CHAPTER 24

Cisco Collaboration Clients and Applications

Revised: January 12, 2012; OL-21733-18

Note This chapter has been revised significantly for the current release of this document. Cisco recommends that you read this entire chapter before attempting to deploy collaboration clients and applications in your Cisco Unified Communications System.

Cisco Collaboration Clients and Applications provide an integrated user experience and extend the capabilities and operations of the Cisco Unified Communications System. These clients and applications enable collaboration both inside and outside the company boundaries by bringing together, in a single easy to use collaboration client, applications such as online meetings, presence notification, instant messaging, audio, video, voicemail, and many more.

Several collaboration clients and applications are available, and each provides an architectural view, deployment considerations, planning, and design guidance around integration into the Cisco Unified Communications System. Use this chapter to determine which of the following collaboration clients and applications are best suited for your deployment:

- Cisco Unified Personal Communicator

  Cisco Unified Personal Communicator is a desktop application that allows users to easily access voice, video, web conferencing, instant messaging, voicemail, and presence information from a rich media interface on their desktop (PC or Mac). Cisco Unified Personal Communicator enhances productivity between teams and allows knowledge workers to collaborate anytime, anywhere, and easily escalate their communications through an easy-to-use user interface. For additional information, see the chapter on Cisco Unified Presence, page 23-1.

- Cisco WebEx Connect

  Cisco WebEx Connect is a Unified Communications client application that is delivered through Software-as-a-Service (SaaS). WebEx Connect provides presence, instant messaging, voice and video, voice messaging, desktop sharing, and conferencing capabilities through a single client on your Windows desktop. WebEx Connect enhances productivity by empowering users to collaborate more securely and effectively from anywhere with colleagues, business partners, and customers.

- Cisco UC Integration™ for Microsoft Lync

  Cisco UC Integration™ for Microsoft Lync allows for integrated Cisco Unified Communications services with Microsoft Lync using the Cisco Unified Client Services Framework, while delivering a consistent user experience. The solution extends the presence and instant messaging capabilities

of Microsoft Lync by providing access to a broad set of Cisco Unified Communications services, including standards-based audio and video, unified messaging, web conferencing, deskphone control, and telephony presence.

- Cisco Virtual Experience Clients

  The Cisco Virtualization Experience Clients (VXC) are the integral collaboration components of the Cisco Virtualization Experience Infrastructure (VXI). The VXCs provide user access to data, applications, and services across various network environments, as well as user preferences and device form factors for a fully integrated voice, video, and virtual desktop environment.

- Cisco Unified Mobile Communicator

  Cisco Unified Mobile Communicator is a mobility solution that gives users the ability to access and leverage Cisco Unified Communications applications from their mobile phones. The Cisco Unified Mobile Communicator and Cisco Mobile graphical clients work in conjunction with a server running the Cisco Unified Mobility Advantage software to provide a rich user interface for accessing and controlling mobile phone features and functionality. The system integrates into existing corporate LDAP directories, allowing users to use a single set of credentials across all devices. For more information, refer to the chapter on Mobile Unified Communications, page 25-1.

- Third-party XMPP clients and applications

  Cisco Unified Presence, with support for SIP/SIMPLE and Extensible Messaging and Presence Protocol (XMPP), provides support of third-party clients and applications to communicate presence and instant messaging updates between multiple clients. Third-party XMPP clients, MomentIM, Adium, Spark, Pidgin, and others, allow for enhanced interoperability across various desktop operating systems. In addition, web-based applications can obtain presence updates, instant messaging, and roster updates using the HTTP interface with SOAP, REST, or BOSH (based on JabberWerx AJAX API). For additional information on the third-party open interfaces, see the chapter on Cisco Unified Presence, page 23-1.

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:	Revision Date
Minor corrections to a few illustrations	Figure 24-3; Figure 24-4	January 12, 2012
Cisco Virtualization Experience Infrastructure (VXI) and Virtualization Experience Client (VXC)	Cisco Virtualization Experience Client Architecture, page 24-33	December 22, 2011
Cisco WebEx Connect	Cisco WebEx Connect Architecture, page 24-16	August 31, 2011
High availability for Cisco Unified Personal Communicator	High Availability for Cisco Unified Personal Communicator, page 24-13	January 31, 2011
Microsoft Office Communicator name changed to Microsoft Lync	Various sections throughout this chapter	January 31, 2011

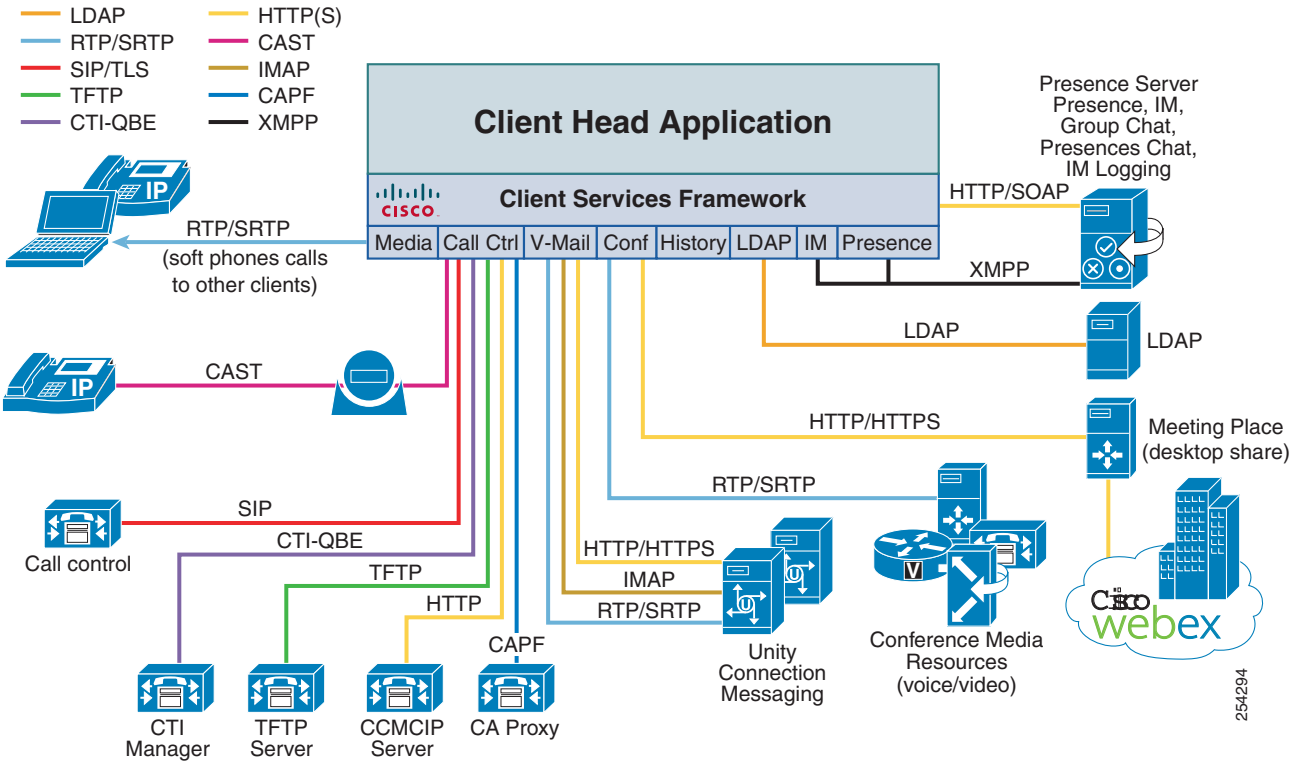
Cisco Unified Client Services Framework Architecture

Cisco Unified Personal Communicator, Cisco WebEx Connect, and Cisco UC Integration™ for Microsoft Lync all use the Client Services Framework as a base building block for the client application. Cisco Unified Client Services Framework is a software application that combines a number of services into an integrated client. An underlying framework is provided for integration of Unified Communications services, including audio, video, web collaboration, visual voicemail, and so forth, into a presence and instant messaging application.

