Mobility and Unified CM Assistant phone service, Unified CM acts as more than a redirect server, and performance impacts should be considered. See the sections on Extension Mobility (EM), page 24-9, and Unified CM Assistant, page 24-17, for specific performance and scalability considerations for these applications.

Because the IP Phone is either an HTTP client or server, estimating the required bandwidth used by an IP Phone service is similar to estimating the bandwidth of an HTTP browser accessing the same text as HTTP content residing on a web hosting server.

Guidelines and Restrictions for IP Phone Services

With the exception of the integrated Extension Mobility and Unified CM Assistant applications' Phone Services, IP Phone services must reside on a separate web server. Running phone services other than Extension Mobility and Unified CM Assistant on the Unified CM server is not supported.

Extension Mobility (EM)

The Cisco Extension Mobility (EM) feature enables users to configure a Cisco Unified IP Phone as their own, on a temporary basis, by logging in to that phone. After a user logs in, the phone adopts the user's individual device profile information, including line numbers, speed dials, services links, and other user-specific properties of a phone. For example, when user X occupies a desk and logs in to the phone, that user's directory number(s), speed dials, and other properties appear on that phone; but when user Y uses the same desk at a different time, user Y's information appears. The EM feature dynamically configures a phone according to the authenticated user's device profile. The benefit of this application is that it allows users to be reached at their own extension on any phone within the Unified CM cluster, regardless of physical location, provided the phone supports EM.

EM Phone Support

The following Skinny Client Control Protocol (SCCP) phones support EM:

- Cisco Unified IP Phone 7905G

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phones 7912G and 7912G-A
- Cisco Unified Wireless IP Phones 7920 and 7921G
- Cisco Unified IP Phone 7931G
- Cisco Unified IP Phones 7940G, 7941G, 7941G-GE, 7942G, and 7945G
- Cisco Unified IP Phones 7960G, 7961G, 7961G-GE, 7962G, and 7965G
- Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G
- Cisco IP Communicator

The following Session Initiation Protocol (SIP) phones support EM:

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

Note EM is not supported on Cisco Unified IP Phones 7905G, 7912G, 7940G, or 7960G running SIP loads.

Unified CM Services and EM Service Parameters

To enable the EM application, the system administrator must activate and start a number of Unified CM services from the Cisco Unified Serviceability interface. In addition, EM service parameters provide configuration and customization options for determining how the EM application behaves.

Unified CM Services for EM

The EM application relies on the Cisco Extension Mobility feature service, which you must activate manually from the Serviceability page.

EM also relies on the following network services, which are activated automatically on all Unified CM nodes during installation:

- Cisco Extension Mobility Application
- Cisco CallManager Cisco IP Phone Services

The Cisco Extension Mobility Application service provides an interface between the EM user phone and the Cisco Extension Mobility service. In addition, the Cisco Extension Mobility Application service subscribes to the change notification indications within the cluster and maintains a list of nodes in the cluster that have an active Cisco Extension Mobility service. By subscribing to change notification within the cluster, the Cisco Tomcat network service and the Cisco Extension Mobility feature service do not have to be restarted after changes are made to the EM service parameters.

The Cisco CallManager Cisco IP Phone Services service is needed to provide access to the EM phone service. The URL used to define the EM phone service is:

http://<*Unified-CM_Server_IP-Address*>/emapp/EMAppServlet?device=#DEVICENAME#

For example:

http://10.1.1.1/emapp/EMAppServlet?device=#DEVICENAME#

EM Service Parameters

The following items represent a partial list of Cisco EM Service Parameters related to Extension Mobility functionality:

- Validate IP Address (Default value = False)

  This parameter indicates whether EM login and logout restrictions are enabled. If the value is set to false, login and logout restrictions do not take effect. If the value is set to true, the login and logout restrictions take effect, and EM attempts to validate the IP address sending the login or logout request.

- Trusted List of IP Addresses (Default value = <blank>)

  This parameter takes effect only when Validate IP Address is set to true. This parameter is a text field of size 1024 characters that takes a semicolon-separated string of IP addresses and host names. EM attempts to use this list as a source for EM login and logout IP address validation checks.

- Allow Proxy (Default value = False)

  This parameter takes effect only when Validate IP Address is set to true. This parameter indicates whether login and logout requests are allowed via proxy servers. If the value is set to false, EM rejects all login and logout requests coming via proxy servers. If the value is set to true, EM attempts to validate the IP address of proxy servers proxying EM login and logout requests.

- EM Device Cache Size (Default value = 10000)

  This parameter takes effect only when Validate IP Address is set to true. This parameter is a text field to configure the size of the device cache that is maintained by EM. Setting this parameter to a higher value will increase the number of entries that can be stored in the EM device cache. Setting this parameter to a lower value will decrease the number of entries that can be stored.

- Enforce Maximum Login Time (Default value = False)

  This parameter indicates whether EM users will be logged out automatically when the Maximum Login Time is reached. By default the value is set to False, meaning EM users are not automatically logged out.

- Maximum Login Time (Default value = 8:00)

  This parameter indicates the number of hours and/or minutes (*hh*:*mm*) an EM user can stay logged in before being logged out automatically. Automatic logout at the time specified occurs only if the Enforce Maximum Login Time parameter is set to True.

- Multiple Login Behavior (Default value = Multiple Logins Not Allowed)

  This parameter indicates whether an EM user is allowed to log in to more than one device at one time. By default multiple logins by a single user are not allowed, and attempts by a user to log in to another device while logged on to one device results in the following message:

  Login Unsuccessful
  [25]User logged in elsewhere.

- Remember the Last User Logged In (Default value = False)

  This parameter indicates whether the last userID used to log in to a device will be remembered during subsequent attempts to log in to that same device. If this value is set to True, the last logged-in userID information is stored in a table in the Unified CM database for efficient retrieval. Upon a subsequent login attempt, the UserID field in the login screen on phone is pre-populated with the stored userID value.

- Clear the call log (Default value = False)

  This parameter indicates whether the call logs specified for the Directories button menu are cleared at EM login and logout. This parameter affects the following logs: Missed Calls, Received Calls, and Placed Calls. If the value is set to True, then these logs are cleared during login and manual logout.

  One exception is that these logs are not cleared when the user is logged out automatically. Therefore, logs are not cleared when the Maximum Login Time is reached (assuming Enforce Maximum Login Time is set to True) and the user is automatically logged out of the phone. Likewise, if a Unified CM Administrator clicks on the Log Out button under the Extension section of the phone/device configuration screen, the logs are not cleared.

For a complete list of Extension Mobility service parameters, consult the *Cisco Extension Mobility* chapter of the *Cisco Unified Communications Manager Features and Services Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

EM Architecture

Figure 24-4 depicts the message flows and architecture of the EM application. When a phone user wants to access the EM application, the following sequence of events occurs:

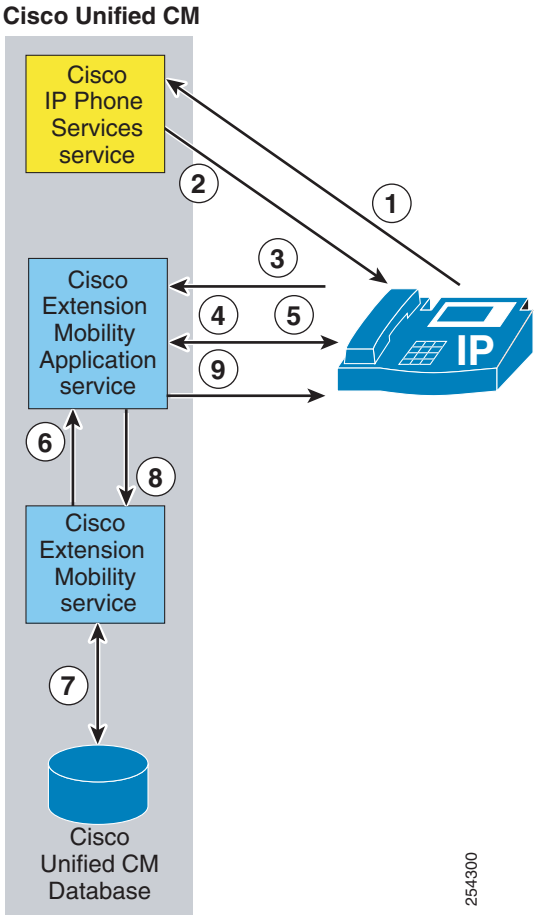
1. When the user presses the Services button on the phone, this action generates a call to the URL specified under the URL Services parameter on the Enterprise Parameter configuration page (see IP Phone Service Enterprise Parameters, page 24-3) (see also step 1 in Figure 24-4).
2. An HTTP/XML call is generated to the IP Phone Services, which returns a list of all services to which the user's phone is subscribed (see step 2 in Figure 24-4).

Note With the Services Provisioning enterprise parameter set to Internal, steps 1 and 2 are bypassed. Alternatively, with Services Provisioning set to External URL or Both, a Service URL button can be configured for EM on a user's phone so that the user can press a line or speed-dial button to generate a direct call to the Extension Mobility Application service, also bypassing steps 1 and 2.

3. Next the user selects the Extension Mobility phone service listing. This selection in turn generates an HTTP call to the Extension Mobility Application service, which serves as the interface between the phone and the Cisco Extension Mobility service (see step 3 in Figure 24-4).
4. The Extension Mobility Application service then forwards an XML response back to the phone requesting user login credentials (userID and PIN) or, if the user is already logged in, a response asking if the user wants to log off the phone (see step 4 in Figure 24-4).
5. Assuming the user is attempting to log in, the user must use the phone's keypad to enter a valid userID and PIN. After the user presses the Submit softkey, a response containing the userID and PIN just entered is forwarded back to the Extension Mobility Application service (see step 5 in Figure 24-4).

6. The Extension Mobility Application next forwards this login information to the Extension Mobility service, which interacts with the Unified CM database to verify the user's credentials (see step 6 in Figure 24-4).
7. Upon successful verification of the user's credentials, the Extension Mobility service also interacts with the Unified CM database to read and select the appropriate user device profile and to write needed changes to the phone configuration based on this device profile (see step 7 in Figure 24-4).
8. Once these changes have been made, the Extension Mobility service sends back a successful response to the Extension Mobility Application service (see step 8 in Figure 24-4).
9. The Extension Mobility Application service, in turn, sends a reset message to the phone, and the phone resets and accepts the new phone configuration (see step 9 in Figure 24-4).

Figure 24-4 EM Application Architecture and Message Flow



EM Redundancy

According to the EM architecture illustrated in Figure 24-4, reads and writes to the Unified CM database are required. EM is a user-facing feature, and database writes pertaining to EM can be performed by subscriber nodes. Therefore, if the Unified CM publisher is unavailable, EM logins and logouts are still possible.

From a redundancy perspective, the following three component levels of redundancy must be considered for full EM resiliency:

- Cisco CallManager Cisco IP Phone Services

  See IP Phone Services Redundancy, page 24-8.

- EM IP phone service

  The EM IP phone service is the service that is selected by the user from the IP phone services menu (or, alternatively, from a services line button) in order to log in or log out of a phone. This phone service points to the Cisco Extension Mobility Application service running on a particular Unified CM node. As indicated previously, the Cisco EM Application service provides the interface between the user (or phone) and the Cisco Extension Mobility service. The EM IP phone service can point to only a single IP address or host name.

- Cisco Extension Mobility service

  The Cisco Extension Mobility service is required for EM login and logout. This service takes user credentials from the Cisco EM Application service and then writes to and reads from the local Unified CM database.

In order to provide redundancy for the Cisco CallManager Cisco IP Phone Services (or URL Services) and the EM IP phone service components, Cisco recommends using a Server Load Balancer (SLB) to serve as a front end to process EM login and logout requests for multiple Unified CM nodes. In this design, SLB functionality provides a virtual IP address or DNS-resolvable hostname, as depicted in Figure 24-3, which is used as the destination address for EM login and logout requests from the IP phones. The SLB is configured to distribute these EM requests to the real IP addresses of the subscriber nodes that have the Cisco EM Application service enabled.

Most SLB devices, such as the Cisco Application Control Engine (ACE) or the Cisco IOS SLB feature, can be configured to monitor the status of multiple servers and automatically redirect requests during failure events. By using the SLB virtual IP address (or DNS hostname) for the URL Services and EM IP phone service, you can ensure that both components are still available during a node failure and, therefore, EM login and logouts will continue.

Note Multiple subscriber nodes in a cluster can have the Cisco EM Application service enabled to provide redundancy, but it supports only two subscriber nodes in a cluster actively handling login/logout requests at a given time. The SLB device configuration must support this design criteria.

Note Cisco does not recommend a redundancy design using DNS records with multiple IP listings. With multiple IP addresses returned to a DNS request, the phones must wait for a timeout period before trying the next IP address in the list, and in most cases this results in unacceptable delays to the end user. In addition, this can result in more than two subscriber nodes with the Cisco EM Application service enabled to handle login/logout requests, which is not supported.

Because the Cisco Extension Mobility Application service subscribes to cluster change notification, it maintains a list of all nodes in the cluster with the Cisco Extension Mobility service activated. Therefore, to provide redundancy for the Cisco Extension Mobility service component, this service should be run on multiple nodes within the cluster, and the Cisco Extension Mobility Application service will provide automatic failover to any nodes running the Cisco Extension Mobility service.

EM Security

Beginning with Cisco Unified CM releases 7.0 and 6.1(3), the EM feature provides an optional level of security for EM login and logout requests by validating the source IP address of the request. By default, EM does not perform this request validation; therefore, to enable EM security, the administrator must set the cluster-wide service parameter Validate IP Address to true. Once this parameter is enabled, the EM service will use the following three sources in the order indicated to validate the EM login and logout requests:

1. Cache of trusted devices

   During initialization, the EM service first queries the Unified CM database for all EM-enabled devices. It then queries the Real-Time Information Server (RIS) Data Collector service to obtain an IP address mapping for those devices that have registered with Unified CM. The number of device-to-IP-address mappings contained in the cache is limited by the size of the cache specified in the EM Device Cache Size service parameter.

2. Trusted List of IPs service parameter

   This service parameter allows the administrator to provide a semicolon-separated list of trusted IP addresses. This allows organizations to validate separate applications or proxy servers that perform login and logout requests on behalf of users.

3. New RIS Data Collector query

   If no matches are present in the cache of trusted devices or in the Trusted List of IPs service parameter, a specific query for the requesting device is made to the RIS Data Collector service. This allows login and logout requests to be validated if the device registered after cache creation or if the cache is full.

Whenever a login or a logout request is received by an EM service enabled for Validate IP Address, EM performs the IP address validation by first attempting to locate the device-to-IP mapping in the cache of trusted devices. If the mapped IP address for that device matches the source IP address of the login or logout request, the request is performed. If the device is not found in the cache or if the IP address does not match, the EM service checks the Trusted List of IPs service parameter. If the IP address of the source requesting the login or logout is located in this list, the request is performed. If the IP address is not validated here, the EM service then creates a new RIS Data Collector query for the device making the request. If the response to this query contains the IP address of the source requesting the login or logout, EM performs the login and adds this device-to-IP mapping to the cache of trusted devices if the EM device cache size has not been exceeded. If the IP address is not validated during this step, an error is displayed on the requesting device.

For organizations that implement a web proxy to handle EM login and logout HTTP requests, the Allow Proxy service parameter must be set to true. A proxy server, while forwarding the HTTP request, will set the via-field of the HTTP header with its hostname. If there are multiple proxy servers between the device and Unified CM, and if the request is forwarded by all the servers, then the via-field in the HTTP header will have a comma-separated list of hostnames for each of the proxy servers in the forwarding path. The Allow Proxy service parameter, if set to true, will allow EM login and logouts received via a web proxy. In addition, if the proxied EM requests use the source IP address of the proxy server, this IP address must also be configured in the Trusted List of IPs service parameter.

Guidelines and Restrictions for EM

The following guidelines and restrictions apply with regard to the deployment and operation of EM within the Unified CM telephony environment:

- EM is supported only within a single Unified CM cluster.

  EM is not currently supported between clusters. EM users of one Unified CM cluster can not log on to a phone in a second cluster unless a separate device profile and userID for that user has been created in the second cluster.

- EM users should not move between locations or sites within a cluster when Automated Alternate Routing (AAR) and/or the Voice over PSTN (VoPSTN) deployment model are in use.

  EM functionality relies on the use of the IP network for routing calls. Call routing via the PSTN is more problematic because E.164 PSTN numbers are static and the PSTN is unable to account for movement of EM user directory numbers (DNs) from their home sites. AAR relies on the PSTN for call routing, as does the VoPSTN deployment model. In both cases, EM user movement between locations and sites is supported only if all sites the user is traversing are in the same AAR group. For additional information, see Extension Mobility, page 10-92.

- Restarting the Extension Mobility Service or the node on which the service is running will affect auto-logout settings.

  If Cisco Extension Mobility is stopped or restarted, the system does not auto-logout users who are already logged in after the expiration of the maximum login interval. These phones have to be logged out manually.

EM Performance and Capacity

The Cisco EM application supports the following cluster-wide login and logout capacities:

- Maximum of 250 sequential logins and/or logouts per minute with the Cisco MCS-7845H2/I2 server.
- Maximum of 235 sequential logins and/or logouts per minute with the Cisco MCS-7835H2/I2 server.
- Maximum of 200 sequential logins and/or logouts per minute with the Cisco MCS-7825H2/I2 server.

Note Deploying earlier server models will result in diminished capacity.