Users are allowed to access a variety of communications services that interface into Cisco Unified Communications Manager (Unified CM), Cisco Unity, Cisco Unity Connection, Cisco Unified MeetingPlace, and a Lightweight Directory Access Protocol (LDAP) version 3 (v3) server. The Client Services Framework, shown in Figure 24-1, also allows for integration into various desktop clients such as Microsoft Lync, Cisco WebEx Connect, and Cisco Unified Personal Communicator.

The ability to communicate and abstract services and APIs, as shown in Figure 24-1, allows the Client Services Framework to coordinate the management of protocols to these services and APIs, handle event notifications, and control the low-level connection logic for local system resources.

Figure 24-1 Cisco Unified Client Services Framework



Contact Management

The Client Services Framework handles the management of contacts through a hierarchy of sources. These include directory integration, supporting LDAP and LDAPS, where a customizable attribute table mapping must be configured, Client Services Framework Cache, and Local Address Book contacts. The Client Services Framework contact management allows for up to five search bases to be defined for LDAP queries, and it handles reverse number lookup to map incoming telephone number to contact, in addition to photo retrieval.

Directory

LDAP Directory integration with the Client Services Framework allows attributes to be mapped and configured for contacts to be managed from a central directory location. The most common directory attribute mapping is listed in Table 24-2.

Table 24-2 Directory Attribute Mapping

Client Services Framework Name	LDAP Directory Attribute
businessPhone	telephoneNumber
commonName	cn
companyName	company
displayName	displayName
email	mail
firstName	givenName
homePhone	homePhone
lastName	sn
mobilePhone	mobile
objectclassKey	objectclass
objectclassValue	person
otherPhone	otherTelephone
photoUri	photoUri
title	title
uri	msRTCSIP-PrimaryUserAddress
userAccountName	sAMAccountName / uid
userLogonName	userPrincipalName / uid

Client Services Framework Cache

The Client Services Framework maintains a local cache of contact information derived from previous directory queries and contacts already listed, as well as the local address book.

Directory Search

When a contact cannot be found in the local Client Services Framework cache, a directory search for the contact information can be made through LDAP or LDAPS. The Client Services Framework utilizes a predictive search whereby the local cache is queried as contact information is being entered. If no matches are found locally, then the user can use the directory search option, which forms a searchRequest, for matches with cn, sn, uid, and givenName, and can send the request to the LDAP server based on the LDAP profile configured. All results matching the request are returned and listed.

Call Control

Cisco Unified Client Services Framework can operate in two modes, softphone mode (audio on a computer) or deskphone control mode (using a deskphone for audio). The Client Services Framework in softphone mode (audio on a computer) is directly registered as a SIP endpoint to Unified CM for audio and video call control functionality, and is configured on Unified CM as a new device type, Client Services Framework. The Client Services Framework in deskphone control mode (using a deskphone for audio) uses CTI / JTAPI to initiate, monitor, and terminate calls, monitor line state, and provide call history, while controlling a Cisco Unified IP Phone. The CCMCIP service on Unified CM is used by the Client Services Framework to discover the users associated devices.

Softphone Mode (Audio on Computer)

When operating in softphone mode (audio on computer), the Client Services Framework is a SIP line-side registered device on Unified CM, utilizing all the call control capabilities and functionality of a Cisco Unified IP Phone, including configuration of registration, redundancy, regions, locations, dial plan management, authentication, encryption, user association, and so forth. The Client Services Framework supports a single line appearance for the user.

The SIP registered device of the Client Services Framework must be factored in as a regular SIP endpoint, as any other SIP registered endpoint, for purposes of sizing calculations for a Unified CM cluster.

Deskphone Control Mode (Using Deskphone for Audio)

When operating in deskphone control mode (using deskphone for audio), the Client Services Framework uses CTI / JTAPI to provide the ability to place, monitor, and receive calls using Cisco Unified IP Phones. When calls are received or placed in this mode, the audio path is through the Cisco Unified IP Phone. The Client Services Framework uses the CCMCIP service on Unified CM to discover the associated devices of the user. When using video, the Client Services Framework and the Unified IP Phone being controlled use Cisco Discovery Protocol (CDP) to discover one another, and they use Cisco Audio Session Tunnel (CAST) to set up and manage the video call. The PC being used for the Client Services Framework must be a 32-bit operating system and be physically plugged into the PC port of the Unified IP Phone, and that PC port of the Unified IP Phone must be enabled.

When using deskphone control mode for the Client Services Framework, factor the CTI scaling numbers into the Unified CM deployment calculations. For additional information around capacity planning, see the chapter on Call Processing, page 8-1.

Media

A number of standard audio and video codecs for use in low bandwidth or high fidelity deployments are supported with the Client Services Framework. Audio codecs include G.729a, iLBC, G.711, G.722, and iSAC, while video codecs include H.264 AVC (Advanced Video Coding) with support for H.264 baseline profile levels 1 through 3.1. Video formats supported include QCIF, CIF, VGA, and 720p HD at a rate of up to 30 frames per second.

The Client Services Framework always attempts to transmit and receive high definition video; however, there are a number of throttling factors that need to be considered when deploying video. These throttling considerations include the capability of the device communicating with, the local processing capability of the PC, administrative or user settings, local camera capabilities, and any call admission control policies in place.

There are a number of decision points the Client Services Framework uses to determine the video frame rate for a call. One of the key decision points is based on the Windows Experience Index (WEI) for the personal computer being used (http://technet.microsoft.com/en-us/library/cc507870.aspx). The minimum values for encoding and decoding high definition video require a processor WEI encode value of 5.9 and a bandwidth requirement of 1 Mbps for 720p at 15 frames per second or 2 Mbps for 720p at 30 frames per second. For a listing of other video frame rates based on H.264 Level and WEI encode and decode values, refer to the following application release notes:

- Cisco Unified Personal Communicator release notes

  http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html

- Cisco UC Integration™ for Microsoft Lync release notes

  http://www.cisco.com/en/US/products/ps10317/prod_release_notes_list.html

The receive levels for video can be controlled within the Client Services Framework by manually adjusting the video settings, either by administrative or user control. The ability to manually adjust the mode of operation and the corresponding H.264 level allows for throttling of the video stream rates and Windows Experience Index. These throttling considerations include the capability of the device communicating with the Client Services Framework, the local processing capability of the PC, administrative or user settings, local camera capabilities, and any call admission control policies in place. Refer to the application release notes for the relationship of the Windows Experience Index to video resolution.

Bandwidth utilization for audio and video calls from the Client Services Framework can be maintained using the Unified CM regions and locations call admission control mechanisms. Administratively placing the Client Services Framework in a device pool for a region provides the ability to control bandwidth usage in scenarios where network bandwidth is at a premium. Unified CM regions call admission control provides the ability to specify which codecs can be used, as well as the per-call inter-region and intra-region bandwidth allowed. Unified CM locations call admission control provides location-to-location audio and video bandwidth control, or the use of RSVP. The Client Services Framework requires the Unified CM region to be sufficient to cover both the audio and video portions of the call. For example, to have a video call at a frame size of 720p and a frame rate of 30 frames per second, the signaling bit rate needs to be 2,000 kbps just for video; therefore, the region bandwidth for a call must account for the audio portion at 64 kbps (assuming a G.711 or G.722 codec) as well as the video portion at 2,000 kbps (assuming 720p at 30 fps). For more information on Unified CM support for regions and locations call admission control, see the chapter on Call Processing, page 8-1.

The signaling and media traffic, both audio and video, for the Client Service Framework is marked by means of Differentiated Services Code Point (DSCP) to allow for greater flexibility and control of a deployment. The Client Services Framework marks all signaling with a CS3 classification. The media associated with audio-only calls is marked EF, and video calls are marked with a DSCP value of AF41

for both audio and video. However, the operating system might not honor these markings, thus resulting in the traffic from the PC being untrusted. For additional details, see the QoS recommendations for Software-Based Endpoints, page 18-44.

Dial Plan

Dial plan and number normalization considerations must be taken into account when deploying the Client Services Framework as part of any Unified Communications endpoint strategy. The Client Services Framework, as part of a Unified Communications collaboration client, will typically use the directory for searching, resolving, and adding contacts. The number that is associated with those contacts must be in a form that the client can recognize, resolve, and dial.

Deployments may vary, depending on the configuration of the directory and Unified CM. In the case where the directory contains E.164 numbering (for example, +18005551212) for business, mobile, and home telephone numbers and Unified CM also contains an E.164 dial plan (Unified CM 7.*x* or later releases), the need for additional dial rules is minimized because every lookup, resolution, and dialed event results in an E.164 formatted dial string.

When a deployment of Unified CM has implemented a private dial plan (for example, 51212), then translation of the E.164 number to a private directory number needs to occur on Unified CM. Outbound calls are translated by means of application dial rules. This allows the number being dialed, +18005551212, to be presented to the endpoint as the private number of 51212. Inbound calls are translated by means of directory lookup rules. This allows an incoming number of 51212 to be presented for reverse number lookup caller identification as +18005551212.

Private numbering plan deployments may arise, where the dial plan for your company and the telephone number information stored in the LDAP directory may require defining application dialing rules and directory lookup rules on Cisco Unified Communications Manager. These rules define how to reformat the inbound call ID to be used as a directory lookup key and how to transform a phone number retrieved from the LDAP directory for outbound dialing.

Application Dialing Rules

Application dialing rules are used to manipulate numbers that are dialed and to automatically strip numbers from, or add numbers to, phone numbers that the user dials. Cisco Unified CM 7.*x* and later releases supports rules that contain the plus (+) character in dialed numbers, whereas Unified CM releases prior to 7.*x* do not support the plus character. Application dial rules are configured on Unified CM and are downloaded through TFTP to the client from Unified CM.

Directory Lookup Rules

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory, and a rule specifies which numbers to transform based on the initial digits and the length of the number. Directory Lookup rules are configured on Unified CM and are downloaded through TFTP to the client from Unified CM.

Translation Patterns

Translation patterns are used by Unified CM to manipulate the dialed digits before a call is routed, and they are strictly handled by Unified CM. When using Unified CM 7.*x* and later releases, Cisco recommends using translation patterns instead of application dialing rules for increased flexibility with number resolution in a Client Services Framework deployment.

For additional guidelines on translation pattern usage and dial plan management, see the chapter on Dial Plan, page 9-1.

Client Transformation

Before a call is placed through contact information, the client application removes everything from the phone number to be dialed, except for letters and digits. The application transforms the letters to digits and applies the dialing rules. The letter-to-digit mapping is locale-specific and corresponds to the letters found on a standard telephone keypad for that locale. For example, for a US English locale, 1-800-4UCSRND transforms to 18004827763. Users cannot view or modify the client transformed numbers before the application places the call.

Deploying Client Services Framework

Because the Client Services Framework is a fundamental building block for desktop client integration and communication, it is necessary to deploy these devices to a number of users. Cisco recommends using the Bulk Administration Tool for the Client Services Framework deployment. The administrator can create a phone template for device pool, device security profile, and phone buttons, and can create a CSV data file for the mapping of device name to directory number. The administrator can also create a User template to include user groups and CTI, if enabled, as well as a CSV data file to map users to the appropriate controlled device.

Capacity Planning for Client Services Framework

Cisco Unified Client Services Framework operates as a SIP registered endpoint to Unified CM or as a deskphone controller of a Unified IP Phone using CTI to Unified CM. When planning a deployment using Client Services Framework, Cisco partners and employees can use the Cisco Unified Communications Sizing Tool (available at http://tools.cisco.com/cucst) to assist in the appropriate sizing of SIP registered endpoints or CTI controlled devices. The following additional items must be considered for a Client Services Framework deployment:

- TFTP — When configured in softphone (audio on computer) mode, a Client Services Framework device configuration file is downloaded to the client for Unified CM call control configuration information. In addition, any application dial rules or directory lookup rules are also downloaded through TFTP.
- CTI — When configured in deskphone (using desk phone for audio) mode, the Client Services Framework establishes a CTI connection to Unified CM upon login and registration to allow for control of the IP phone.
- CCMCIP — The Client Services Framework uses the Unified CM IP Phone Services to gather information about the devices associated with the user to be able to list the IP phones available for control.
- IMAP — When configured for voicemail, the Client Services Framework updates and retrieves voicemail through an IMAP connection to the mailstore.
- LDAP — Client login and authentication, contact profile information, and incoming caller identification are all handled through an LDAP query, unless stored in the local Client Services Framework cache.

With the exception of the integrated Extension Mobility and Unified CM Assistant applications' IP 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.