Cisco Extension Mobility login and logout functionality can be distributed across a pair of subscriber nodes to increase login/logout cluster capacity. To distribute the EM load evenly between the two subscriber nodes, the phones should be divided into two groups, with one group of phones subscribed to an EM phone service pointing to one of the subscriber nodes and the other group of phones subscribed to a second EM phone service that is pointing to a second subscriber node. When the EM load is distributed in this way, evenly between two MCS-7845H2/I2 servers, the maximum cluster-wide capacity is 375 sequential logins and/or logouts per minute.

Note Multiple subscriber nodes in a cluster can have the Cisco EM Application service enabled to provide redundancy. However, for increased capacity, a maximum of only two subscriber nodes in a cluster can actively handle EM login and logout requests at a given time.

Note Enabling EM Security does not diminish performance.

EM Interactions: Unified CM Assistant, Attendant Console, and WebDialer

EM can be used by both Unified CM Assistant Managers and attendant console users to log into their phones. For the details and guidelines governing the use EM with these other applications, see Unified CM Assistant Interactions with EM, page 24-34.

WebDialer users can also use EM to log on to their phones. See WebDialer Interactions with EM, page 24-61, for more information.

Unified CM Assistant

Cisco Unified Communications Manager Assistant (Unified CM Assistant) is a Unified CM integrated application that enables assistants to handle incoming calls on behalf of one or more managers. With the use of the Unified CM Assistant Console desktop application or the Unified CM Assistant Console phone service on the assistant phone, assistants can quickly determine a manager's status and determine what to do with a call. Assistants can manipulate calls using their phone's softkeys and service menus or via the PC interface with either keyboard shortcuts, drop-down menus, or by dragging and dropping calls to the managers' proxy lines.

Unified CM Assistant Phone Support

The following SCCP phones support Unified CM Assistant:

- Cisco Unified IP Phones 7940G, 7941G, 7941G-GE, 7942G, and 7945G
- Cisco Unified IP Phones 7960G, 7961G, 7961G-GE, 7962G, and 7965G
- Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G

The following SIP phones support Unified CM Assistant:

- Cisco Unified IP Phones 7941G, 7941G-GE, 7942G, and 7945G
- Cisco Unified IP Phones 7961G, 7961G-GE, 7962G, and 7965G
- Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G

Note The Cisco Unified IP Phone Expansion Module 7914 is supported with any of the following phones: Cisco Unified IP Phone 7960G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G-GE, or 7975G. Up to two Cisco 7914 Modules are supported per phone.

Unified CM Services and Unified CM Assistant Service Parameters

To enable the Unified CM Assistant application, the system administrator must activate and start several Unified CM feature services from the Cisco Unified Serviceability interface. In addition, Unified CM Assistant service parameters provide configuration and customization options for determining how the Unified CM Assistant application and services behave.

Unified CM Services for Unified CM Assistant

The Unified CM Assistant application relies on the following feature services, which must to be activated manually from the Serviceability page:

- Cisco IP Manager Assistant
- Cisco CTIManager

The Unified CM Assistant application also relies on the Cisco CallManager Cisco IP Phone Services network service, which is automatically activated on Unified CM during installation.

The Cisco IP Manager Assistant service provides an interface for the Unified CM Assistant Console and Manager Configuration applications as well as interacting with the Cisco CTIManager service and Unified CM database. The Cisco CTIManager service interfaces and interacts with the Cisco CallManager service and the Cisco IP Manager Assistant service for phone and call control.

The Cisco Unified IP Phone Services are needed to provide access to the Unified CM Assistant phone service from the manager and assistant phones. The URL used to define the Unified CM Assistant phone service is:

http://<*Server_IP-Address*>:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

(where <*Server_IP-Address*> is the IP address of any node in the cluster)

Note Cisco recommends that you configure two instances of the Unified CM Assistant phone service. One Unified CM Assistant phone service instance should point to the primary Unified CM Assistant server and the other should point to the backup Unified CM Assistant server. By configuring a primary and a secondary phone service in this manner, you can provide redundancy for the assistant phone console. See Device and Reachability Redundancy, page 24-30, for additional information.

Unified CM Assistant Service Parameters

The following items represent a partial list of Cisco IP Manager Assistant service parameters related to Unified CM Assistant functionality:

- CTIManager Connection Security Flag (Default value = Non Secure)

  This parameter determines whether a secure Transport Layer Security (TLS) connection is used between the Cisco IP Manager Assistant service and the CTIManager. If enabled, a secure connection is configured using the Certificate Authority Proxy Function (CAPF) profile configured for the instance ID of the application user IPMASecureSysUser. The instance ID must be specified under the service parameter CAPF Profile Instance ID for Secure Connection to CTIManager.

  Note The application user IPMASecureSysUser is a system account created automatically at installation. It cannot be deleted.

- CAPF Profile Instance ID for Secure Connection to CTIManager (Default value = <None>)

  The CAPF Profile Instance ID is a unique string of numbers and/or letters used to identify the TLS connection or instance that is made between the Unified CM Assistant server and CTIManager for the IPMASecureSysUser application user. If the CTI Manager Connection Security Flag parameter is set to True, then this parameter must be configured with a value.

- CTIManager (Primary) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the primary CTIManager that the Cisco Unified CM Assistant server uses to process calls. A primary CTIManager can be configured on each Unified CM Assistant server.

- CTIManager (Backup) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the backup CTIManager that this Cisco Unified CM Assistant server uses to process calls when the primary CTIManager is down. A backup CTIManager can be configured on each Unified CM Assistant server.

- Cisco IPMA Server (Primary) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the primary Cisco Unified CM Assistant server. This is a cluster-wide parameter and only two Unified CM Assistant servers, a primary and a backup, may be configured.

- Cisco IPMA Server (Backup) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the backup Cisco Unified CM Assistant server. The backup server provides Unified CM Assistant functionality when the primary Unified CM Assistant server fails. This is a cluster-wide parameter.

- Cisco IPMA Assistant Console Heartbeat Interval (Default value = 30)

  This parameter specifies how often, in seconds, the IPMA server will send keep-alive messages (commonly referred to as heartbeats) to each Unified CM Assistant Console desktop application. The Unified CM Assistant Console desktop applications will initiate a failover to the backup IPMA server when they fail to receive a keep-alive message from the primary server before the specified time expires.

- Cisco IPMA Assistant Console Request Timeout (Default value = 30)

  This parameter specifies the time, in seconds, that Unified CM Assistant Console desktop applications will wait to receive a response from the active or primary IPMA server.

- Cisco IPMA RNA Forward Calls (Default value = False)

  When set to True, this parameter enables calls to an assistant's phone to be ring-no-answer (RNA) forwarded to the manager's next available assistant when the RNA value specified by the Cisco IPMA RNA Timeout parameter expires. If this parameter is set to False, then the call will ring the first assistant indefinitely or, if a voicemail profile is configured, the call will be forwarded to voicemail.

- Cisco IPMA RNA Timeout (Default value = 10)

  This parameter specifies the time, in seconds, that the Cisco Unified CM Assistant server waits before RNA forwarding an unanswered call to the next available assistant. RNA forwarding will occur only if the Cisco IPMA RNA Forward Calls parameter is set to True. If a voicemail profile is configured on the line and no other assistant is available, the call will be forwarded to voicemail when the timeout expires.

Advanced Service Parameters

The following service parameters are hidden by default and are available only when you click the **Advanced** button or icon:

- Enable Multiple Active Mode (Default value = False)

  When set to True, this parameter enables more than one Unified CM Assistant pair to be configured for increased Unified CM Assistant capacity.

- Pool 2: Cisco IPMA Server (Primary) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the primary Cisco Unified CM Assistant server in Pool 2. This is a cluster-wide parameter and only two Unified CM Assistant servers, a primary and a backup, may be configured in this pool.

- Pool 2: Cisco IPMA Server (Backup) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the backup Cisco Unified CM Assistant server in Pool 2. The backup server provides Unified CM Assistant service when the primary Unified CM Assistant server in Pool 2 fails. This is a cluster-wide parameter.

- Pool 3: Cisco IPMA Server (Primary) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the primary Cisco Unified CM Assistant server in Pool 3. This is a cluster-wide parameter and only two Unified CM Assistant servers, a primary and a backup, may be configured in this pool.

- Pool 3: Cisco IPMA Server (Backup) IP Address (Default value = <blank>)

  This parameter specifies the IP address of the backup Cisco Unified CM Assistant server in Pool 3. The backup server provides Unified CM Assistant service when the primary Unified CM Assistant server in Pool 3 fails. This is a cluster-wide parameter.

For a complete list of Unified CM Assistant service parameters, refer to the Unified CM Assistant information in the *Cisco Unified Communications Manager Features and Services Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

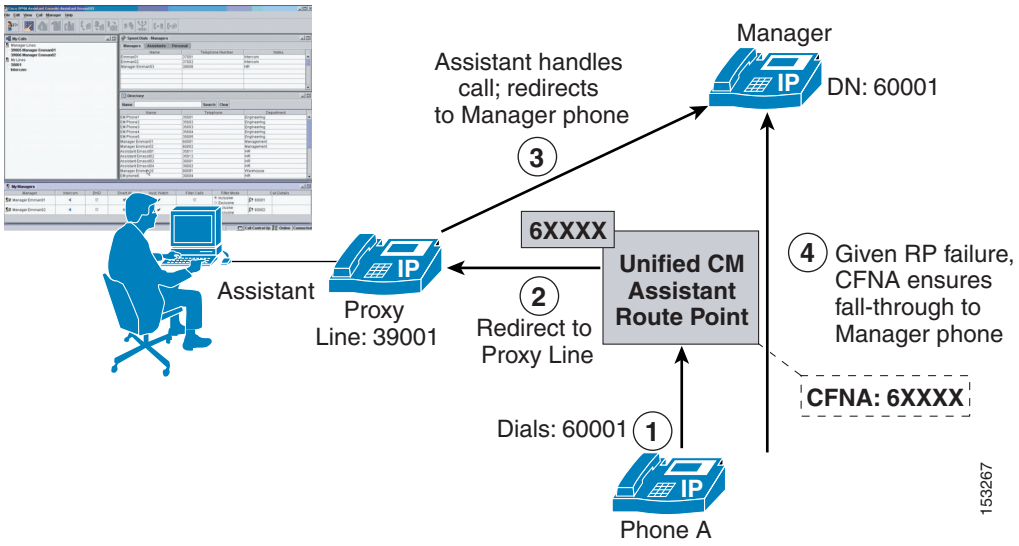
Unified CM Assistant Functionality and Architecture

The Unified CM Assistant application can operate in two modes: proxy line mode and shared line mode. The operation and functionality of each mode is different, and each has specific advantages and disadvantages. Both modes can be configured within a single cluster. However, mixing modes on the same assistant is not allowed. A single assistant providing support for one or more managers can support those managers in either shared line mode or proxy line mode.

Unified CM Assistant Proxy Line Mode

Figure 24-5 illustrates a simple call flow with Unified CM Assistant in proxy line mode. In this example, Phone A calls the Manager phone with directory number (DN) 60001 (step 1). The CTI/Unified CM Assistant Route Point (RP) intercepts this call based on a configured DN of 6XXXX. Next, based on the Manager DN, the call is redirected by the route point to the Manager's proxy line (DN: 39001) on the Assistant's phone (step 2). The Assistant can then answer or handle the call and, if appropriate, redirect the call to the Manager's phone (step 3). In the event of Unified CM Assistant application failure or if the Unified CM Assistant RP fails, a fall-through mechanism exists via the Call Forward No Answer (CFNA) 6XXXX configuration of the RP, so that calls to the Manager's DN will fall-through directly to the Manager's phone (step 4).

Figure 24-5 Unified CM Assistant Proxy Line Mode

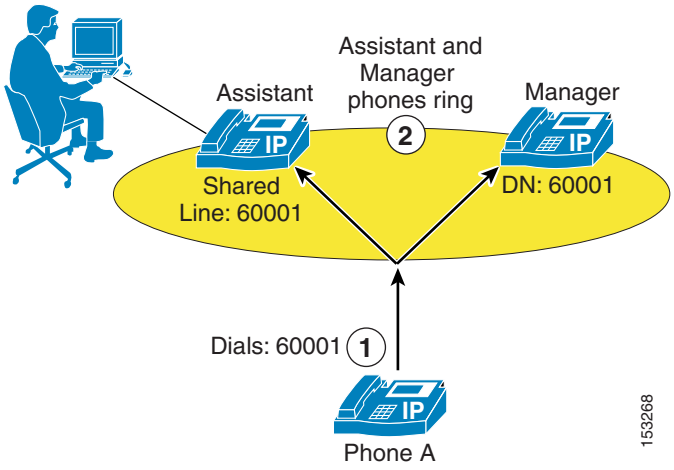


Note The CFNA fall-through mechanism illustrated in Figure 24-5 requires configuration of the same summarized digit-string as the Unified CM Assistant RP directory number in both the Forward No Answer Internal and Forward No Answer External fields under the Unified CM Assistant RP directory number configuration page. In addition, the calling search space (CSS) field for each of these call forward parameters should be configured with the calling search space containing the partition with which the Manager phone DNs are configured, so that the Manager phone DNs can be reached if the Unified CM Assistant RP or Unified CM Assistant application fails.

Unified CM Assistant Share Lined Mode

Figure 24-6 illustrates a simple call flow with Unified CM Assistant in shared line mode. In this example, Phone A calls the Manager phone with directory number (DN) 60001, which is a shared line on the Assistant phone (step 1). The call will ring at both the Assistant and Manager phones unless the Manager has invoked the Do Not Disturb (DND) feature, in which case the Assistant's phone will be the only phone that rings audibly (step 2).

Figure 24-6 Unified CM Assistant Shared Line Mode



In Unified CM Assistant shared line mode, the Unified CM Assistant RP is not needed or required for intercepting calls to the Manager phone. However, the Do Not Disturb (DND) feature on the Manager phone and the Unified CM Assistant Console desktop application still depend on the Cisco IP Manager Assistant and Cisco CTIManager services. Furthermore, in Unified CM Assistant shared line mode, features such as call filtering, call intercept, assistant selection, and Assistant Watch are not available.

Unified CM Assistant Architecture

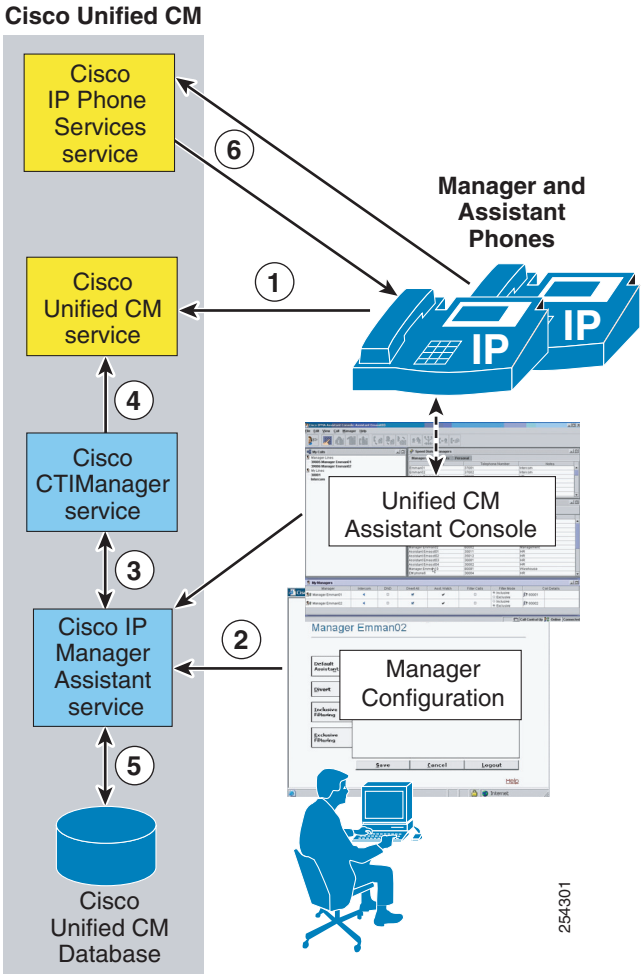
The architecture of the Unified CM Assistant application is as important to understand as its functionality. Figure 24-7 depicts the message flows and architecture of Unified CM Assistant. When Unified CM Assistant has been configured for Unified CM Assistant Manager and Assistant users, the following sequence of interactions and events can occur:

1. Manager and Assistant phones register with the Cisco CallManager Service, and the phone's keypad and softkeys are used to handle call flows (see step 1 in Figure 24-7).
2. Both the Unified CM Assistant Console desktop application and the Manager Configuration web-based application communicate and interface with the Cisco IP Manager Assistant service (see step 2 in Figure 24-7).
3. The Cisco IP Manager Assistant service in turn interacts with the CTIManager service for exchanging line monitoring and phone control information (see step 3 in Figure 24-7).
4. The CTIManager service passes Unified CM Assistant phone control information to the Cisco CallManager service and also controls the Unified CM Assistant RP (see step 4 in Figure 24-7).
5. In parallel, the Cisco IP Manager Assistant service reads and writes Unified CM Assistant application information to and from the Unified CM database (see step 5 in Figure 24-7).
6. The Manager may choose to invoke the Unified CM Assistant phone service by pushing the Services button, thus generating a call to the IP Phone Services service that will return a list of all services (including the Unified CM Assistant phone service) to which the phone is subscribed (see step 6 in Figure 24-7).

The Unified CM Assistant phone service is controlled by the Cisco IP Manager Assistant service, and configuration changes made by the Manager using the phone are handled and propagated via the Cisco IP Manager Assistant service.