High Availability for Client Services Framework

Cisco Unified Client Services Framework provides primary and secondary servers for each of the configuration components, TFTP Server, CTI Manager, CCMCIP Server, Voicemail Server, and LDAP Server. When operating in softphone (audio on computer) mode, the Client Services Framework is a SIP registered endpoint with Cisco Unified CM and supports all of the registration and redundancy capabilities of a registered endpoint of Unified CM. When operating in deskphone mode, the Client Services Framework is controlling a Cisco Unified IP Phone using CTI and supports configuration of a primary and secondary CTI Manager. For additional details on CTI deployment, see the chapter on Call Processing, page 8-1

Design Considerations for Client Services Framework

Observe the following design considerations when deploying the Cisco Unified Client Services Framework:

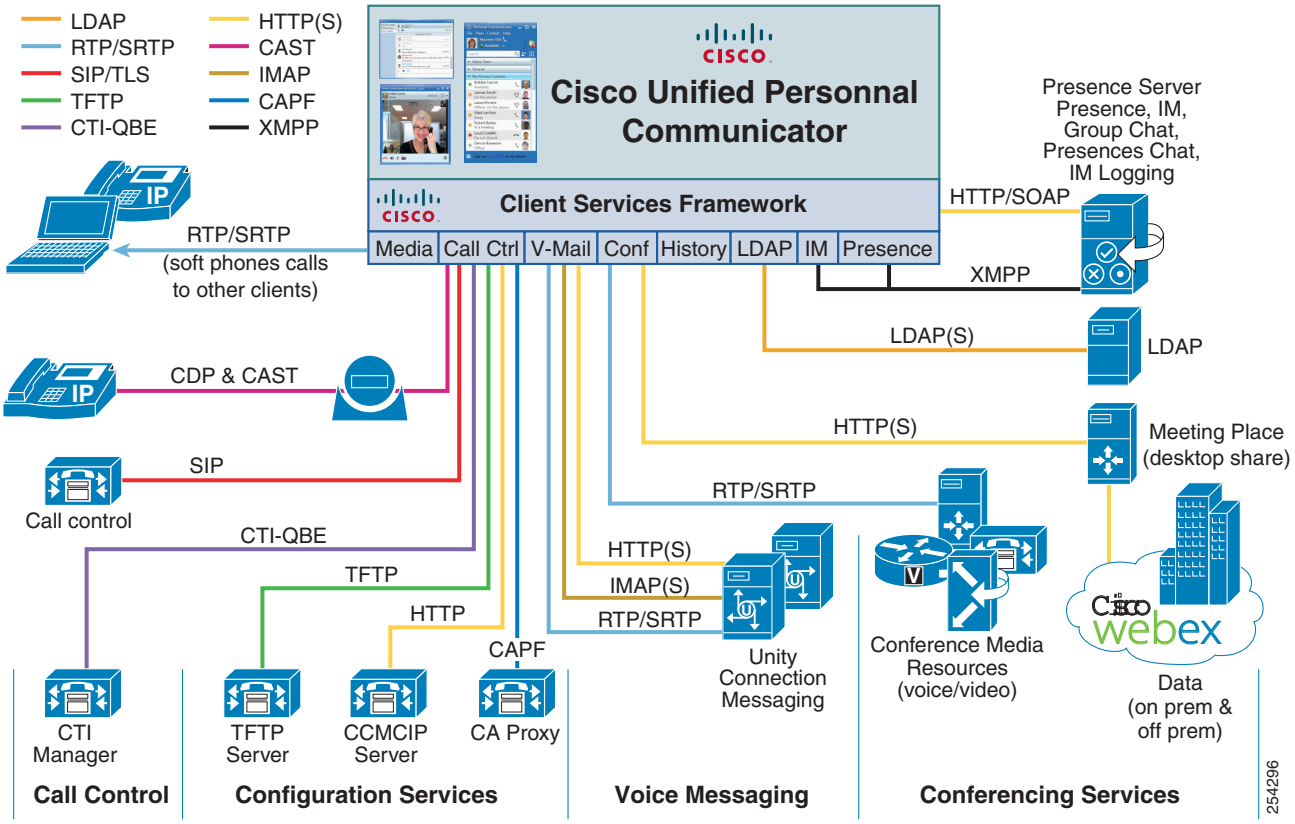
- The administrator must determine how to install, deploy, and configure the Unified Client Services Framework in their organization. Cisco recommends using a well known installation package such as Altiris to install the application, and use Group Policies to configure the user registry settings for the required components of TFTP Server, CTI Manager, CCMCIP Server, Voicemail Pilot, LDAP Server, LDAP Domain Name, and LDAP search contexts.
- The userid and password configuration of the Cisco Unified Client Services Framework user must match the userid and password of the user stored in the LDAP server to allow for proper integration of the Unified Communications and back-end directory components.
- The directory number configuration on Cisco Unified CM and the telephoneNumber attribute in LDAP should be configured with a full E.164 number. A private enterprise dial plan can be used, but it might involve the need to use application dialing rules, directory lookup rules, or translation patterns.
- The use of deskphone mode for control of a Cisco Unified IP Phone uses CTI; therefore, when sizing a Unified CM deployment, you must also account for other applications that require CTI usage.
- For firewall and security considerations, the port usage required for the Client Services Framework and corresponding applications being integrated can be found in the product release notes for each application.
- To reduce the impact on the amount of traffic (queries and lookups) to the back-end LDAP servers, configure concise LDAP search bases for the Client Services Framework rather than a top-level search base for the entire deployment.

Cisco Unified Personal Communicator Architecture

Cisco Unified Personal Communicator allows for a fully integrated Cisco Unified Communications solution, delivering a consistent user experience in a single desktop client using the Cisco Unified Client Services Framework. The solution incorporates the always-on presence and instant messaging capabilities of Cisco Unified Presence, while providing access to a broad set of Cisco Unified Communications services, including standards-based audio and video, unified messaging, web conferencing, deskphone control, and telephony presence.

The solution architecture for a Cisco Unified Personal Communicator deployment, shown in Figure 24-2, includes Cisco Unified Communications Manager for user association, audio, and video services, Cisco Unified Presence for presence and instant messaging services, LDAP for user account information, and Cisco Unified Client Services Framework for PC audio or deskphone control.

Figure 24-2 Cisco Unified Personal Communicator



With a Cisco Unified Personal Communicator deployment, Cisco recommends that the administrator populate the user directory number information with an E.164 value (for example, +18005551212) and enable LDAP synchronization and authentication on Unified CM for user account consistency. Cisco Unified Personal Communicator is tightly integrated with all the Cisco Unified Communications components using Cisco Unified CM for audio and video control and Cisco Unified Presence for presence and instant messaging. For those who are not deploying the full Unified Communications solution, Cisco Unified Personal Communicator can also operate in an IM-only configuration to provide presence and instant messaging services from Cisco Unified Presence. For deployment guidelines for an IM-only solution, see the chapter on Cisco Unified Presence, page 23-1.

Deploying Cisco Unified Personal Communicator

When deploying Cisco Unified Personal Communicator, observe the following guidelines:

Configuration Settings

Cisco Unified Personal Communicator downloads its configuration information from Cisco Unified Presence over the SOAP interface. All the configuration information is created, stored, and assigned to the users in profiles on Cisco Unified Presence (Voicemail, Conferencing, CTI Gateway, LDAP, and CCMCIP profiles). Cisco recommends ensuring that the user is already created, licensed, and assigned prior to associating profile configuration settings to the user. For profile configuration details, refer to the Cisco Unified Personal Communicator documentation available at

http://www.cisco.com/en/US/products/ps6844/tsd_products_support_series_home.html

Software Installation

The software installation deployment can be handled a number of different ways and is designed to be deployed using desktop management tools such as Microsoft Active Directory Group Policy, Systems Management Server (SMS), Altiris, or self-extracting executable with script/batch file. Because customer topologies vary, there is no recommendation about which method to use. For details on the software deployment method, refer to the Cisco Unified Personal Communicator documentation available at

http://www.cisco.com/en/US/products/ps6844/tsd_products_support_series_home.html

Capacity Planning for Cisco Unified Personal Communicator

When designing and sizing a solution for Cisco Unified Personal Communicator, you must consider the following scalability impacts for all the components:

- Client scalability

  The Cisco Unified Presence server hardware deployment determines the number of users a cluster can support. The Cisco Unified Personal Communicator deployment must balance all users equally across all servers in the cluster. This can be done automatically by setting the User Assignment Mode Sync Agent service parameter to **balanced**.

  The maximum number of contacts in the contact list is 200.

- IMAP scalability

  The number of IMAP or IMAP-Idle connections is determined by the platform overlay (Cisco Unity or Cisco Unity Connection) for messaging integration. For specific configuration sizing, refer to the Cisco Unity or Cisco Unity Connection product documentation available at http://www.cisco.com.

- Web conferencing

  Cisco Unified MeetingPlace web licensing determines the number of concurrent web conferencing participants allowed. For specific configuration sizing, refer to the Cisco Unified MeetingPlace product documentation available at http://www.cisco.com.

- Video sizing capability

  Videoconferencing and switching are determined by Cisco Unified Videoconferencing MCU sizing and configuration, by Cisco MeetingPlace Hardware Media Server (HMS) sizing and configuration, or by Cisco Unified MeetingPlace Express VT for concurrent voice, video, and web participants. For specific configuration sizing, refer to the Cisco Unified Videoconferencing or Cisco Unified MeetingPlace Express VT product documentation available at http://www.cisco.com.

Cisco Unified Personal Communicator interfaces with Unified CM. Therefore, the following guidelines for the current functionality of Unified CM apply when Cisco Unified Personal Communicator voice or video calls are initiated:

- CTI scalability

  In Desk Phone mode, calls from Cisco Unified Personal Communicator use the CTI interface on Unified CM. Therefore, observe the CTI limits as defined in the chapter on Call Processing, page 8-1. You must include these CTI devices when sizing Unified CM clusters.

- Call admission control

  Cisco Unified Personal Communicator applies call admission control for voice and video calls by means of Unified CM locations or RSVP.

- Codec selection

  Cisco Unified Personal Communicator voice and video calls utilize codec selection through the Unified CM regions configurations.

All Cisco Unified Personal Communicator configuration and contacts are stored in the Cisco Unified Presence database and have the potential to contain large amounts of data. The current conversation history list is limited to 50 entries for each tab (Chats, Voice Messages, Calls), while the contact list size is limited to 200 contacts. Therefore, bandwidth utilization must be taken into consideration for presence data exchange as well as for conferencing, video, and messaging traffic.

The following bandwidth considerations also apply to Cisco Unified Personal Communicator:

- A Presence User Profile (PUP) takes into consideration the number of logins, presence state changes, and roster changes to determine a user deployment traffic pattern. With a typical PUP, where the number of logins is 0.5 per hour, the number of presence state changes is 0.5 per hour, and the number of roster changes is 0.25 per hour, you can use the following formula as a general guideline for calculating bandwidth utilization (in kilobits per second) between Cisco Unified Presence and Unified Personal Communicator (see Table 24-3 for examples):

  USERS * [30 + ROSTER*7 + IM*3 + CALLS * (33 + 3*ROSTER)] / 1000

  where:

  - USERS = number of users using Unified Personal Communicator.
  - ROSTER = average roster size of a Unified Personal Communicator user.
  - IM = number of instant messages per hour for a Unified Personal Communicator user.
  - CALLS = number of softphone calls per hour.

Table 24-3 Examples of Bandwidth Requirement for Unified Personal Communicator

Enterprise	Number of Users	Roster Size	Number of IMs	Calls per Hour	Bandwidth Utilization
Small	1,000	100	25	4	2,100 kbps (2.1 Mbps)
Large	5,000	200	25	4	20,185 kbps (20.2 Mbps)

- For Cisco Unified MeetingPlace voice, video, and web collaboration sessions, see Cisco Unified MeetingPlace, page 22-13.
- For video calls, see the chapter on IP Video Telephony, page 12-1.
- For Cisco Unity or Unity Connection, see the section on Managing Bandwidth, page 21-34, in the chapter on Cisco Voice Messaging, page 21-1.

High Availability for Cisco Unified Personal Communicator

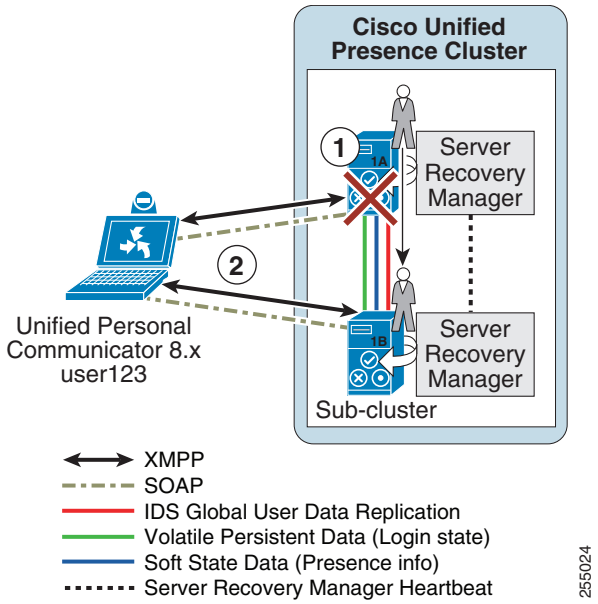
All users in the Cisco Unified Presence cluster must be assigned to a server prior to any exchange of information. Cisco Unified Presence, by default, allows for automatic user assignment that is equally balanced across all servers in the cluster. The administrator can control where users are assigned by setting the User Assignment Mode Sync Agent service parameter to **None** instead of the default **balanced**. If this parameter is set to **None**, user assignment is done from the **System** > **Topology** menu.

Cisco Unified Personal Communicator provides for basic deployment, a highly available deployment for automatic redundancy, and an IM-only deployment. In a Cisco Unified Presence two-server subcluster, users associated with one server are known by the other server in the subcluster, thus allowing for automatic failover when service communication with the configured server is interrupted. Cisco Unified Personal Communicator high availability is supported only within a Cisco Unified Presence subcluster.