Note With the Services Provisioning enterprise parameter set to Internal, steps 1 and 2 are bypassed. Alternatively, with Services Provisioning set to External URL or Both, a Service URL button can be configured for the Unified CM Assistant phone service on a user's phone so that the user can press a line or speed-dial button to generate a direct call to the Cisco IP Manager Assistant service, also bypassing steps 1 and 2.

Figure 24-7 Unified CM Assistant Architecture



Note While Figure 24-7 shows the IP Phone Services, Cisco CallManager, CTIManager, and Cisco IP Manager Assistant services all running on the same node, this configuration is not a requirement. These services can be distributed between multiple nodes in the cluster but have been shown on the same node here for ease of explanation.

Unified CM Assistant Dial Plan Considerations

Dial plan configuration is extremely important for Unified CM Assistant configured in proxy line mode. To ensure that calls to Manager DNs are intercepted by the Unified CM Assistant RP and redirected to the Assistant phone, calling search spaces and partitions must be configured in such a way that Manager DNs are unreachable from all devices except the Unified CM Assistant RP and the Manager's proxy line on the Assistant phone.

Figure 24-8 shows an example of a proxy line mode Unified CM Assistant dial plan with the minimum requirements for calling search spaces, partitions, and the configuration of various types of devices within these dial plan components. Three partitions are required for proxy line mode, and for the example in Figure 24-8 they are as follows:

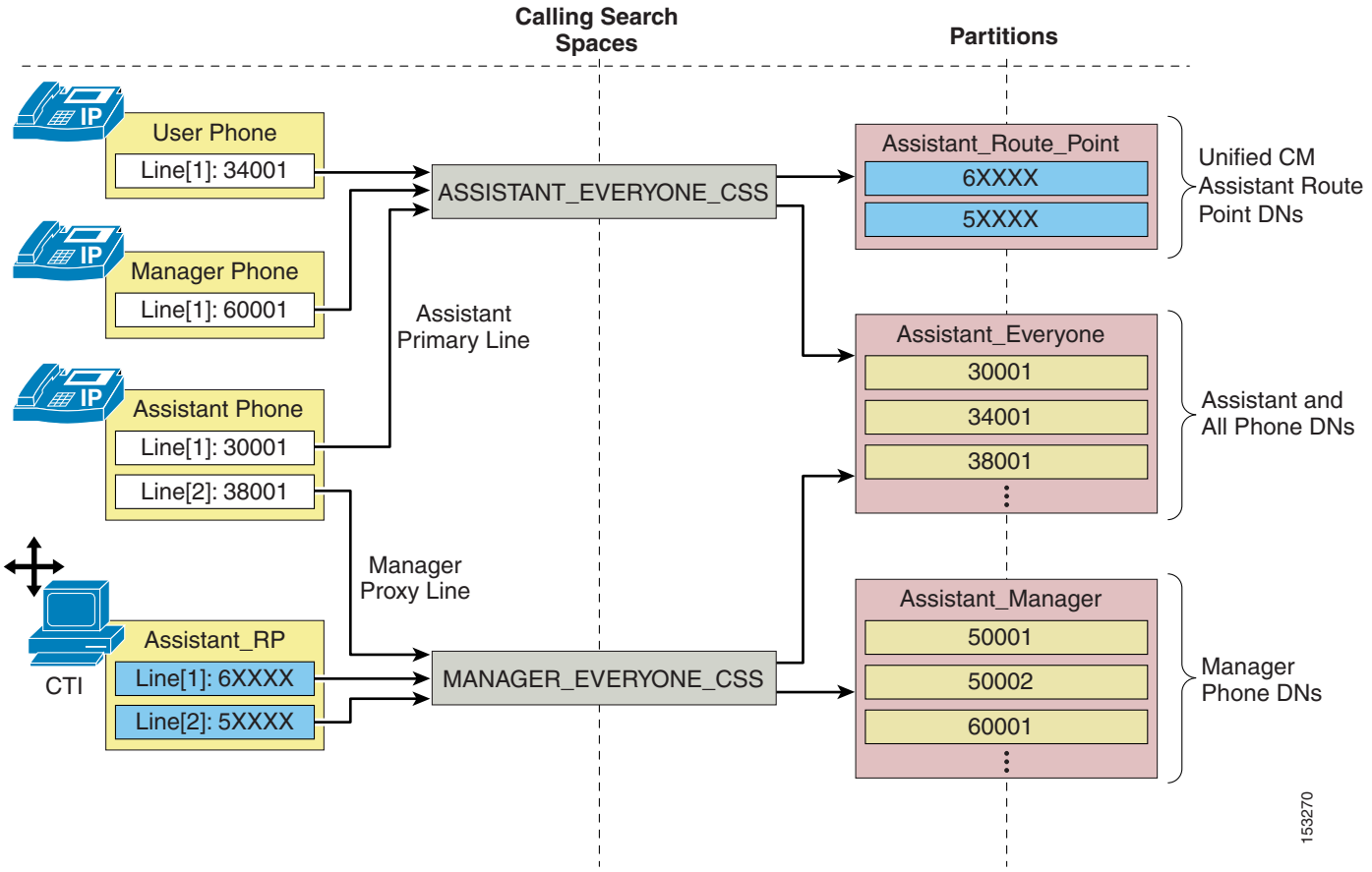
- Assistant_Route_Point partition, containing all the Unified CM Assistant RP DNs
- Assistant_Everyone partition, containing all the Assistant and other user phone DNs
- Assistant_Manager partition, containing all the Manager phone DNs

In addition, two calling search spaces are required, and for the example in Figure 24-8 they are as follows:

- ASSISTANT_EVERYONE_CSS calling search space, containing both the Assistant_Route_Point and Assistant_Everyone partitions.
- MANAGER_EVERYONE_CSS calling search space, containing both the Assistant_Manager and Assistant_Everyone partitions.

That is the extent of the dial plan for this example. However, it is also important to properly configure the various phone and Unified CM Assistant RP DNs or lines with the appropriate calling search spaces so that call routing works as required. In this case all user, Assistant primary (or personal), and Manager phone lines would be configured with the ASSISTANT_EVERYONE_CSS calling search space so that all of these lines can reach all the DNs in the Assistant_Everyone and Assistant_Route_Point partitions. Intercom lines and any other lines configured on devices within the telephony network would be configured with this same calling search space. All Manager proxy lines and all Assistant_RP lines are configured with the MANAGER_EVERYONE_CSS calling search space so that all of these lines can reach the Manager DNs in the Assistant_Manager partition as well as all the DNs belonging to the Assistant_Everyone partition. In this way, the dial plan ensures that only the Assistant_RP lines and the Manager proxy lines on the Assistant phones are capable of reaching the Manager phone DNs directly.

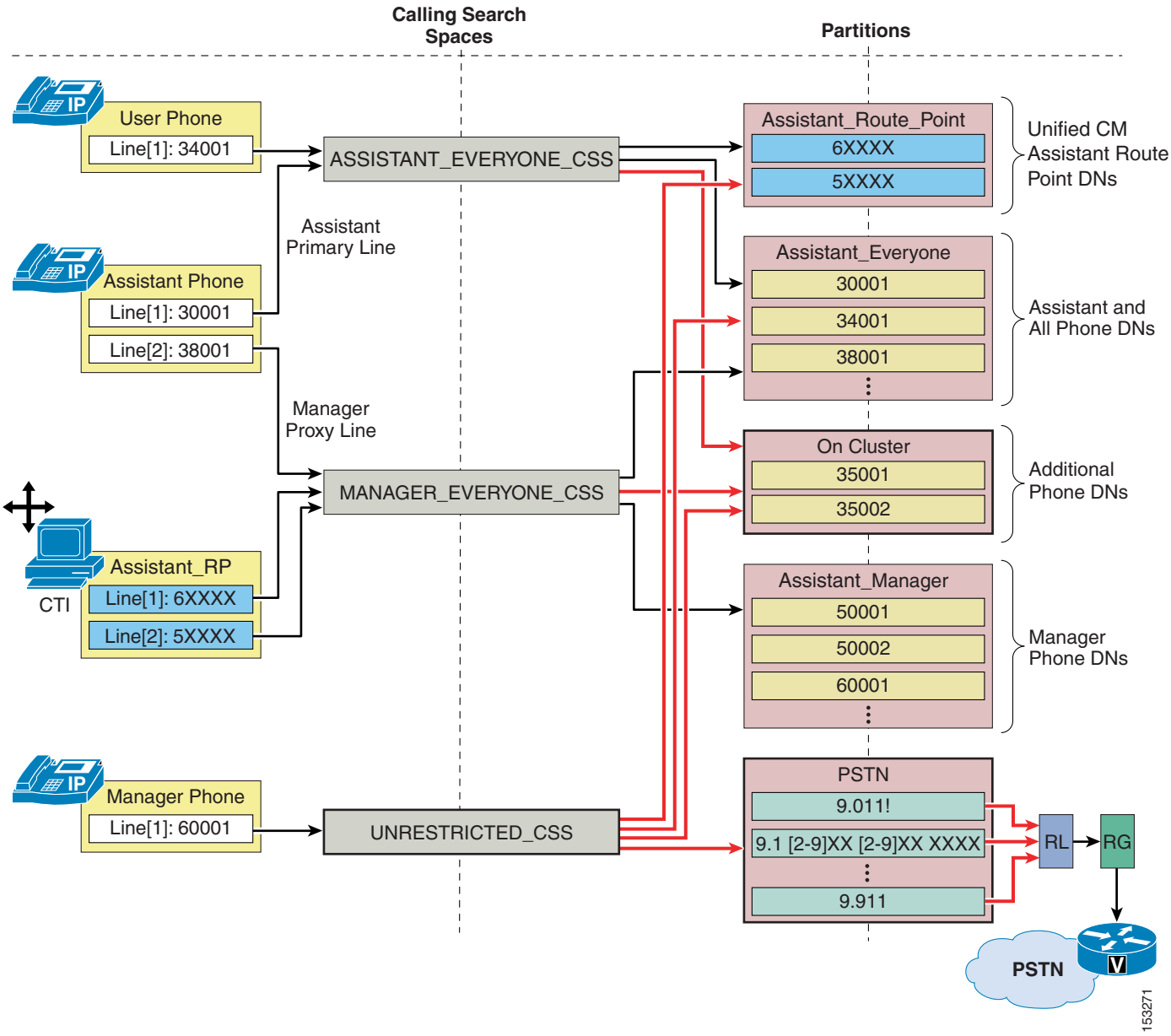
Figure 24-8 Unified CM Assistant Proxy Line Mode Dial Plan Example



The example in Figure 24-8 shows the minimum dial plan requirements for Unified CM Assistant in proxy line mode. However, most real-world telephony networks will have additional or existing dial plan requirements that must be integrated with the Unified CM Assistant calling search spaces and partitions. Figure 24-9 illustrates such an integration dial plan. In this example, the previously discussed dial plan must now handle two additional partitions and an additional calling search space. The On Cluster partition has been added in Figure 24-9, and it contains some additional phone DNs. The On Cluster partition has been added to both of the existing Unified CM Assistant calling search spaces (ASSISTANT_EVERYONE_CSS and MANAGER_EVERYONE_CSS) so that existing devices can reach these added DNs. The UNRESTRICTED_CSS calling search space has also been added to the existing dial plan. This calling search space is configured with the Assistant_Route_Point, Assistant_Everyone, and the recently added On Cluster partitions. In addition, a second new partition called PSTN has been added, and it contains a set of route patterns used for routing calls to the PSTN via the common route list (RL), route group (RG), and voice gateway mechanism. This PSTN partition is configured as part of the UNRESTRICTED_CSS calling search space.

Phone and device line calling search space configurations may be adjusted to incorporate the newly added partitions and calling search spaces, provided the Assistant_RP and Assistant phone Manager proxy lines remain assigned to the MANAGER_EVERYONE_CSS calling search space. In this example, the Manager phone line has been moved from the originally configured ASSISTANT_EVERYONE_CSS calling search space to the new UNRESTRICTED_CSS because it is likely that a Manager would be given unrestricted access to the PSTN.

Figure 24-9 Unified CM Assistant Proxy Line Mode Dial Plan Integration Example



As Figure 24-9 illustrates, integrating additional partitions and calling search spaces into a new or existing Unified CM Assistant dial plan is feasible, but care must be taken to ensure that the underlying proxy line mode mechanism remains intact.

For Unified CM Assistant shared line mode, no special dial plan provisioning is required. Manager and Assistant phones can be configured with calling search spaces and partitions like any other phones in the network because there are no Unified CM Assistant RPs or proxy lines to be concerned about. The only requirement with regard to shared line mode is that the Manager and Assistant DNs must be in the same partition so that shared line functionality is possible.

Unified CM Assistant Console

The Unified CM Assistant Console desktop application or the Unified CM Assistant Console phone service is required in order for assistants to handle calls on a manager's behalf. The desktop application provides assistants with a graphical interface for handling calls, while the phone service provides a menu-driven interface for handling calls. Both the desktop application and the IP phone service allow the assistant to configure the Manager phone and environment and monitor line status and availability. In addition, the desktop application provides other functions such as click-to-call speed dialing and directory entries, which can also be performed on the assistant phone using the traditional softkey and menu approach.

Unified CM Assistant Console Installation

The Unified CM Assistant Console desktop application can be installed from the following URL:

https://<*Server_IP-Address*>:8443/ma/Install/IPMAConsoleInstall.jsp

(where <*Server_IP-Address*> is the IP address of any node in the cluster)

The Unified CM Assistant Console phone service does not require any installation. To enable the Assistant's phone as a console, subscribe the phone to the Unified CM Assistant phone service. (This is the same service to which Manager phones must also be subscribed.)

Unified CM Assistant Desktop Console QoS

After installation, and in order to handle calls on a Manager's behalf, the Assistant must log on to the application by providing userID and password (as configured in the End-user directory on Unified CM) and will have to toggle status to "online" by clicking the Go Online icon or menu item. Once the user is logged in and online, the desktop application communicates with the Unified CM Assistant server at TCP port 2912. The application chooses an ephemeral TCP port when sourcing traffic. Because the Unified CM Assistant server on Unified CM interfaces with the desktop application for call control (generation and handling of call flows), traffic sourced from Unified CM on TCP port 2912 is QoS-marked by Unified CM as Differentiated Services Code Point (DSCP) of 24 or Per Hop Behavior (PHB) of CS3. In this way, Unified CM Assistant phone control traffic can be queued throughout the network like all other call signaling traffic.

In order to ensure symmetrical marking and queuing, the Unified CM Assistant Console application traffic destined for Unified CM TCP port 2912 should also be marked as DSCP 24 (PHB CS3) to ensure this traffic is placed in the appropriate call signaling queues along the network path toward Unified CM and the Unified CM Assistant server. The Unified CM Assistant Console application marks all traffic as best-effort. This means that you will have to apply an access control list (ACL) at the switch port level (or somewhere along the network path, preferably as close to the console PC as possible) to remark traffic sent by the application PC destined for Unified CM on TCP port 2912 from DSCP 0 (PHB Best Effort) to DSCP 24 (PHB CS3).

Unified CM Assistant Console Directory Window

The directory window within the Assistant Console desktop application enables an assistant to search for end-users in the Unified CM Directory. Search strings entered into the Name field of the directory window are sent to the Unified CM Assistant server, and searches are generated directly against the Unified CM database. Responses to search queries are then sent back to the desktop application by the Unified CM Assistant server.

While the additional traffic generated by directory searches within the desktop application is nominal, this traffic can be problematic in centralized call processing deployments when one or more Unified CM Assistant console applications are running at remote sites. A directory search resulting in a single entry generates approximately one (1) kilobit of traffic from the Unified CM Assistant server to the desktop application. Fortunately, a maximum of 25 entries can be retrieved per search, meaning that a maximum of approximately 25 kilobits of traffic can be generated for each search made by the desktop application. However, if directory searches are made by multiple Unified CM Assistant Console desktop applications across low-speed WAN links from the Unified CM Assistant server, the potential for congestion, delay, and queuing is increased. In addition, directory retrieval traffic is sourced from Unified CM on TCP port 2912, like all other Unified CM Assistant traffic to the desktop. This means that directory retrieval traffic is also marked with DSCP 24 (PHB CS3) and therefore is queued like call signaling traffic. As a result, directory retrieval could potentially congest, overrun, or delay call control traffic.

Note If a directory search generates more than 25 entries, the assistant is warned via a dialog box with the message: "Your search returned more than 25 entries. Please refine your search."

Given the potential for network congestion, Cisco recommends that administrators encourage Unified CM Assistant Console users to do the following:

- Limit their use of the directory window search function.
- To reduce the number of entries returned, enter as much information as possible in the Name field and avoid wild-card or blank searches when using the feature.

These recommendations are especially important if either of the following conditions is true:

- There are many Unified CM Assistant Assistants within the cluster.
- There are many assistants separated from the Unified CM and/or Unified CM Assistant servers by low-speed WAN links.

Unified CM Assistant Phone Console QoS

In order to handle calls on a Manager's behalf using the Unified CM Assistant Phone Console phone service, the Assistant must log on to the service by providing a userID and PIN (as configured in the End-user directory on Unified CM). Once the user is logged in, the phone console service communicates with Unified CM using HTTPS and SCCP. Call control traffic for Unified CM Assistant call generation and call handling is sent between the phone and Unified CM using SCCP. By default this traffic is marked as Differentiated Services Code Point (DSCP) of 24 or Per Hop Behavior (PHB) of CS3, thus ensuring it is queued throughout the network as call signaling traffic, therefore no additional QoS configuration or marking is required.

Unified CM Assistant Redundancy

Unified CM Assistant application redundancy can be provided at two levels:

- Redundancy at the component and service level

  At this level, redundancy must be considered with regard to Unified CM Assistant service or server redundancy and CTIManager service redundancy. Likewise, the lack of publisher redundancy and the impact of this component failing should also be considered.

- Redundancy at the device and reachability level

  At this level, redundancy should be considered as it relates to Assistant and Manager phones, the Unified CM Assistant route point, and the Unified CM Assistant Console desktop application and phone service, as well as redundancy in terms of Assistant and Manager reachability.

Service and Component Redundancy

As shown in Figure 24-7, Unified CM Assistant functionality is primarily dependent on the Cisco IP Manager Assistant service and the Cisco CTIManager service. In both cases, redundancy is automatically built-in using a primary and backup mechanism. Up to three pairs of active and backup Unified CM Assistant servers (nodes running the Cisco IP Manager service) can be defined, for a total of six Unified CM Assistant servers within a single cluster. Active and backup Unified CM Assistant server pairs are configured using the Cisco IPMA Server IP Address, Pool 2 Cisco IPMA Server IP Address, and Pool 3 Cisco IPMA Server IP Address service parameters (see Unified CM Assistant Service Parameters, page 24-18). With the configuration of these parameters, the required Cisco IP Manager service is made redundant. Given a failure of any of the primary Unified CM Assistant servers, the backup or standby Unified CM Assistant servers are able to handle Unified CM Assistant service requests. For each pair of Unified CM Assistant servers, only one Unified CM Assistant server can be active and handling request at a given time, while the other Unified CM Assistant server will be in a standby state and will not handle requests unless the active server fails.

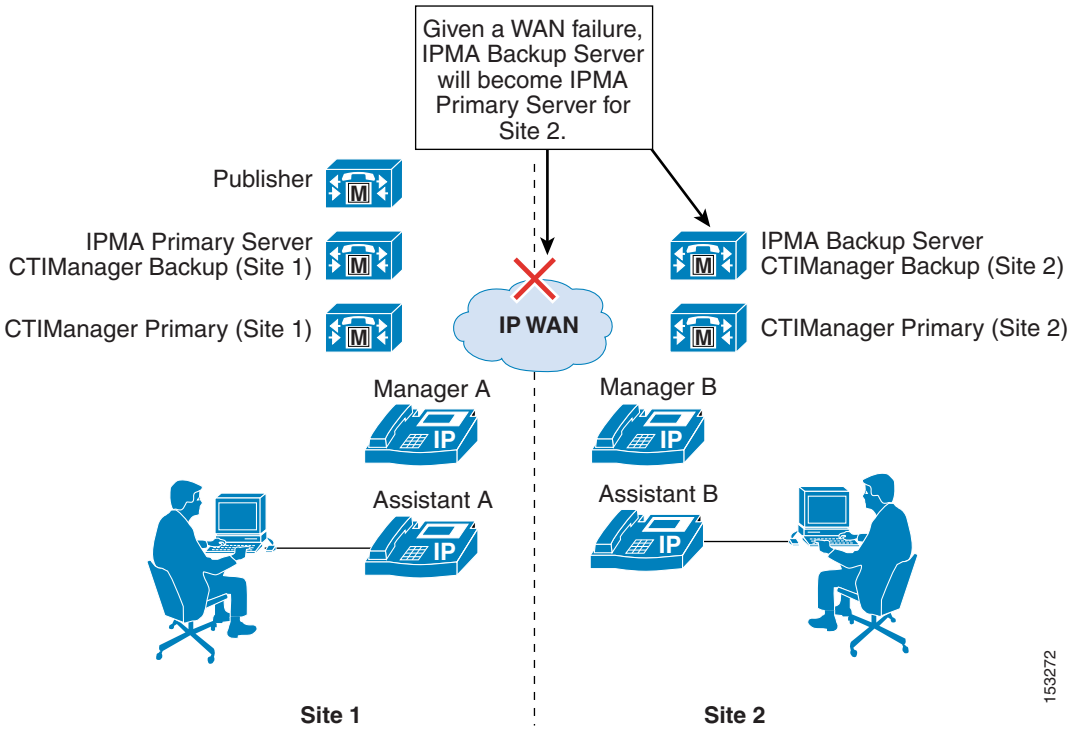
In addition, two CTIManager servers or services can be defined for each Unified CM Assistant server using the CTIManager (Primary) IP Address and CTIManager (Backup) IP Address service parameters (see Unified CM Assistant Service Parameters, page 24-18). By configuring these parameters, you can make the CTIManager service redundant. Thus, given a failure of a primary CTIManager, CTIManager services can still be provided by the backup CTIManager. If all Cisco IP Manager Assistant and CTIManager services on cluster nodes fail, the Unified CM Assistant route point, Unified CM Assistant Console desktop application and phone service, and in turn the Unified CM Assistant application as a whole will fail. However as noted previously, given a failure of the Unified CM Assistant application, the CFNA fall-through mechanism will continue to work, allowing calls to a Manager to be routed directly to the Manager's phone.

Note If configured in Unified CM Assistant shared-line mode, a complete failure of Cisco IP Manager Assistant and CTIManager service will not keep the Assistant from continuing to handle calls on behalf of the Manager because the phones will continue to shared a line. However, the Unified CM Assistant Console desktop application and phone service and the DND feature will not be available.

Figure 24-10 shows an example redundancy configuration for Unified CM Assistant and CTIManager primary and backup servers in a two-site deployment with clustering over the WAN. In order to provide maximum redundancy, a node at Site 1 is configured as the primary Unified CM Assistant server and a node at Site 2 is configured as the backup Unified CM Assistant server. In the event of a WAN failure, the backup Unified CM Assistant server at Site 2 will become a primary Unified CM Assistant server because the existing primary Unified CM Assistant server will be unreachable from Site 2. In this way, Unified CM Assistant servers can be made redundant in the clustering-over-the-WAN environment given a WAN failure. Furthermore, with a primary and backup CTIManager configured at both Site 1 and Site 2, CTIManager is made redundant given a WAN failure, and additional redundancy is provided for a CTIManager failure at each site.

Note The redundancy scenario depicted in Figure 24-10 shows a special circumstance. During normal operation it is not possible to have any pair of Unified CM Assistant servers active at the same time. If an active and backup pair of Unified CM Assistant servers can communicate over the network, then one server will be in backup mode and cannot handle requests.

Figure 24-10 Unified CM Assistant Redundancy with Two-Site Clustering over the WAN



As previously mentioned, the publisher is a single point of failure when it comes to writing Unified CM Assistant information to the Unified CM database. Given a publisher failure, all aspects of the Unified CM Assistant application will continue to work; however, no changes to the Unified CM Assistant application configuration can be made. Configuration changes via the Unified CM Assistant Console desktop application, the Manager configuration web-based application, the phone softkeys, or the Unified CM Assistant phone service, will not be possible until the publisher is restored. This condition includes enabling or disabling features such as Do Not Disturb, DivertAll, Assistant Watch, and call filtering, as well as changing call filter and assistant selection configuration.

Device and Reachability Redundancy

Redundancy for Unified CM Assistant at the devices level relies on a number of mechanisms. First and foremost, manager and assistant phones as well as the Unified CM Assistant RP rely on the built-in redundancy provided by a combination of the device pool and Unified CM group configuration for device registration.

In addition, some devices rely on component services for additional redundancy and functionality. For example, the Unified CM Assistant RP also relies on CTIManager for call control functionality and therefore must rely on the primary and back CTIManager mechanism described in the previous section.

The Unified CM Assistant Console desktop application also relies on the component services for redundancy and functionality. The Assistant Console desktop application supports automatic failover from the primary to the backup Unified CM Assistant server (and vice versa) in order to continue to handle incoming calls for managers. The amount of time this automatic failover will take can be controlled using the Cisco IPMA Assistant Console Heartbeat Interval and the Cisco IPMA Assistant Console Request Timeout service parameters (see Unified CM Assistant Service Parameters, page 24-18). Although the heartbeat or keep-alive frequency can be configured so that failures of the Unified CM Assistant server are detected by the desktop application more quickly, be careful not to affect the network adversely by sending keep-alives too frequently. This consideration is especially important if there are a large number of Assistant Console desktop applications in use.

The Unified CM Assistant Console phone service, unlike the Unified CM Assistant Console desktop application, requires manual intervention for redundancy given the failure of the primary Unified CM Assistant server. If the primary Unified CM Assistant server goes down, assistants using the phone console will not see an indication of this condition. However, the assistant phone will receive a "Host not found Exception" message upon trying to use a softkey. In order to continue using the phone console with the backup Unified CM Assistant server, the user must manually select the secondary Unified CM Assistant phone service from the IP Services menu and log in again.

There are several other failover mechanisms which ensure that Manager and Assistant reachability are redundant. First, calls sent to a Manager's Assistant via the Unified CM Assistant application (in proxy line mode) can be forwarded to the Manager's next available Assistant if the call is not answered after a configured amount of time. If the next Assistant does not answer the call after the configured amount of time, the call can again be forwarded to the Manager's next available Assistant, and so on. The mechanism is configured using the Cisco IPMA RNA Forward Calls and Cisco IPMA RNA Timeout service parameters (see Unified CM Assistant Service Parameters, page 24-18). Second, as mentioned previously, if all Cisco IP Manager Assistant and CTI services on cluster nodes fail, the Unified CM Assistant RP will become unavailable. However, based on the CFNA configuration of the Unified CM Assistant RP, calls to all Manager DNs will fall-through directly to the Manager phones so that Manager reachability is sufficiently redundant.

Guidelines and Restrictions for Unified CM Assistant

Unified CM Assistant has the following limitations with regard to overlapping and shared extensions, which you should keep in mind when planning directory number provisioning:

- With Unified CM Assistant in proxy line mode, the proxy line number(s) on the assistant phone should be unique, even across different partitions.
- With Unified CM Assistant in proxy line mode, two Managers cannot have the same Unified CM Assistant controlled line number (DN), even across different partitions.

When enabling Multiple Active Mode and using more than one Unified CM Assistant server pool, ensure that the appropriate server pool (1 to 3) is selected in the Assistant Pool field under the end user Manager Configuration page so that Managers and Assistants are evenly distributed between the Unified CM Assistant server pools. A Manager's associated Assistant will automatically be assigned to the pool where their Manager is configured.

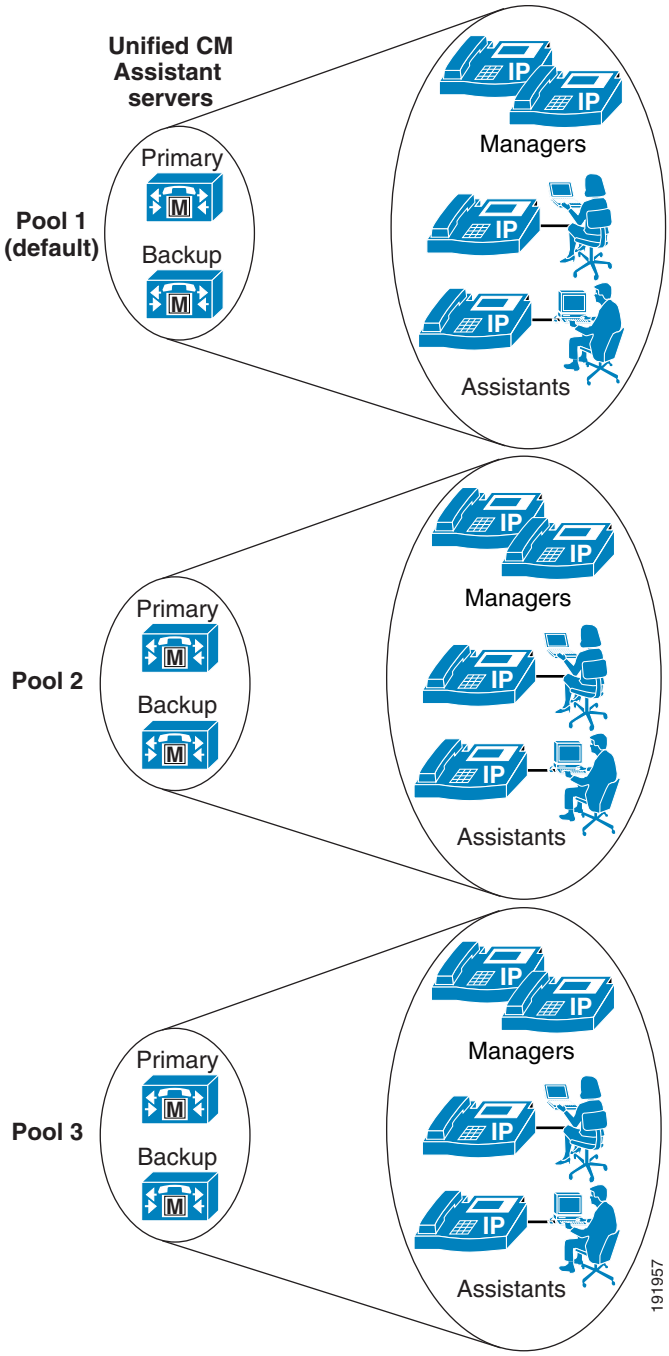
Unified CM Assistant Performance and Capacity

The Cisco Unified CM Assistant application supports the following capacities:

- A maximum of 10 Assistants can be configured per Manager.
- A maximum of 33 Managers can be configured for a single Assistant (if each Manager has one Unified CM Assistant-controlled line).
- A maximum of 3500 Assistants and 3500 Managers (7000 total users) can be configured per cluster using the Cisco MCS 7845 server.
- A maximum of three pairs of primary and backup Unified CM Assistant servers can be deployed per cluster if the Enable Multiple Active Mode advanced service parameter is set to True and a second and third pool of Unified CM Assistant servers are configured (see Unified CM Assistant Service Parameters, page 24-18).

In order to achieve the maximum Unified CM Assistant user capacity of 3500 Managers and 3500 Assistants (7000 users total), multiple Unified CM Assistant server pools must be defined. As illustrated in Figure 24-11, up to three pools can be configured. Each pool consists of a primary and backup Unified CM Assistant server and a group of Managers and Assistants. Pool 1's Unified CM Assistant servers are configured with the Cisco IPMA Server (Primary/Backup) IP Address service parameters, Pool 2's servers are configured with the Pool2: Cisco IPMA Server (Primary/Backup) IP Address advanced service parameters, and Pool 3's servers are configured with the Pool3: Cisco IPMA Server (Primary/Backup) IP Address advanced service parameters (see Unified CM Assistant Service Parameters, page 24-18).

Figure 24-11 Multiple Active Mode with Unified CM Assistant Server Pools



The Cisco Unified CM Assistant application interacts with the CTIManager for line monitoring and phone control. Each line (including Intercom lines) on a Unified CM Assistant or Manager phone requires a CTI line from the CTIManager. In addition, each Unified CM Assistant route point requires a CTI line instance from the CTIManager. When you configure Unified CM Assistant, the number of required CTI lines or connections must be considered with regard to the overall cluster limit for CTI lines or connections. (For more information on CTI connection limits per cluster, see Unified CM Capacity Planning, page 8-22.) If additional CTI lines are required for other applications, they can limit the capacity of Unified CM Assistant.

Unified CM Assistant Interactions with EM

Unified CM Assistant Managers can use EM to log in to their phones in both proxy-line and shared-lined modes. However, the Manager must be configured as a Mobile Manager under the Cisco Unified CM Assistant Manager configuration page of the End-user Directory. When using EM in conjunction with Unified CM Assistant, users should not be able to log in to more than one phone using EM. This behavior can be enabled/disabled via the EM service parameter Multiple Login Behavior (see EM Service Parameters, page 24-11). If multiple EM logins by the same user are required within the cluster, Unified CM Assistant Managers who use EM should be instructed not to log in to multiple phones. Allowing a manager to log in to two different phones with EM violates the previously stated restriction that, in proxy line mode, two Managers cannot have the same Unified CM Assistant controlled line number (DN), even across different partitions.

Note Unified CM Assistants cannot use EM to log in to their phones because there is no concept of a Mobile Assistant.

Attendant Consoles

Attendant console integrations enable a receptionist to answer and transfer or dispatch calls within an organization from a desktop application designed specifically for this purpose. Attendant consoles allow for access to the corporate directory and, in some cases, monitoring of line state for specific users. The Cisco Unified Communications portfolio provides two distinct types of attendant consoles:

- Cisco Unified Communications Manager Attendant Console, page 24-34
- Cisco Unified Department, Business, and Enterprise Attendant Consoles, page 24-46

Cisco Unified Communications Manager Attendant Console

The Cisco Unified Communications Manager Attendant Console (Unified CM Attendant Console) is a client/server Java application installed on an attendant's Windows PC. The Unified CM Attendant Console application connects to the Cisco CallManager Attendant Console Server service enabled on a Unified CM subscriber node for login services, line state, and directory services. Multiple Unified CM Attendant Consoles can connect to a single Cisco CallManager Attendant Console Server service.

Note The Cisco Unified Communications Manager Attendant Console has reached End Of Sale (EoS) status, and it is no longer available to new installations of Cisco Unified Communications Manager 7.0 or later releases. Existing Cisco Unified Communications Manager customers on an earlier release, who are upgrading to 7.0, will be able to retain the use of their Cisco Unified Communications Manager Attendant Console. For more information on the EoS announcement, visit http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps7046/ps7282/end_of_life_notice_c51-499091.html.