As illustrated in Figure 24-3, the server recovery manager monitors the various services on Cisco Unified Presence to determine if a service has failed to initiate an XMPP failover event. The following sequence of events occurs during an XMPP failover:

1. When the server recovery manager determines that a service is no longer communicating, a failover user move operation from server 1A to server 1B is initiated. User123 is moved from home server 1A and is now homed to server 1B.
2. Unified Personal Communicator determines connectivity with server 1A is lost through time-out, connection loss, or XMPP protocol update, and it initiates a new connection to server 1B.

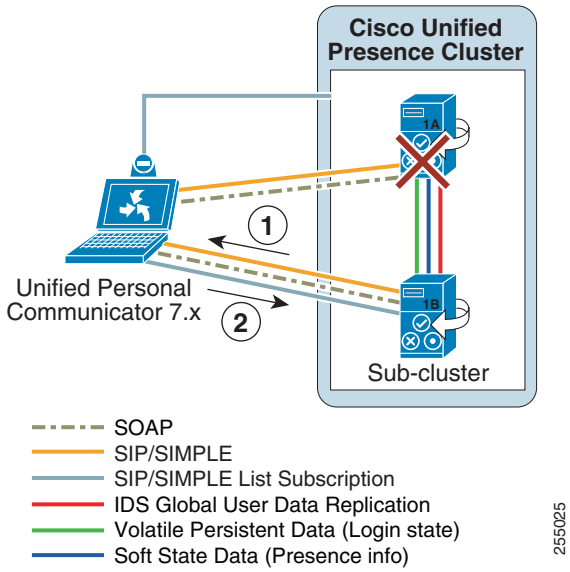
Figure 24-3 Unified Personal Communicator XMPP Failover



As illustrated in Figure 24-4, failure of Cisco Unified Presence server 1A initiates the following sequence of events for SIP-enabled clients:

1. Cisco Unified Presence server 1B sends a SIP NOTIFY message to Cisco Unified Personal Communicator 7.*x*, terminating its Presence and Unified Client Change Notification (UCCN) Subscription-State on server 1A.
2. Cisco Unified Personal Communicator 7.*x* sends a SIP SUBSCRIBE message to Cisco Unified Presence server 1B to reactivate its Presence and UCCN Subscription-State.

Figure 24-4 Unified Personal Communicator SIP Failover



Design Considerations for Cisco Unified Personal Communicator

The required interfaces for Cisco Unified Personal Communicator are Cisco Unified Presence, Cisco Unified Communications Manager (Unified CM), and an LDAP v3 compliant server. Cisco Unified Personal Communicator optional interfaces include Cisco Unity, Cisco Unity Connection, Cisco Unified MeetingPlace, Cisco Unified Videoconferencing, and Cisco Unified MeetingPlace Express VT. In addition to the capacity planning guidelines, when designing and sizing a solution, you must consider the following design considerations:

- The administrator must determine how to install, deploy, and configure the Cisco Unified Personal Communicator in their organization. Cisco recommends using a well known installation package such as Altiris to install the application. Cisco Unified Personal Communicator gathers its configuration information through the SOAP interface on Cisco Unified Presence for the LDAP, CTI, Voicemail, Conferencing, and CCMCIP profiles assigned for the user.
- When using text conferencing rooms, observe the following limits:
  - The maximum users in a text conference is 100 users.
  - The maximum number of messages displayed in the text conference history is 100.
- LDAP Search Context

  The ability to specify an LDAP filter to search an object class, which allows for the retrieval of only users and not computers from the directory, is done by appending &(objectclass=user) to the search context. For example:

  cn=user,**dc**=example,**dc**=com;&(objectclass=user)

  The ability to specify more than a single LDAP search context is done using a # as a delimiter in the LDAP Search Context field on Cisco Unified Presence Administration. An example of the supported format is:

  ou=test,**dc**=example,**dc**=com#**ou**=testing,**dc**=example,**dc**=com

  The Cisco Unified Personal Communicator will search both Organizational Units in order, 'test' then 'testing'.

  Note that the LDAP search context field is limited to 255 characters; thus, the number of supported Organizational Units can vary, depending on the size and number of characters for each individual search context.

Cisco Unified Personal Communicator also allows for federated contacts to be added once Cisco Unified Presence has been configure for a federated deployment. This allows for the user to input and control contacts within their existing domain as well as users of other domains. With this additional contact functionality there is also the ability for users to control privacy settings such as blocked lists and domains that are available for communication.

Cisco Unified Personal Communicator marks Layer 3 IP packets via Differentiated Services Code Point (DSCP). Cisco Unified Personal Communicator marks call signaling traffic with a value of DSCP 24 (PHB CS3), and it marks voice media traffic with a value of DSCP 46 (PHB EF). However, personal computer traffic is typically untrusted, and the network will strip DSCP markings made by an application from the PC. Therefore, access routers and switches must be configured to allow these DSCP markings for the port ranges that Cisco Unified Personal Communicator utilizes. For details on traffic marking, refer to the *Enterprise QoS Solution Reference Network Design (SRND)*, available at

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

Cisco WebEx Connect Architecture

Cisco WebEx Connect consists of two main components:

- Cisco WebEx Connect Client, page 24-16
- Cisco WebEx Connect Platform, page 24-16

Cisco WebEx Connect Client

The Cisco WebEx Connect client is a rich client that resides on an end user's personal computer, running Microsoft Windows XP, Vista, or Windows 7 Operating Systems, and provides availability status, enterprise-grade instant messaging, VoIP audio, PC-to-PC video, desktop sharing, Cisco WebEx meetings integration, Cisco Unified Communications integration, Microsoft Outlook integration for calendaring, presence, instant messaging, click to call, and IBM Lotus Notes calendar integration. Additional details can be found in the *Cisco WebEx Connect Data Sheet*, available at

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

Cisco WebEx Connect Platform

The Cisco Connect Platform is a multi-tenant Software-as-a-Service (SaaS) platform for synchronous and asynchronous collaboration. The WebEx Connect Platform is hosted inside the Cisco WebEx Collaboration Cloud and it enables collaborative applications and integrations, which allows for organizations and end users to customize their work environments. For additional WebEx Connect Platform information, refer to the *WebEx Connect Platform Technical Overview*, available at

http://developer.webex.com/c/document_library/get_file?folderId=11836&name=DLFE-260.pdf