Unified CM Attendant Console Phone Support

The following SCCP phones support Unified CM Attendant Console functionality:

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phones 7912G and 7912G-A
- Cisco Unified IP Phones 7940G, 7941G, 7941G-GE, 7942G, and 7945G
- Cisco Unified IP Phones 7960G, 7961G, 7961G-GE, 7962G, and 7965G
- Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G
- Cisco IP Communicator

Unified CM Attendant Console is not supported on SIP phones.

Unified CM Services and Unified CM Attendant Console Service Parameters

To enable the Unified CM Attendant Console application, the system administrator must activate and start a number of Unified CM feature services from the Cisco Unified Serviceability interface. In addition, Unified CM Attendant Console service parameters provide configuration and customization options for determining how the Unified CM Attendant Console application behaves.

Unified CM Services for Unified CM Attendant Console

The Unified CM Attendant Console application relies on the following feature services, which must to be activated manually from the Serviceability page:

- Cisco CallManager Attendant Console Server
- Cisco CTIManager

The Cisco CallManager Attendant Console Server service provides an interface for the Unified CM Attendant Console Desktop application and interacts with the Cisco CTIManager service and Unified CM database. The Cisco CTIManager service interfaces and interacts with the Cisco CallManager service and the Cisco CallManager Attendant Console Server service for phone and call control. It also interfaces with the Unified CM Attendant Console Desktop application.

Unified CM Attendant Console Service Parameters

The following items represent a partial list of Cisco CallManager Attendant Console Server Service Parameters related to Unified CM Attendant Console functionality:

- Directory Sync Period (Default value = 3)

  This parameter specifies the frequency interval, in hours, for the synchronization of the Unified CM Attendant Console server AutoGenerated.txt file with the Unified CM End-user Directory. Changes to the End-user Directory will not be reflected in the AutoGenerated.txt file until this interval is reached.

- JTAPI Username (Default value = ac)

  This parameter specifies the application user name that the Unified CM Attendant Console server uses to log into and communicate with the CTIManager.

- Device Authentication Application Username (Default value = ACDeviceAuthenticationUser)

  This parameter specifies the application user name that the Unified CM Attendant Console server uses for authentication of the attendant phone.

For a complete list of Attendant Console service parameters, refer to the Unified CM Attendant Console information in the *Cisco Unified Communications Manager Features and Services Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Unified CM Attendant Console Device Authentication Application Users

For proper operation of Unified CM Attendant Console, an application user named **ac** must be configured in Unified CM. The ac application user is required in order for the Unified CM Attendant Console server to interact with the CTIManager. Without this application user configuration, attendants will not be able to receive calls.

Note Application users are different than end users within the Cisco Unified CM database, and application users are stored separately from the end users in the directory. Therefore, directory searches will not return application user entries. For more details on Application Users and End Users in Cisco Unified CM see LDAP Directory Integration, page 17-1.

The ac user must be configured with the following group permissions under the application user configuration page:

- Standard CTI Allow Control of All Devices
- Standard CTI Allow Call Park Monitoring
- Standard CTI Enabled

By configuring the ac application user with the "Standard CTI Allow Control of All Devices" group permissions, you enable the CTI Super Provider feature. The Super Provider feature allows the Unified CM Attendant Console application to control and monitor (via CTI) any device or line, which eliminates the need for associating attendant phones and Unified CM Attendant Console pilot points to the ac application user, thus greatly simplifying configuration.

An administrator might want to change this application user name to something other than ac. If a user name other than ac is configured, the JTAPI Username service parameter (see Unified CM Attendant Console Service Parameters, page 24-35) must be set to the new user name.

In addition to adding the ac user and assigning the group permissions listed above, you should create a device authentication application user named ACDeviceAuthenticationUser. Once configured, all attendant phones must be associated with this application user. This application user is used by the Unified CM Attendant Console server to authenticate attendant phones. No group permissions need to be configured for this application user account.

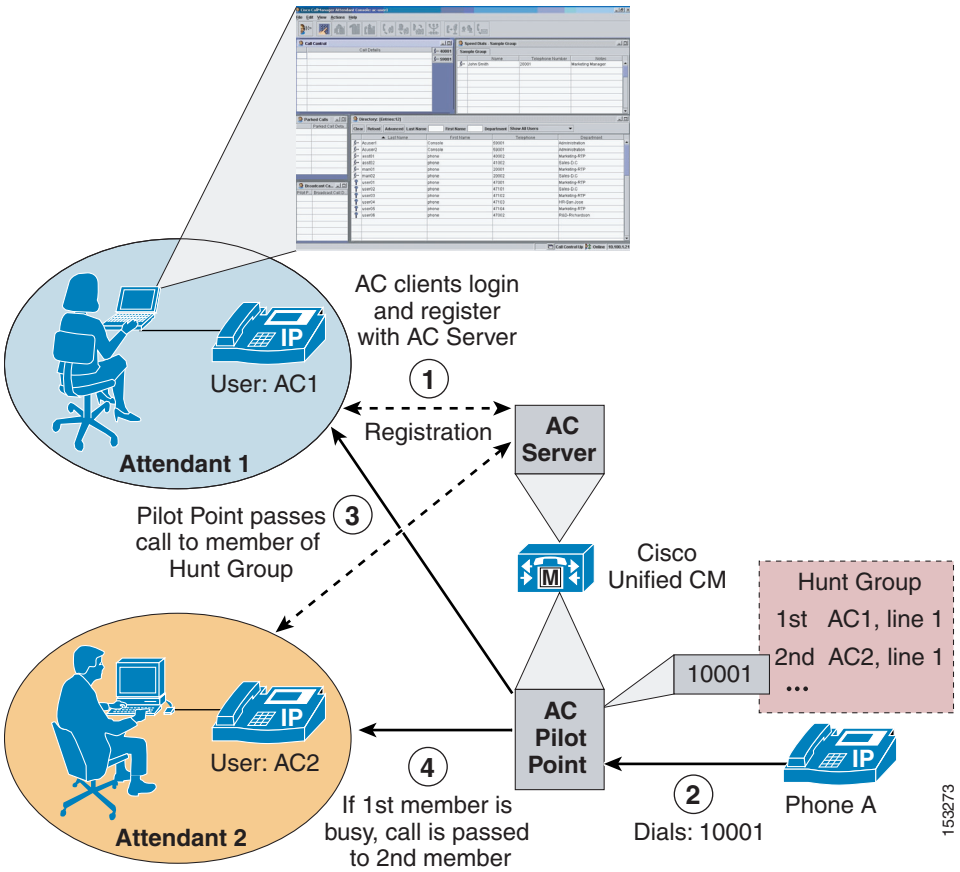
If an administrator chooses to use a different application user account name instead of ACDeviceAuthenticationUser, the Device Authentication Application Username service parameter (see Unified CM Attendant Console Service Parameters, page 24-35) must be changed to match the configured application user name.

Unified CM Attendant Console Functionality and Architecture

Figure 24-12 illustrates a basic example of Unified CM Attendant Console functionality and operation. First, the Unified CM Attendant Console clients log into and register with the Unified CM Attendant Console server on Unified CM (step 1). Next, Phone A calls directory number (DN) 10001 configured

for the Unified CM Attendant Console pilot point on Unified CM (step 2). The Unified CM Attendant Console pilot point intercepts this call and, based on the hunt group configuration, directs the call to one of its available members. In this case, the call is sent to line 1 of the Attendant user AC1's phone (step 3). If a second call comes into the pilot point number 10001 while user AC1 is still on the first call, the second call is routed to another available member of the hunt group, and in this case the call is forwarded to line 1 of Attendant user AC2's phone (step 4).

Figure 24-12 Basic Unified CM Attendant Console Operation



For purposes of routing calls, pilot points determine the next available member of a hunt group based on one of the following routing algorithms (configured in the "Route Calls to" field under the pilot point):

- First available

  With this algorithm, incoming calls are routed to the first member of the group who is available.

- Longest idle

  With this algorithm, incoming calls are routed to the member who has been idle (not handled a call) the longest.

- Circular hunting

  With this algorithm, incoming calls are routed to the available members in a round-robin fashion.

- Broadcast hunting

  With this algorithm, incoming calls are queued, and indication is sent to the Unified CM Attendant Console desktop application of all available members simultaneously.

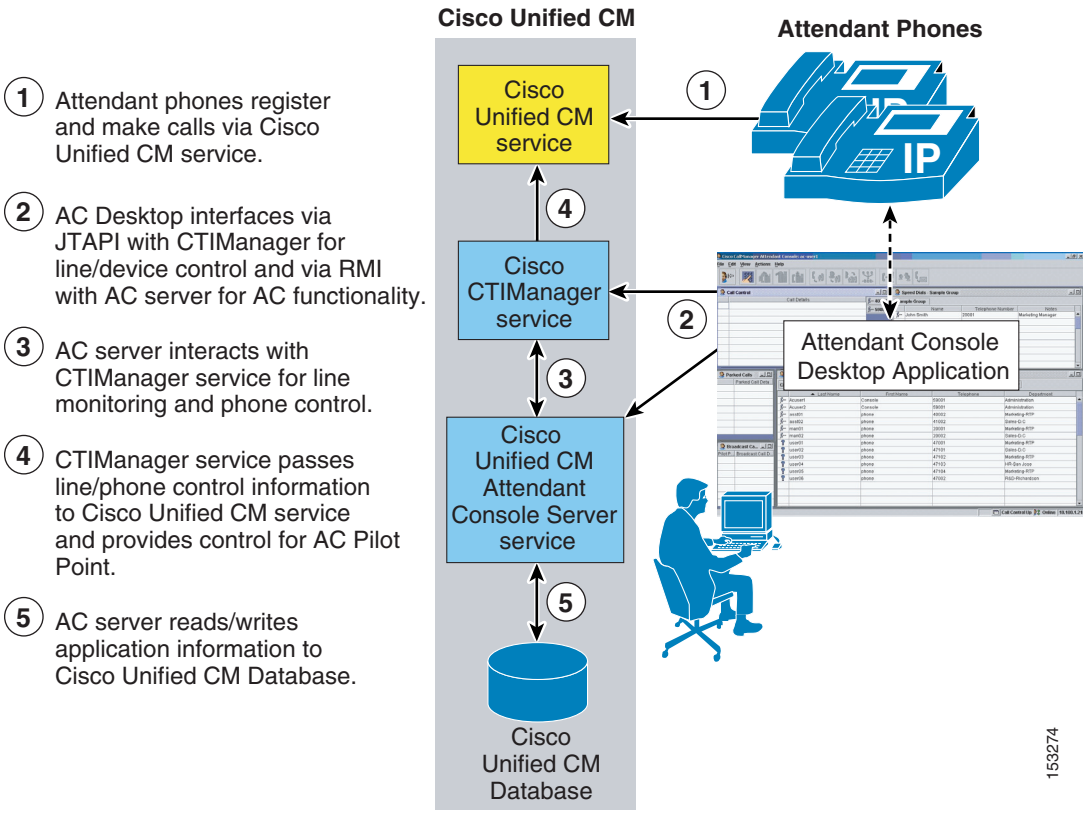
With the example shown in Figure 24-12, the First Available algorithm is used. The hunt group routing algorithm as well as the queuing settings for the Broadcast routing algorithm are all configured under the Pilot Point configuration page on Unified CM.

Unified CM Attendant Console Architecture

The architecture of the Unified CM Attendant Console application is as important to understand as its functionality. Figure 24-13 depicts the message flows and architecture of Unified CM Attendant Console. When Unified CM Attendant Console has been configured for attendant console users, the following sequence of interactions and events can occur:

1. Attendant phones register with the Cisco CallManager service, and the phone's keypad and softkeys are used to handle call flows (see step 1 in Figure 24-13).
2. The Attendant Console desktop application communicates and interfaces with the CTIManager service, using JTAPI for phone and line control. In addition, the desktop application interfaces with the Unified CM Attendant Console service and server via Remote Method Invocation (RMI) for Unified CM Attendant Console functionality (see step 2 in Figure 24-13).
3. The Unified CM Attendant Console server in turn interacts with the CTIManager service for exchanging line monitoring and phone control information (see step 3 in Figure 24-13).
4. Likewise, the CTIManager service passes Unified CM Attendant Console phone control information to the Cisco CallManager service and also controls the Unified CM Attendant Console pilot point (see step 4 in Figure 24-13).
5. In parallel, the Unified CM Attendant Console server reads and writes Unified CM Attendant Console application information to and from the Unified CM Database (see step 5 in Figure 24-13).

Figure 24-13 Unified CM Attendant Console Architecture



Note Although Figure 24-13 shows the Cisco CallManager, CTIManager, and Cisco CallManager Attendant Console Server services all running on the same node, this configuration is not a requirement. These services can be distributed among multiple nodes in the cluster, but they are shown on the same node here for ease of explanation.

Attendant Console Desktop Application

The Attendant Console desktop application is used by attendants to handle calls via a graphical virtual console. Besides call handling, the application provides additional functions such as click-to-dial speed dialing and directory entries, environment configuration, and line status and availability indication for other users within the directory and speed dial windows.

Attendant Console Installation

The Attendant Console desktop application can be downloaded from the following URL:

https://<*Server_IP-Address*>:8443/plugins/CiscoAttendantConsoleClient.exe

(where <*Server_IP-Address*> is the IP address of any node in the cluster)

Once the CiscoAttendantConsoleClient.exe file has been downloaded to an attendant's PC, it must also be installed.

Attendant Console QoS

After installing the Attendant Console desktop application, an attendant logs on to the console application by providing a Unified CM Attendant Console userID and password (as configured under the Cisco Unified CM Attendant Console User page on Unified CM).

Note Unified CM Attendant Console userIDs are required for logging into the Unified CM Attendant Console desktop application and are separate from the users configured in the end-user directory as well as the application users on Unified CM. Because these users are stored separately from the end user-directory, directory searches will not return Unified CM Attendant Console user entries.

Once the Unified CM Attendant Console user is logged on, the Unified CM Attendant Console desktop application communicates with Unified CM using Remote Method Invocation (RMI) and Java Telephony Application Programming Interface (JTAPI) protocols predominantly. RMI is used for communication between the, desktop client and the Unified CM Attendant Console server including registration, keep-alives, and information exchange. RMI traffic is sourced from Unified CM on TCP ports 1101 to 1129 and sourced from the desktop application on one or more ephemeral TCP ports. All RMI traffic is marked as best-effort.

JTAPI traffic carries device and line control information and call control traffic between the CTIManager on Unified CM and the Unified CM Attendant Console desktop application. JTAPI Traffic is sourced from Unified CM on TCP port 2748 and sourced from the desktop application on an ephemeral TCP port.

Because the JTAPI traffic between the CTIManager and Unified CM Attendant Console client is used for call control (generation and handling of call flows), this traffic is QoS-marked by Unified CM with DSCP of 24 (PHB of CS3). In this way, Unified CM Attendant Console phone control traffic can be queued throughout the network like all other call signaling traffic. In order to ensure symmetrical marking and queuing, the Attendant Console desktop application traffic destined for Unified CM TCP port 2748 should also be marked as DSCP 24 (PHB CS3) to ensure this traffic is placed in the appropriate call signaling queues along the network path toward Unified CM and the CTIManager. However, because the Unified CM Attendant Console client application marks all traffic as best-effort, an access control list (ACL) must be configured to re-mark this traffic properly.

The Unified CM Attendant Console server and desktop client marking can be summarized as follows:

- Unified CM appropriately marks all JTAPI traffic sourced from TCP port 2748 with DSCP of 24 (PHB of CS3).
- The Attendant Console desktop application marks JTAPI traffic destined for Unified CM TCP port 2748 as best-effort. This means that an ACL should be applied at the switch port level to re-mark the JTAPI traffic sent by the application to the Unified CM and Unified CM Attendant Console server from a DSCP of 0 to a DSCP of 24 (PHB of CS3).

Attendant Console Directory Window

The directory window within the Attendant Console desktop application enables an attendant to search for end-users within the Unified CM telephony environment. Typically directory listings are obtained by searching against a directory file rather than searching against the Unified CM directory itself. One of the following directory files will be searched when a Unified CM Attendant Console application user enters a search in the directory window:

- User list

  This directory file is stored on the local PC or on a local drive path. In order for this file to be searched, its name and location must be configured in the Path Name of Local Directory File field under the Advanced tab of the Attendant Settings dialog box. If a file name and location has not been configured in this field, this option is skipped and a directory search will be conducted against one of the other directory files.

- AutoGenerated.txt

  This directory file is automatically generated from the Unified CM database end-user table by the Unified CM Attendant Console server and is stored on the Unified CM server. If the local directory user list file is not configured, then the Unified CM Attendant Console desktop application will download this file from Unified CM automatically. The AutoGenerated.txt file is periodically regenerated or synchronized by the Unified CM Attendant Console server against the end-user directory to ensure that the information in the file is accurate. The frequency of this synchronization is determined by the Directory Sync Period Unified CM Attendant Console service parameter (see Unified CM Attendant Console Service Parameters, page 24-35), which by default is set to three hours, meaning that the AutoGenerated.txt file will be updated every three hours.

- CorporateDirectory.txt

  This file is available only if manually imported to Unified CM by an Administrator using the Cisco Unified CM Attendant Console User File Upload tool (under **Application > Cisco Unified CM Attendant Console**). If uploaded, this file will replace the AutoGenerated.txt file on the Unified CM server. Therefore, the Unified CM Attendant Console desktop application will download this file rather than the AutoGenerated.txt file, provided that the local user list file has not been configured.

One of the directory files listed above is downloaded (in the case of the AutoGenerated or Corporate Directory.txt files) and loaded every time the Unified CM Attendant Console desktop application is launched. The directory file is then downloaded and/or reloaded periodically, as long as the application is up, based on the Directory Reload Interval setting on the Advanced tab of the Attendant Settings dialog box. All the directory files conform to a comma-delimited format with one user entry per line.

While the additional traffic generated by downloading directory files for directory window searches within the desktop application is typically nominal, this traffic can be problematic for a number of reasons. First, if the Unified CM directory size is large, the directory file downloaded by the console application containing the entire directory can generate large amounts of traffic on the network. When this factor is coupled with large numbers of Unified CM Attendant Console desktop applications within the network, short download intervals, a centralized call processing deployment, and console applications running at remote sites over low-speed WAN links, the potential for network congestion, delay, and queuing is highly probable.

Although the use of local user list files on the desktop application PCs could likely eliminate many of the concerns about network bandwidth and congestion, the Advanced search feature within the directory window of the Unified CM Attendant Console desktop is more problematic. Whereas all other directory searches within the Unified CM Attendant Console desktop application directory window are conducted against either the local user list file or one of the downloaded files, there is an exception for searches done using the Advanced search window triggered by the Advanced button in the directory window.

Searches made using the Advanced search window bypass the directory file search convention and instead are generated directly against the Unified CM end-user directory in real time. This means additional traffic on the network above and beyond the periodic downloading of directory files. Furthermore, there is no limit on the number of entries that can be downloaded using the Advanced search feature. Not only will these real-time searches and retrievals generate additional network load, but because there is no limiting of returned entries, this additional load can be quite large. Fortunately, the traffic generated by both the directory file download and the Advanced directory search use the RMI protocol, which is marked as best-effort, so there is no risk of congesting priority voice media and provisioned call signaling queues on the network path. However, the possibility still exists that the Unified CM Attendant Console desktop application directory traffic could cause congestion of the best-effort queues and lead to dropping of both directory traffic and other best-effort network data traffic.

Given the potential for network congestion with Unified CM Attendant Console desktop application directory file downloads and directory searches, Cisco recommends the following practices:

- Administrators should encourage all Attendant Console users to limit their use of the Advanced directory search feature. Furthermore, if users are going to use the feature, they should be urged to enter as much information as possible in the Advanced search parameter fields in order to reduce the number of entries returned.
- In centralized call processing deployment scenarios, user list files on the Unified CM Attendant Console client PCs or on a network shares should be utilized for remote site Unified CM Attendant Console users to eliminate periodic downloading of a directory file from Unified CM across low-speed WAN links. One method for achieving this goal with minimal management overhead is to make a user list file available on a local network share at each remote site. It should be investigated to have a user list file automatically generated from the directory and then loaded onto remote network shares during off-peak or overnight hours, thereby eliminating the potential for network congestion during peak business hours. Then each morning, when Unified CM Attendant Console users launch the desktop console, the application can download the most up-to-date directory user list.

These recommendations are especially critical if one or more of the following conditions are true:

- There are many Unified CM Attendant Console users within a Unified CM cluster.
- There are significant numbers of Unified CM Attendant Console users separated from Unified CM servers by low-speed WAN links.
- The end-user directory is very large.

Unified CM Attendant Console Redundancy

Unified CM Attendant Console application redundancy can be provided at two levels:

- Redundancy at the component and service level

  At this level, redundancy must be considered with regard to Unified CM Attendant Console service or server redundancy and CTIManager service redundancy. Likewise, the lack of publisher redundancy and the impact of this component failing should also be considered.

- Redundancy at the device and reachability level

  At this level, redundancy should be considered as it relates to attendant phones, the Unified CM Attendant Console pilot point, and the Attendant Console desktop application, as well as redundancy in terms of attendant and pilot point reachability.

Service and Component Redundancy

As shown in Figure 24-13, Unified CM Attendant Console functionality is primarily dependent on the Cisco CallManager Attendant Console Server service and the Cisco CTIManager service. In both cases, redundancy is built into the Unified CM cluster architecture. Redundancy for both the Unified CM Attendant Console Server service and the CTIManager service is determined by the number of nodes within the cluster where each service is running. Redundancy is determined by the number of server failures that can occur while still providing the required service, which can be expressed using the formula (N - 1), where N is the number of servers running the service. For example, if three servers in the cluster are running the Cisco CallManager Attendant Console Server service, then N = 3. Redundancy for this service can then be calculated as (3 - 1), or 2. Thus, redundancy is ensured for up to two server failures. CTIManager redundancy can be calculated using the same formula. In order to provide maximum redundancy for these services, Cisco recommends running both the Unified CM Attendant Console Server and CTIManager services on all call processing nodes within the cluster. However, for minimum redundancy, each of these services should run on at least two call processing nodes within the cluster.

The publisher is a single point of failure when it comes to writing Unified CM Attendant Console application information to the Unified CM Database. The affect of a publisher failure on the Unified CM Attendant Console application is minimal. Given a publisher failure, all aspects of the Unified CM Attendant Console application will continue to work; however, no changes to Unified CM Attendant Console application configuration can be made. Configuration changes to Unified CM Attendant Console pilot points, hunt groups, and attendant phones will not be possible until the publisher is restored.

Device and Reachability Redundancy

Redundancy for Unified CM Attendant Console at the device level relies on a number of mechanisms. First and foremost, attendant phones as well as the Unified CM Attendant Console pilot point rely on the built-in redundancy provided by a combination of the device pool and Unified CM group configuration for device registration.

In addition, some devices rely on component services for additional redundancy and functionality. For example, the Unified CM Attendant Console pilot point also relies on CTIManager for call control functionality and must therefore rely on CTIManager redundancy as described in the previous section.

The Attendant Console desktop application also relies on the component services for redundancy and functionality. The Unified CM Attendant Console desktop application supports automatic failover between redundant Unified CM Attendant Console Servers and CTIManager services in order to continue to handle incoming calls. Redundancy of these services from perspective of the Unified CM Attendant Console desktop application is determined by the Unified CM group mechanism as described below. First, when the Unified CM Attendant Console desktop application is launched and the attendant logs in, the application downloads a list of Unified CMs based on the device pool and Unified CM group configuration of the attendant phone. This list is stored in the GlobalSettings.xml file on the local PC and determines CTIManager service redundancy for the desktop.

Note Cisco recommends that the IP address of the primary Unified CM server configured in the Unified CM group for the attendant's phone be entered in the Attendant Server Host Name or IP Address field under the Basic tab of the Attendant Settings dialog boxes. This entry ensures that, if a failure occurs, both the attendant phone and the Unified CM Attendant Console desktop application will simultaneously fail-over to the next server in the phone's configured Unified CM group.

Next, the desktop application relies on the device pool and Unified CM group of the Unified CM Attendant Console pilot point (of which the attendant phone is a member) for Unified CM Attendant Console server redundancy. In both cases, up to tertiary redundancy is provided because up to three servers can be configured in a Unified CM group.

Further redundancy for these services can be provided for the desktop application via the Call Processing Server Host Names or IP Addresses field under the Advanced tab of the Attendant Settings dialog box. By configuring a comma-separated list of Unified CM servers in this field, additional redundancy beyond the Unified CM group mechanism can be provided. However, because this additional redundancy is useful only if the group mechanism has been exhausted, it might be unnecessary. This additional redundancy would really be used only in the event that the first three servers providing registration services for the attendant phone and Unified CM Attendant Console pilot point are unavailable, which means that the attendant phone and Unified CM Attendant Console pilot point are also unavailable. If the phone and pilot point are unavailable, then the desktop application is of no use.

Finally, besides the reachability redundancy built into the hunt group mechanism under the Unified CM Attendant Console pilot point, which provides incoming callers with attendant redundancy, additional redundancy can be provided for a Unified CM Attendant Console pilot point failure. If a Unified CM Attendant Console pilot point fails, incoming callers dialing the pilot point number will receive a busy tone. In order to provide a failover mechanism for pilot points, another Unified CM Attendant Console pilot point number can be configured in the Call Forward No Answer (CFNA) fields of the pilot point line configuration screen. This CFNA mechanism ensures that callers to a failed pilot point will be forwarded to another pilot point for call handling and routing.

Guidelines and Restrictions for Unified CM Attendant Console

Unified CM Attendant Console is aware of partitions at the JTAPI level, therefore the Attendant Console desktop application is aware of partitions in terms of line control. However, other Unified CM Attendant Console components are not aware of partitions, or they have some limitations with regard to overlapping and shared extensions. Keep the following guidelines in mind when planning directory number provisioning:

- Hunt groups
  - Shared lines must not be used by any hunt group members.
  - Overlapping extensions must not be used by any hunt group members.
  - Hunt group member directory numbers must not be added to Unified CM line groups.
- Pilot points
  - Shared lines must not be used as pilot point directory numbers.
  - Pilot point directory numbers must not be added to Unified CM line groups.
- Console directory and speed-dial windows

  Line status displays within the console directory and speed-dial windows are unable to account for shared lines or overlapping extensions. As a result, only the status of the most recently changed line instance is shown when encountering shared or overlapping line appearances.

Also ensure that all Unified CM Attendant Console pilot points are configured with a calling search space that includes all partition in which hunt group member directory numbers reside. Failure to do so will result in one or more members being unreachable.

Unified CM Attendant Console Performance and Capacity

The Cisco Unified CM Attendant Console application supports the following capacities:

- Maximum of 500 attendants per cluster.
- Maximum of 500 pilot points per cluster.
- Maximum of 125 attendant and pilot point pairs per Cisco MCS-7845 server
- Maximum of 100 attendant and pilot point pairs per Cisco MCS-7835 server
- Maximum of 75 attendant and pilot point pairs per Cisco MCS-7825 server
- The Cisco MCS-7845 server supports a maximum of 1250 Unified CM Attendant Console devices.
- The Cisco MCS-7835 server supports a maximum of 1000 Unified CM Attendant Console devices.
- The Cisco MCS-7825 server supports a maximum of 750 Unified CM Attendant Console devices.

Note The Unified CM Attendant Console device capacity numbers can be divided among hunt pilots and hunt pilot members. For example, with an MCS-7845 server, the maximum number of Unified CM Attendant Console devices is 1250. This capacity can be allocated in a number of ways, such as 125 hunt pilots with 10 members in each hunt pilot, or 10 hunt pilots with 125 members in each hunt pilot.

In order to support the maximum of 500 attendants and 500 pilot points, attendants and pilot points must be distributed across multiple servers in groups of no more than 125 pairs per MCS-7845 server, no more than 100 pairs per MCS-7835 server, and no more than 75 pairs per MCS-7825 server.

The Cisco Unified CM Attendant Console application interacts with the CTIManager for line monitoring and phone control. Each line on an Attendant phone requires a CTI line from the CTIManager. In addition, each Unified CM Attendant Console pilot point requires a CTI line from the CTIManager. When you configure the Unified CM Attendant Console application, the number of required CTI lines or connections must be considered with regard to the overall cluster limit for CTI lines or connections. (For more information on CTI connection limits per cluster, see Unified CM Capacity Planning, page 8-22.) If additional CTI lines are required for other applications, they can limit the capacity of the Unified CM Attendant Console application.

Unified CM Attendant Console Interactions with EM

Unified CM Attendant Console users can log in to their phones using EM. However, the Unified CM Attendant Console desktop application requires Unified CM Attendant Console users to log out and back into the application whenever there is a configuration change on the attendant phone. Because an EM login (or logout) results in a configuration change on the phone, when using Unified CM Attendant Console and EM together, users should first log in to their phone using EM and then log in to the Unified CM Attendant Console desktop application, thus eliminating the need to log out and back on to the desktop application.

In addition, EM and Unified CM Attendant Console user DNs should be added to Unified CM Attendant Console pilot point hunt groups as User Members rather than Device Members. This practice ensures that incoming calls will not be routed to a Unified CM Attendant Console user who is unavailable due to the fact that they are not logged into their phone using EM. User Members of a hunt group are configured with both a user name and line number, while Device Members are simply configured with a directory number. The pilot point routes calls to Device Members after checking to see only that the directory number is not busy. The pilot point routes calls to User Members after verifying that the line number of the attendant phone is available and that the Unified CM Attendant Console user is logged on

and online. Thus, by adding EM Unified CM Attendant Console users to a hunt group as User Members, you can ensure that a call will be sent to that user phone only if the EM Unified CM Attendant Console user is logged in.

Cisco Unified Department, Business, and Enterprise Attendant Consoles

The Cisco Unified Department, Business, and Enterprise Attendant Consoles have a client attendant console application that installs on an attendant's Windows PC. It also requires an attendant console server application installed on a separate physical server than Unified CM. The attendant console application communicates with the attendant console server application, and the attendant console server application communicates with Unified CM securely through CTI and AXL over Secure Socket Layer (SSL). Multiple attendant consoles can connect to a single attendant console server. The Department, Business, and Enterprise versions of the attendant console differ in their limits to various capabilities such as the number of supported operator clients and the number of supported directory entries.

Functionality and Architecture

Figure 24-14 illustrates the high-level architecture of a Cisco Unified Department, Business, or Enterprise Attendant Console integration. Understanding the functionality and operation of the solution enhances the understanding of the architecture itself. The following steps (denoted in Figure 24-14) detail the events involved for a typical call into an attendant console.

1. A call comes into Unified CM, and the called number matches the directory number configured on a CTI route point.
2. The CTI route point is CTI-controlled by the attendant console server application and is associated with a Queue Direct Dial In (DDI) configured on the server.
3. The attendant console server application immediately redirects the call internally to one of its Computer Telephony (CT) Gateway Devices. As part of this process, the attendant console server application sends a CTI redirect message to the CTI Manager service to redirect the call to a CTI port.

Note A CTI redirect message does not result in a connected call; the call is not answered and there is no media connection.

4. The attendant console server application now associates the call with the CT Gateway Device and controls the call on the CTI port.
5. At this point, the call is presented to the attendant console client applications in the system that are associated with the Queue DDI.
6. Once an attendant chooses to answer the call through the attendant console client application, another CTI redirect message is sent to the CTI Manager service, which moves the call from the CTI port to the answering attendant's physical phone. The call is automatically connected on the attendant's phone, either to the handset or the headset, depending on the phone configuration. The region and location settings of the attendant's phone and the initiating gateway or phone dictate the codec used for media.
7. When a transfer to another extension is required, the attendant initiates the transfer through the attendant console client application, which communicates the transfer to the attendant console server application.

8. The attendant console server application internally associates the call with a Service Queue and sends a CTI redirect message to the CTI Manager service. This redirects the call from the attendant's phone to a CTI port controlled by the attendant console server application.

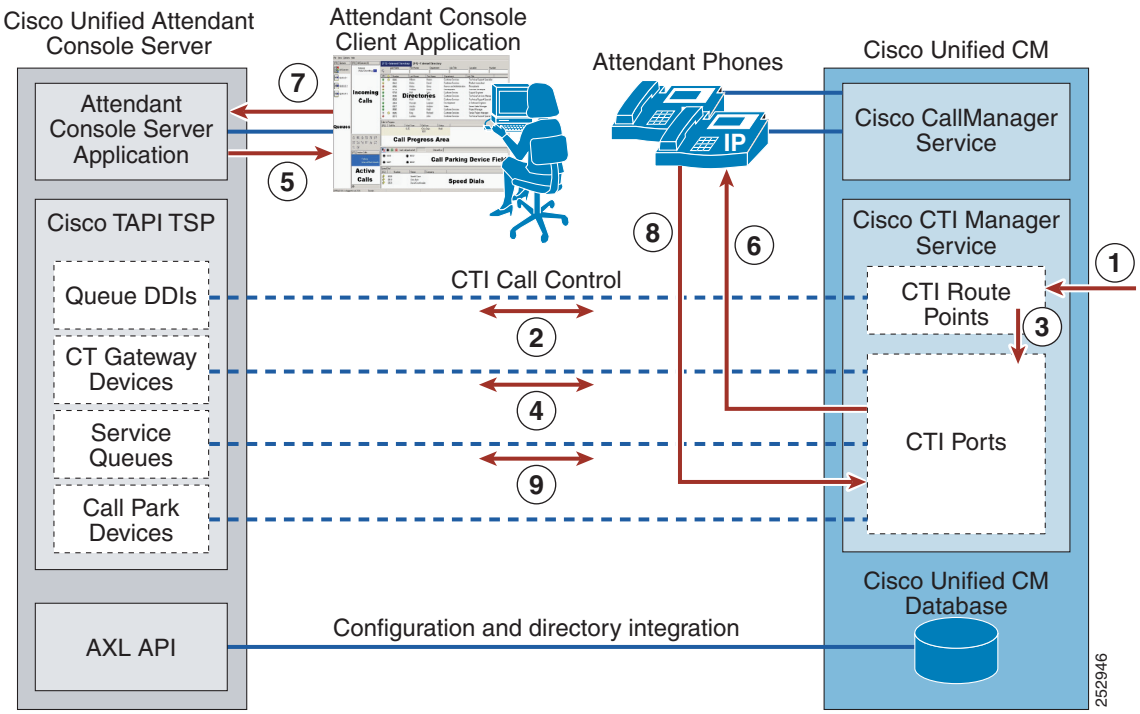
Note A call transfer may also be initiated from the attendant's phone; however, this would remove the attendant console server application from the call flow, and enhanced functionality (such as the transfer recall feature) would no longer be possible.

9. At this stage, the Service Queue actually answers the call (there is a short connect) before issuing the transfer, therefore the Cisco TAPI Wave driver installed on the attendant console server application is invoked. The region and location settings of this CTI port and the call-initiating gateway or phone dictate the codec used for media. The configured Music on Hold (MoH) audio sources of the CTI port also affect the MoH heard by the caller. Transfers are performed in this manner so that the attendant console client application still maintains control of the call if there is no answer. Once the call is received by the final party, the attendant console server application is removed from the call flow.