For more information on the Cisco Collaboration Cloud, refer to

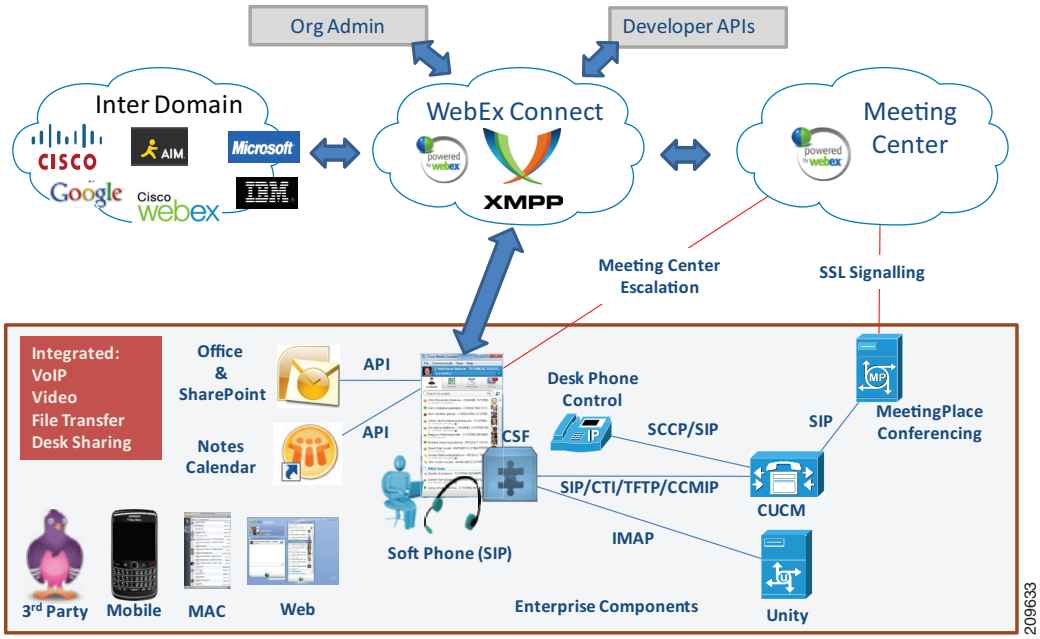
http://www.cisco.com/en/US/prod/ps10352/collaboration_cloud.html

Deploying Cisco WebEx Connect

Cisco WebEx Connect solution deployment consists of the following components, as depicted in Figure 24-5:

- A secure connection (SSL and AES) to the Cisco WebEx Connect XMPP cloud platform for presence, instant messaging, VoIP, PC-to-PC video, media transfer (screen capture and file transfer), and desktop sharing
- Cisco WebEx Meetings
- XMPP federation with other Connect organizations and third-party XMPP clients and XMPP instant messaging (IM) networks
- Cisco Unified Communications integration for call control, voice messaging, and call history
- Microsoft Outlook and IBM Lotus Notes calendar integration
- Integration to Microsoft Outlook for presence and click-to-communicate functionality

Figure 24-5 Deploying Cisco WebEx Connect



Centralized Management

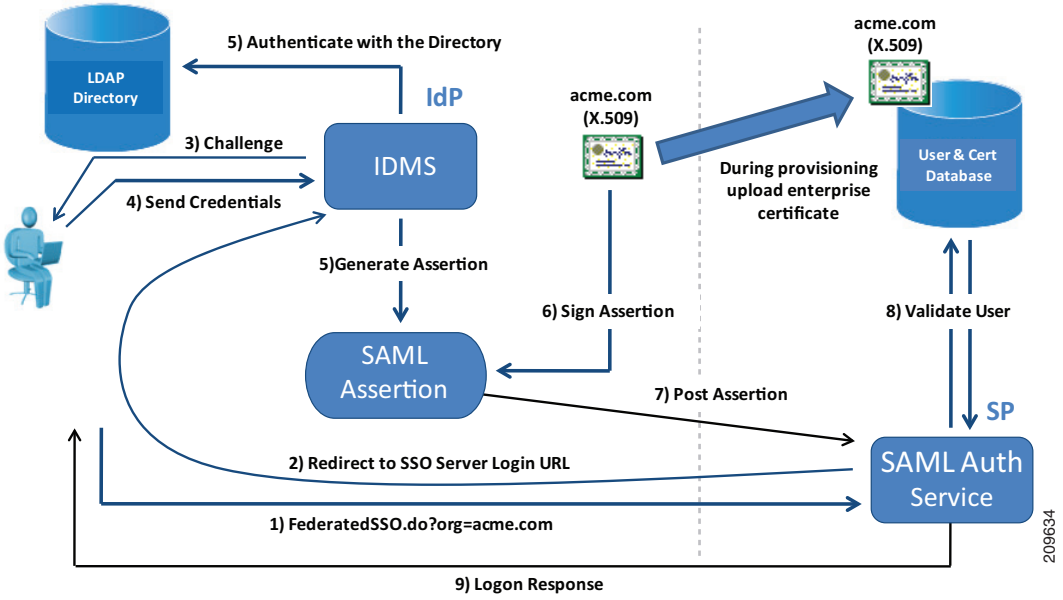
Cisco WebEx Connect provides a web-based administrative tool to manage the solution across the organization. Cisco WebEx Connect users are configured and managed through the Cisco WebEx Connect Administration Tool, which enables administrators to set up basic security and policy controls for features and services. These policies can be applied enterprise-wide, by group, or individually. There are various methods to provision the user database that are further described in the *Cisco WebEx Connect Administrator's Guide*, available at

http://www.webex.com/webexconnect/orgadmin/help/index.htm

Single Sign On

Single Sign On (SSO) enables companies to use their on-premises SSO system, including Security Assertion Markup Language (SAML) support, to simplify the management of Cisco WebEx Connect by allowing users to securely log into Cisco WebEx Connect using their corporate login credentials. The user's login credentials are not sent to Cisco, thus protecting the user's corporate login information. Figure 24-6 shows the credential handshake that occurs on user login to Cisco WebEx Connect.

Figure 24-6 User Login Authentication Process for Cisco WebEx Connect



A user account can be configured to automatically be created the first time a user logs into Cisco WebEx Connect. Users are prevented from accessing Cisco WebEx Connect if their corporate login account is deactivated.

For more information on Single Sign On with WebEx Connect, refer to the *Cisco WebEx Federated SSO Authentication Service Technical Overview*, available at

http://developer.webex.com/documents/10465/22041/Federated+SSO+Authentication+Service.pdf