Note The Cisco TAPI Wave Driver installed on the attendant console server application supports only the G.711 codec. When configuring the CTI ports correlating with Service Queues and Call Park Devices, design the system so that these CTI ports have a region setting with other devices that dictates the use of G.711, or else provide transcoding media resources.

Note Cisco TAPI Wave Driver support for the G.711 a-law codec was introduced in Cisco Unified CM 7.1(2) and in Cisco TSP 7.1(3.3) and later releases.

Figure 24-14 Architecture for Cisco Unified Department, Business, and Enterprise Attendant Consoles



The attendant console server application's call park function does not use the inherent call park feature of Unified CM. Instead, it uses its own call park facility using Call Park Devices. Call Park Devices work very much like the Service Queues as outlined in steps 7 to 9 of Figure 24-14. Similar to transfers, Call Park Devices allow the attendant console server application to maintain control of the call for the duration of the parked call. The Cisco TAPI Wave Driver codec limitation (support of G.711 only) also affects calls involving Call Park Devices.

Redundancy

You should consider providing redundancy on both sides of the integration for both CTI and AXL communication.

Regarding CTI, the attendant console server application uses the Cisco Telephony Service Provider (TSP) plug-in (downloaded from Unified CM) to communicate with the CTI Manager service. Cisco TSP allows for the configuration of a primary and backup CTI Manager service. Cisco recommends enabling the CTI Manager service on at least two Unified CM subscriber nodes in the cluster to gain resilience in case the primary CTI Manager service goes offline. Currently there are no resiliency capabilities for the attendant console server application. Therefore, in the event of an attendant console server failure, resilience can be achieved by configuring a Call Forward No Answer (CFNA) destination on all of the CTI route points associated with Queue DDIs. If the attendant console server application is offline, calls will automatically follow the CFNA setting. For example, the destination could be a Hunt Pilot number or a Directory Number (DN) associated with a single IP phone.

AXL communication is enabled by activating the Cisco AXL Web Service on a Unified CM node. Multiple Unified CM nodes can have the Cisco AXL Web Service enabled, but the attendant console server application has only a single entry for Unified CM connectivity. In the event of a failure, an administrator could update this entry to a backup Unified CM node running the Cisco AXL Web Service.

The Unified CM also has a series of CTI route points and CTI ports configured for integration with the Unified Department, Business, and Enterprise Attendant Console solutions. These devices have a device pool and therefore are assigned a Unified CM group, which specifies a prioritized list of the Unified CM call processing nodes responsible for maintaining registration. When the primary Unified CM in the Unified CM group is offline, the CTI route points and CTI ports have the ability to register with a secondary Unified CM node, thus allowing for high availability of the CTI route points and ports themselves.

Guidelines and Restrictions

The following design guidelines and restrictions apply with regard to the deployment and operation of Cisco Unified Department, Business, and Enterprise Attendant Consoles within the Unified CM telephony environment.

- The following general design guidance applies to the attendant console server application components:
  - Queue DDI

    One unique Queue DDI is required for each unique incoming directory number in the system that should be routed specifically to the attendant consoles.
  - CT Gateway Device

    Every incoming call into a Queue DDI is immediately redirected to a CT Gateway Device. Design the system so that the number of CT Gateway Devices can handle the maximum expected number of incoming calls at any given time.
  - Service Queue

    Each time an attendant transfers a call or places a call on hold, a Service Queue is required. The system should be designed so that there are enough Service Queues to sustain the maximum number of calls that all attendants in the system are in the process of transferring or putting on hold at any given time. A general guideline is to provide 3 or 4 Service Queues per attendant, but some scenarios might require more.
  - Call Park Device

    Each time an attendant invokes the Call Park feature through the attendant console client application, a Call Park Device is required. This feature does not use the inherent Call Park capability of Unified CM. Design the system so that there are sufficient Call Park Devices to handle the maximum number of calls parked by all attendants in the system at any given time.
- Every Queue DDI, CT Gateway Device, Service Queue, and Call Park Device configured in the attendant console server application creates a CTI route point or CTI port in Unified CM. The number of CTI connections required to handle the Unified Department, Business, or Enterprise Attendant Console integration also counts toward the CTI connection limits per cluster. (For more information on CTI connection limits per cluster, see Unified CM Capacity Planning, page 8-22.)
- Each instance of an installed Cisco TSP supports a maximum of 255 CTI ports.
- The Cisco TAPI Wave Driver installed on the attendant console server application supports only the G.711 codec. When configuring the CTI ports correlating with Service Queues and Call Park Devices, design the system so that these CTI ports have a region setting with other devices that dictates the use of G.711, or else provide transcoding media resources.
- The attendant console server application provides Busy Lamp Field (BLF) monitoring of end-user devices, but it is important to note that this does not use the same facility in Unified CM that provides BLF speed dial capability. Instead, the attendant console server application communicates through CTI with Unified CM to obtain line state information on monitored devices.

- With respect to Quality of Service (QoS), the attendant console server application, the attendant console client application, and the Cisco TSP all send their traffic marked as Best Effort (DSCP=0). If this traffic traverses a WAN or a link that is typically congested, packets must be marked to receive preferential treatment through the network. For a complete list of the TCP port numbers associated with these applications, refer to the Unified Department, Business, or Enterprise Attendant Console design guide, available with appropriate login authentication at

  http://www.cisco.com/go/ac

- The attendant console server application is not aware of partitions. Therefore, if the same directory number (DN) exists in multiple partitions, the monitored device might not be the correct DN.
- The Cisco Unified Department, Business, and Enterprise Attendant Consoles can also integrate with a Cisco Unified Presence Server. For more information about this type of integration, refer to the appropriate Unified Department, Business, or Enterprise Attendant Console administration guide, available at

  http://www.cisco.com/en/US/products/ps7282/prod_maintenance_guides_list.html

- For performance and capacity information about the various Unified Department, Business, and Enterprise Attendant Consoles, refer to the product documentation available at

  http://www.cisco.com/en/US/products/ps7282/tsd_products_support_series_home.html

WebDialer

WebDialer is a click-to-call application for Unified CM that enables users to place calls easily from their PCs using any supported phone device. There is no requirement for administrators to manage CTI links or build JTAPI or TAPI applications because Cisco WebDialer provides a simplified web application and HTTP or Simple Objects Access Protocol (SOAP) interface for those who want to provide their own user interface and authentication mechanisms. Alternatively, the **Click to Call** Cisco Unified Communications Widget makes use of the SOAP interface and is currently available for download (login authentication required) at

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

WebDialer Phone Support

The following SCCP phones support WebDialer:

- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phones 7912G and 7912G-A
- Cisco Unified Wireless IP Phones 7920, 7921G, and 7925G
- Cisco Unified IP Phones 7935G, 7936G, and 7937G
- Cisco Unified IP Phones 7940G, 7941G, 7941G-GE, 7942G, and 7945G
- Cisco Unified IP Phones 7960G, 7961G, 7961G-GE, 7962G, and 7965G
- Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G
- Cisco Unified IP Phone 7985G

- Cisco IP Communicator

The following SIP phones also support WebDialer:

- Cisco Unified IP Phone 7906G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phones 7941G, 7941G-GE, 7942G, and 7945G
- Cisco Unified IP Phones 7961G, 7961G-GE, 7962G, and 7965G
- Cisco Unified IP Phones 7970G, 7971G-GE, and 7975G
- Cisco IP Communicator

Note Cisco Unified Personal Communicator supports WebDialer only when running in deskphone mode. With Cisco Unified Personal Communicator in deskphone mode, WebDialer can be used to provide click-to-call functionality for the desk phone as long as it is a phone model supported by WebDialer. Cisco Unified Personal Communicator in softphone mode does not support WebDialer.

Unified CM Services and WebDialer Service Parameters

To enable the WebDialer application, the system administrator must activate and start a number of Unified CM feature services from the Cisco Unified Serviceability interface. In addition, WebDialer service parameters provide configuration and customization options for determining how the WebDialer application and services behave.

Unified CM Services for WebDialer

The WebDialer application relies on the following feature services, which must be activated manually from the Serviceability page:

- Cisco WebDialer Web Service
- Cisco CTIManager

The Cisco WebDialer Service is the interface point between click-to-call web-based and desktop-based applications and Unified CM. The Cisco CTIManager Service processes requests received from the WebDialer service by interacting with the Unified CM call processing and database layers. The net result exposes phone and call control capabilities to the applications.

WebDialer Service Parameters

The following items represent a partial list of Cisco WebDialer Web Service service parameters related to WebDialer functionality:

- CTI Manager Connection Security Flag (Default value = Non Secure)

  This parameter determines whether a secure Transport Layer Security (TLS) connection is used between the Cisco WebDialer Web service and the CTIManager. If enabled, a secure connection is configured using the Certificate Authority Proxy Function (CAPF) profile configured for the instance ID of the application user WDSecureSysUser. The instance ID must be specified under the CAPF Profile Instance ID for Secure Connection to CTIManager service parameter.

Note The application user WDSecureSysUser is a system account created automatically at installation. It cannot be deleted.

- CAPF Profile Instance ID for Secure Connection to CTI Manager (Default value = <None>)

  The CAPF Profile Instance ID is a unique string of numbers and/or letters used to identify the TLS connection or instance that is made between the Cisco WebDialer Web service and CTIManager for the WDSecureSysUser application user. If the CTI Manager Connection Security Flag parameter is set to True, then this parameter must be configured with a value.

- Primary Cisco CTIManager (Default value = 127.0.0.1)

  This parameter specifies the IP address of the Unified CM subscriber running the CTIManager service that WebDialer should use when processing requests. This is a cluster-wide parameter.

- Backup Cisco CTIManager (Default value = <blank>)

  This parameter specifies the IP address of the Unified CM subscriber running the backup instance of the CTIManager service that WebDialer should use when processing requests. This is a cluster-wide parameter.

- List of WebDialers (Default value = <blank>)

  This parameter specifies the IP address and port numbers of all WebDialers in the enterprise. Use a space to separate multiple entries. This parameter must be populated if Redirector functionality is needed.

- User Session Expiry (Default value =0)

  This parameter specifies the time in hours after which the user session or browser cookie will expire. A value of 0 indicates that the session or cookie will never expire.

For a complete list of WebDialer service parameters, refer to the Cisco WebDialer information in the *Cisco Unified Communications Manager Features and Services Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

WebDialer Functionality and Architecture

The WebDialer application contains two servlets: the WebDialer servlet and the Redirector servlet. Both servlets are enabled when the Cisco WebDialer Web service is activated on a subscriber server. While related, they each serve different functions and can be configured to run simultaneously.

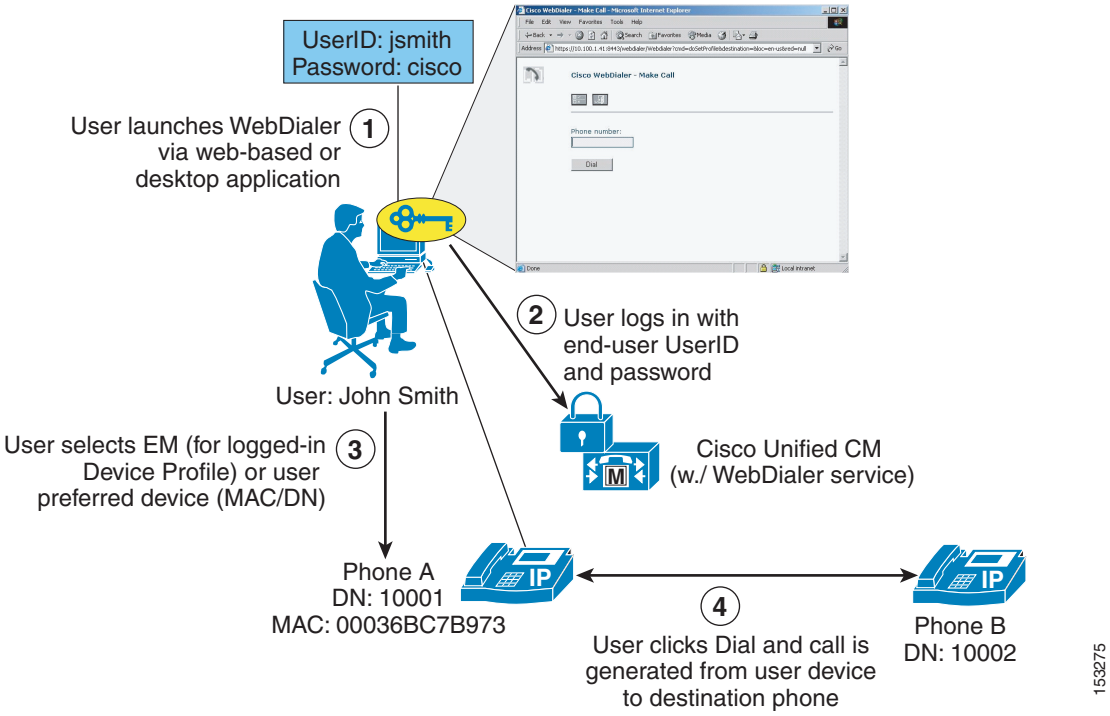
WebDialer Servlet

Figure 24-15 illustrates a simple WebDialer example. In this example, user John Smith launches WebDialer from a web-based or desktop application such as the Click to Call Cisco Unified Communications Widget (step 1). WebDialer responds with a request for login credentials. The user must respond with a valid userID and password as configured in the Unified CM end-user directory. In this case, John Smith submits userID = jsmith and password = cisco (step 2). Next, based on this login, WebDialer responds with the Cisco WebDialer Preferences configuration page, and the user must indicate either “User preferred device” or “Use Extension Mobility” (assuming the user has an EM device profile). In this case, user John Smith selects “User preferred device” and selects the appropriate MAC address (SEP00036BC7B973) and directory number (10001) for his phone from drop-down menus on the configuration page (step 3). Finally, the user is presented with a screen requesting the phone

number to be called (this value may already be indicated) and must click Dial. In this case, John Smith enters 10002 and, after clicking Dial, a call is automatically generated from his phone to Phone B at number 10002 (step 4).

Note If the user has previously logged in to the WebDialer application and a web browser and server cookie are still active, the user will not be prompted to log in again during subsequent requests. The user will be prompted to log in again when the cookie has been cleared at the browser or by a restart of the WebDialer server. Alternatively, the user web browser cookie can be set to expire automatically after a certain number of hours as configured by the User Session Expiry WebDialer service parameter (see WebDialer Service Parameters, page 24-51).

Figure 24-15 WebDialer Servlet Operation



Redirector Servlet

The Redirector servlet provides WebDialer functionality in a multi-cluster or distributed call processing environment. This functionality allows the use of a single enterprise-wide web-based WebDialer application between all Unified CM clusters. Figure 24-16 illustrates the basic operation of the Redirector servlet as part of the WebDialer application. In this example, the enterprise has three Unified CM clusters: New York, Chicago, and San Francisco. All three clusters have been configured with a single WebDialer application. The San Francisco cluster has been designated as the Redirector.

In order to designate the San Francisco WebDialer as the enterprise-wide Redirector, each cluster WebDialer server must have the service parameter List of WebDialers (see WebDialer Service Parameters, page 24-51) configured with its own IP address and the San Francisco WebDialer IP address.

Note In Cisco Unified CM 7.1(2) and later releases, the List of WebDialers can also be configured through the Application Server menu. For more information, refer to the *Cisco Unified Communications Manager Administration Guide*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

The San Francisco WebDialer server will be configured with its own IP address and the addresses of all other WebDialer servers in the enterprise. Based on this example, the List of WebDialers service parameter field for each WebDialer server would be configured as follows:

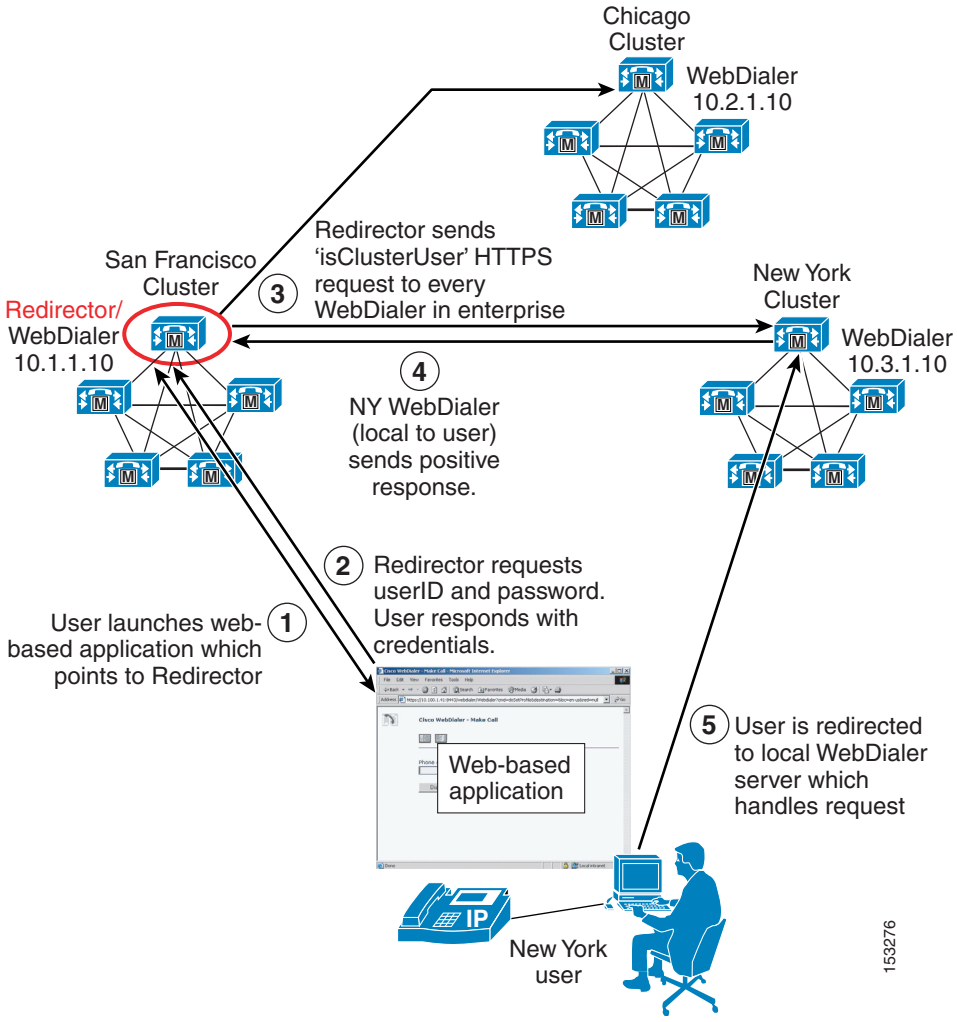
- New York WebDialer — List of WebDialers: 10.1.1.10:8443 10.3.1.0:8443
- Chicago WebDialer — List of WebDialers: 10.1.1.10:8443 10.2.1.0:8443
- San Francisco WebDialer — List of WebDialers: 10.1.1.10:8443 10.2.1.0:8443 10.3.1.0:8443

The enterprise-wide web-based application points to the San Francisco Redirector and is launched by the New York user (see step 1 in Figure 24-16). Next the Redirector requests user login, and the New York user responds back with their userID and password (see step 2 in Figure 24-16).

Note If the user has previously logged in to the WebDialer application and a web browser and server cookie are still active, the user will not be prompted to log in again during subsequent requests. Alternatively, the user web browser cookie can be set to expire automatically after a certain number of hours as configured by the User Session Expiry WebDialer service parameter (see WebDialer Service Parameters, page 24-51).

The Redirector then broadcasts an isClusterUser HTTPS request to every WebDialer in the enterprise simultaneously (as configured in the List of WebDialers service parameter). In this example, the requests go to the Chicago and New York WebDialer servers (see step 3 in Figure 24-16). Because the New York user is local to the New York cluster, the New York WebDialer responds with a positive response (see step 4 in Figure 24-16). Finally, the New York user is redirected to their local WebDialer server, which will handle the application request (see step 5 in Figure 24-16). The user is not notified of the redirect; however, the URL in the browser address bar will be changed as the user is redirected from the Redirector to the local WebDialer server).

Figure 24-16 Redirector Servlet Operation



Note Because the Redirector application is an enterprise-wide application that requires user authentication against the Unified CM Database, Cisco highly recommends that all end-user userIDs be unique across all Unified CM clusters. If they are not, then it is possible that more than one positive response to the isClusterUser request could be received by the Redirector application. If this happens, the user will be asked by the Redirector application to select their local WebDialer server manually. The user will then have to know which server is their local server. If the wrong server is chosen, the WebDialer request will fail.

WebDialer Architecture

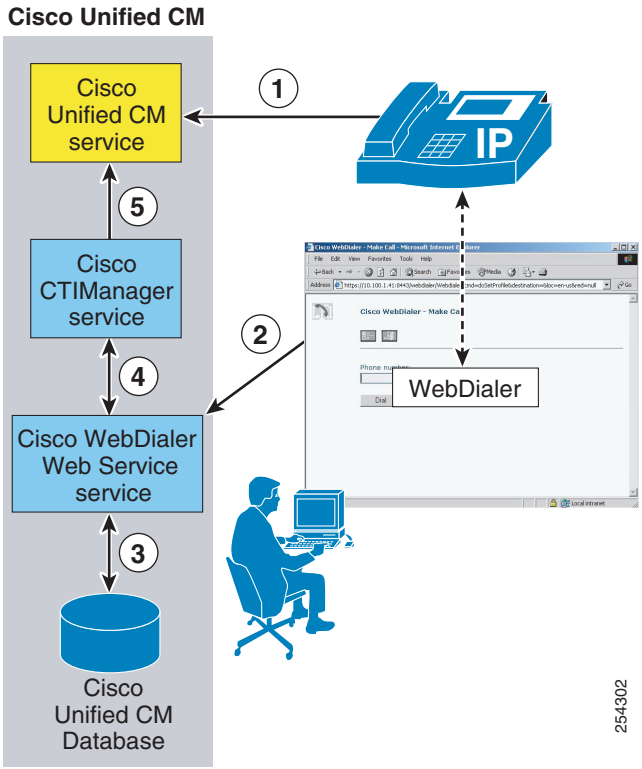
The architecture of the WebDialer application is as important to understand as its functionality. Figure 24-17 depicts the message flows and architecture of WebDialer. The following sequence of interactions and events can occur:

1. WebDialer user phones register and make and receive calls via the Cisco CallManager service (see step 1 in Figure 24-17).
2. The WebDialer application on the user's PC communicates with the Cisco WebDialer Web Service (see step 2 in Figure 24-17) via one of the following interfaces:
   - HTML over HTTPS

     This interface is used by web-based applications based on the HTTPS protocol. This is the only interface that provides access to the WebDialer and Redirector servlets.
   - Simple Object Access Protocol (SOAP) over HTTPS

     This interface is used by desktop applications based on the SOAP interface.
3. The WebDialer Web service reads user and phone information from the Unified CM Database (see step 3 in Figure 24-17).
4. The WebDialer Web service in turn interacts with the CTIManager service for exchanging line and phone control information (see step 4 in Figure 24-17).
5. The CTIManager service passes WebDialer phone control information to the Cisco CallManager service (see step 5 in Figure 24-17).

Figure 24-17 WebDialer Architecture



Note Although Figure 24-17 shows the Cisco CallManager, CTIManager, and WebDialer Web Service services all running on the same node, this configuration is not a requirement. These services can be distributed among multiple nodes in the cluster, but they are shown on the same node here for ease of explanation.

WebDialer URLs

The WebDialer application can be accessed from web-based applications via the HTML-over-HTTPS interface using the following URLs:

- WebDialer servlet

  https://<*Server-IP_Addr*>:8443/webdialer/Webdialer?destination=<*Number_to_dial*>

  (where <*Server_IP-Address*> is the IP address of any node in the cluster running the Cisco WebDialer Web Service service, and where <*Number_to_dial*> is the number that the WebDialer user wishes to dial)

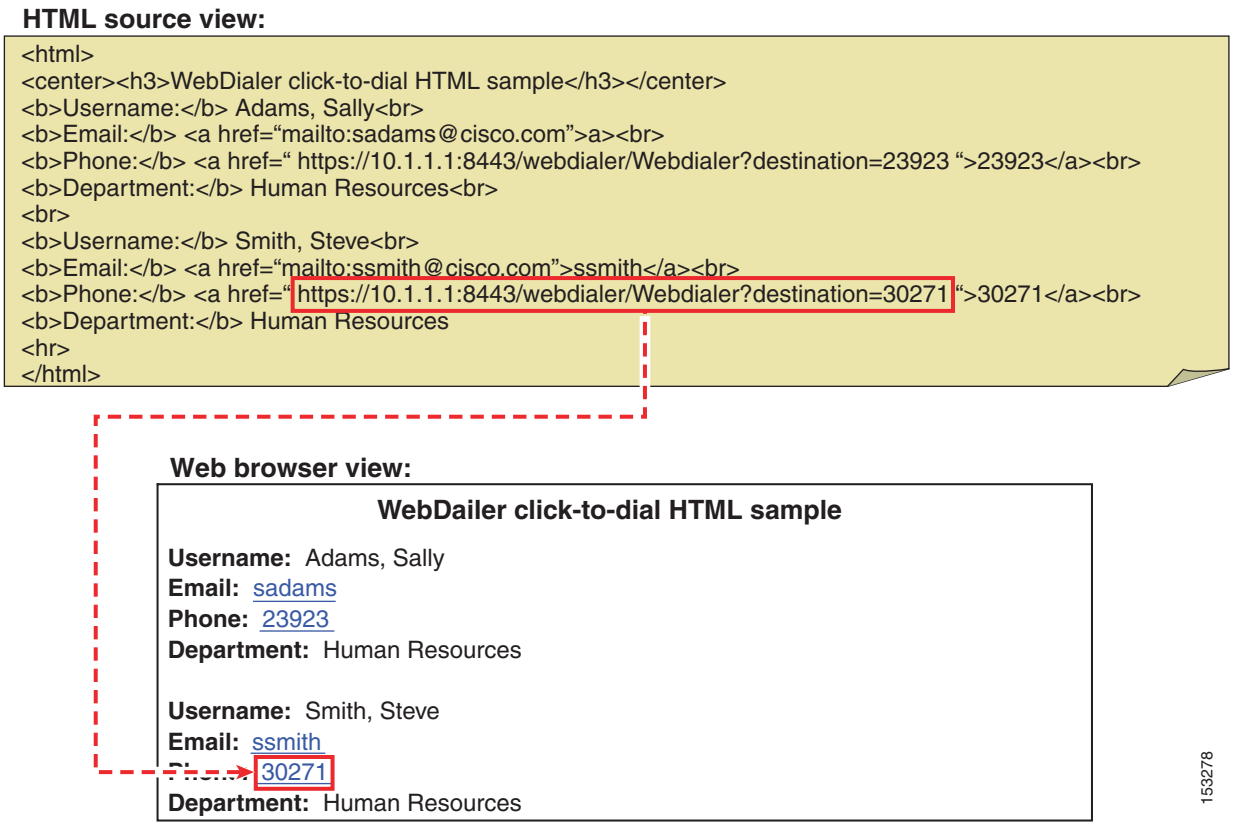
- Redirector servlet

  https://<*Server-IP_Addr*>:8443/webdialer/Redirector?destination=<*Number_to_dial*>

  (where <*Server_IP-Address*> is the IP address of any node in the enterprise running the Cisco WebDialer Web Service service, and where <*Number_to_dial*> is the number that the WebDialer user wishes to dial)

Figure 24-18 gives an example of HTML source code used in a click-to-call web-based application calling the Cisco WebDialer application. In this example, the URL https://10.1.1.1:8443/webdialer/Webdialer?destination=30271 in the HTML source view corresponds to the "Phone: 30721" link for user Steve Smith within the web browser view. A user clicking on this link would launch the WebDialer application and, after logging in and clicking Dial, would generate a call from the user's phone to Steve Smith's phone. The same code could be used for a click-to-call application using the Redirector function by changing the URL to https://10.1.1.1:8443/webdialer/Redirector?destination=30271.

Figure 24-18 WebDialer URL HTML Example



For information and examples of SOAP-over-HTTPS source code to be used in click-to-call desktop applications, refer to the WebDialer API Programming information in the *Cisco Unified Communications Manager Developers Guide*, available at

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

WebDialer Redundancy

WebDialer application redundancy can be provided at two levels:

- Redundancy at the component and service level

  At this level, redundancy must be considered with regard to WebDialer and CTIManager service redundancy. Likewise, the lack of publisher redundancy and the impact of this component failing should also be considered.

- Redundancy at the device and reachability level

  At this level, redundancy should be considered as it relates to user phones and the WebDialer user interface.

Service and Component Redundancy

As shown in Figure 24-17, WebDialer functionality is primarily dependent on the Cisco WebDialer Web Service and the Cisco CTIManager services. In the case of the WebDialer service, redundancy is provided by listing multiple WebDialer server IP addresses in the List of WebDialers service parameter (see WebDialer Service Parameters, page 24-51) and enabling the service on multiple nodes within the cluster. In the case of CTIManager, redundancy is automatically built-in using a primary and backup mechanism. Two CTIManager servers or services can be defined within the cluster using the Primary Cisco CTIManager and the Backup Cisco CTIManager service parameters (see WebDialer Service Parameters, page 24-51). By configuring these parameters, you can make the CTIManager service redundant. Thus, if the primary CTIManager fails, CTIManager services can still be provided by the backup CTIManager. If the WebDialer server to which the web-based (or desktop) application is pointing fails and the primary and backup CTIManager services on cluster nodes also fail, the WebDialer application will fail. The WebDialer service is not dependant upon the Unified CM publisher

Device and Reachability Redundancy

Redundancy for WebDialer at the device level relies on a number of mechanisms. First and foremost, user phones rely on the built-in redundancy provided by a combination of the device pool and Unified CM group configuration for device registration.

The WebDialer service can run on multiple Unified CM subscribers to provide redundancy, however many applications might not be equipped to handle more than one IP address. Cisco recommends using a Server Load Balancer (SLB) to mask the presence of multiple WebDialer servers in the enterprise. SLB functionality provides a virtual IP address or DNS-resolvable hostname that front-ends the real IP addresses of the WebDialer and/or Redirector servers. Most SLB devices, such as the Cisco Application Control Engine (ACE) or the Cisco IOS SLB feature, can be configured to monitor the status of multiple WebDialer servers and automatically redirect requests during failure events. The SLB feature can also be configured to load-balance WebDialer requests when additional click-to-call capacity is required. As an alternative, DNS Service (SRV) records can also be used to provide redundancy.

In enterprise deployments, link cost might also be an important consideration. The Cisco ACE Global Site Selector (GSS) appliance builds upon the capabilities of the SLB feature by adding link cost and location to the load-balancing algorithm, among other features. For more information on ACE and GSS, refer to the product documentation available at http://www.cisco.com.

Guidelines and Restrictions for WebDialer

The following guidelines and restrictions apply with regard to deployment and operation of WebDialer within the Unified CM telephony environment:

- The administrator should ensure that all WebDialer users are associated with a phone or device profile in the Unified CM end-user directory.
  - If the user selects "Use permanent device" under the Cisco WebDialer Preferences screen with no phone association, then the following message is received when the Dial button is pressed:

    “No supported device configured for user”
  - If the user selects Use Extension Mobility under the Cisco WebDialer Preferences screen with no device profile association (or the user is not logged in using a profile), then the following message is received when the Dial button is pressed:

    “Call to <*dialed_ number*> failed: User not logged in on any device”

Note WebDialer and EM applications may be used together. For information about WebDialer interaction with EM, see WebDialer Interactions with EM, page 24-61.

- When configuring the List of WebDialers service parameter (see WebDialer Service Parameters, page 24-51), port number 8443 must be specified along with WebDialer IP address.
- If using Client Matter Codes (CMC) or Forced Authorization Codes (FAC), WebDialer users must enter the proper code at the tone by using the phone's keypad. Failure to enter the appropriate code at the tone will result in call failure signaled by a reorder tone.

WebDialer Performance and Scalability

The WebDialer and Redirector services can run on one or more subscriber nodes within a Unified CM cluster, and they support the following capacities:

- Each WebDialer service can handle up to 2 call requests per second (7,200 calls per hour) per node.
- Each Redirector service can handle up to 8 call requests per second.

The following general formula can be used to determine the number of WebDialer calls per second (cps):

(Number of WebDialer users) * ((Average BHCA) / (3600 seconds/hour))

When performing this calculation, it is important to estimate properly the number of BHCA per user that will be initiated specifically from using the WebDialer service. The following example illustrates the use of these WebDialer design calculations for a sample organization.

Example 24-1 Calculating WebDialer Calls per Second

Company XYZ wishes to enable click-to-call applications using the WebDialer service, and their preliminary traffic analysis resulted in the following information:

- 10,000 users will be enabled for click-to-call functionality.
- Each user averages 6 BHCA.
- 50% of all calls are dialed outbound, and 50% are received inbound.
- Projections estimate 30% of all outbound calls will be initiated using the WebDialer service.

Note These values are just examples used to illustrate a WebDialer deployment sizing exercise. User dialing characteristics vary widely from organization to organization.

10,000 users each with 6 BHCA equates to a total of 60,000 BHCA. However, WebDialer deployment sizing calculations must account for placed calls only. Given the initial information for this sizing example, we know that 50% of the total BHCA are placed or outbound calls. This results in a total of 30,000 placed BHCA for all the users enabled for click-to-call using WebDialer.

Of these placed calls, the percentage that will be initiated using the WebDialer service will vary from organization to organization. For the organization in this example, several click-to-call applications are made available to the users, and it is projected that 30% of all placed calls will be initiated using WebDialer.

(30,000 placed BHCA) * 0.30 = 9,000 placed BHCA using WebDialer

To determine the number of WebDialer servers required to support a load of 9,000 BHCA, we convert this value to the average call attempts per second required to sustain this busy hour:

(9,000 call attempts / hour) * (hour/3600 seconds) = 2.5 cps

Each WebDialer service can support up to 2 cps, therefore 2 nodes should be configured to run the WebDialer service in this example. This would allow for future growth of WebDialer usage. In order to maintain WebDialer capacity during a server failure, additional backup WebDialer servers should be deployed to provide redundancy.

Keep in mind that the Cisco WebDialer application interacts with the CTIManager for phone control. When enabled, each WebDialer service opens a single persistent CTI connection to the CTIManager. In addition, each WebDialer individual MakeCall (or EndCall) request generates a temporary CTI connection. The number of CTI connections required to handle WebDialer call rates also applies against the CTI connection limits per cluster. (For more information on CTI connection limits per cluster, see Unified CM Capacity Planning, page 8-22.)

WebDialer Interactions with EM

WebDialer users can log in to their phones using EM. EM users wishing to use WebDialer simply need to select the Use Extension Mobility setting under the Cisco WebDialer Preferences page.