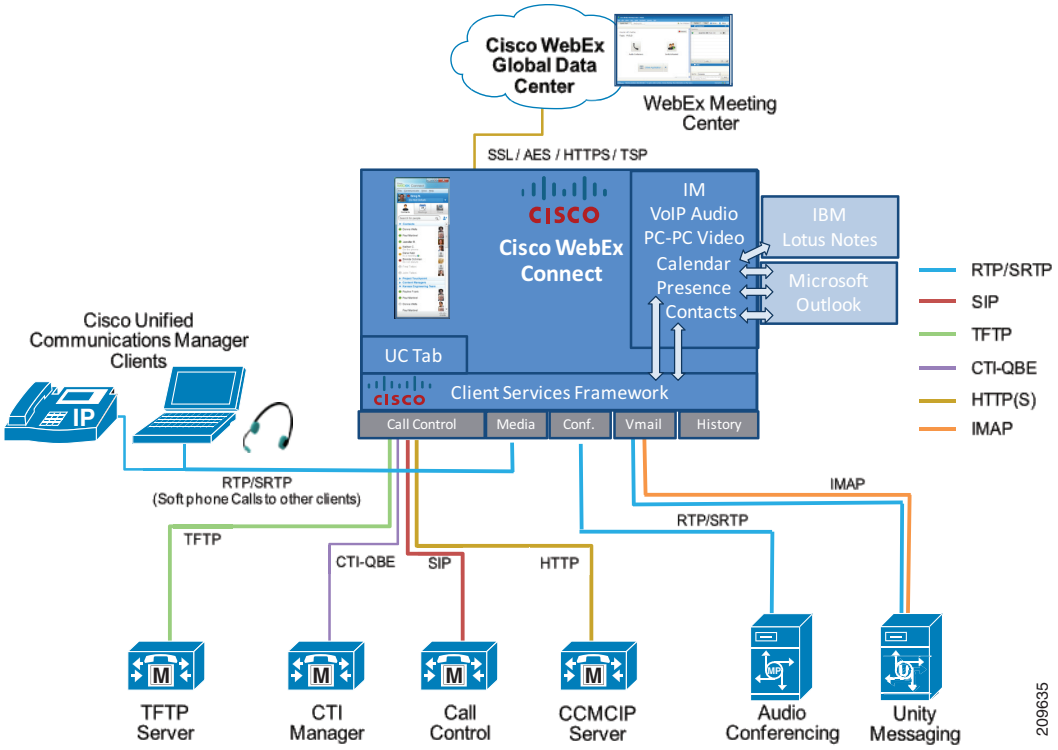
Cisco Unified Communications Integration

Cisco WebEx Connect can be configured for Click-to-Call with Cisco Unified Communications Manager directly from within Cisco WebEx Connect. Cisco Unified Communications can be integrated into Cisco WebEx Connect by means of Cisco Unified Communications Integration™ for Cisco WebEx Connect, page 24-19.

Cisco Unified Communications Integration™ for Cisco WebEx Connect

Cisco Unified Communications Integration™ for Cisco WebEx Connect provides tight integration between Unified CM and Cisco WebEx Connect through the Client Services Framework to enable full call control inside the Cisco WebEx Connect client, as shown in Figure 24-7.

Figure 24-7 Cisco Unified Communications Integration™ for Cisco WebEx Connect

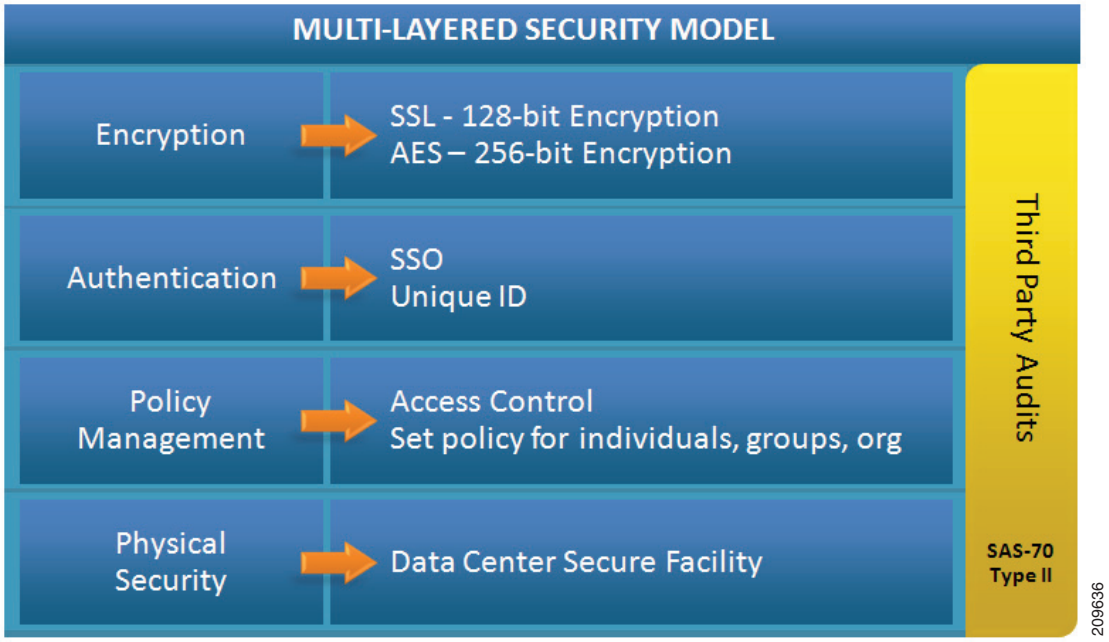


The Client Services Framework allows for softphone call control where the desktop client serves as the audio endpoint, or it allows for desk phone control where the desktop client controls the Cisco Unified IP Phone, and in both cases it is represented by the Phone tab within WebEx Connect. The solution incorporates the instant messaging capabilities, meetings, and calendar integration of Cisco WebEx Connect, while providing access to a broad set of Cisco Unified Communications services, including standards-based audio, unified messaging, deskphone control, and telephony presence, as shown in Figure 24-7.

Security

The Cisco WebEx security model consists of functional layers of security. Figure 24-8 illustrates the separate but interrelated elements that compose each layer.

Figure 24-8 WebEx Security Model



The bottom layer represents the physical security in the Cisco WebEx data centers. All employees go through an extensive background check and must provide dual-factor authentication to enter the datacenter.

The next level is policy management, where the WebEx Connect organization administrator can set and manage access control levels by setting different policies for individual users, groups, or the entire Cisco WebEx Connect organization. White list policies, specific to external users or domains, can be created to allow instant messaging exchanges. The Cisco WebEx Connect organizational model also allows for the creation of specific roles and groups across the entire user base, which allows the administrator to assign certain privileges to roles or groups as well as to set policies, including access control, for the entire organization.

Access to Cisco WebEx Connect is controlled at the authentication layer. Every user has a unique login and password. Passwords are never stored or sent over email in clear text. Passwords can be changed only by the end-users themselves. The administrator can choose to reset a password, forcing the end-user to change his or her password upon the next login. Alternatively, an administrator may choose to use the Single Sign On (SSO) integration between Cisco WebEx Connect and the company's directory to simplify end-user access management. The Single Sign On integration is achieved through the use of an Identity Management System (IDMS).

The encryption layer ensures that all instant messaging communications between Cisco WebEx Connect users is encrypted. All instant messaging communication between Cisco WebEx Connect users and the server in the Connect Collaboration cloud is encrypted by default using SSL encryption. An additional level of security is available whereby IM communication can be encrypted end-to-end using 256-bit AES level encryption. Voice calls using Cisco Unified Communications Integration for Cisco WebEx Connect

in PC (softphone) mode can be encrypted using Secure Real-time Transport Protocol (SRTP). Instant messaging security options are controlled through policy by the Cisco WebEx Connect site administrator, while Cisco Unified Communications Integration for Cisco WebEx Connect security options are controlled by the Cisco Unified Communications Manager administrator or by the end user through the Cisco WebEx Connect client settings under the Unified Communications tab.

Cisco WebEx Connect Platform uses third-party audits such as the SAS70 Type II audit to provide customers with an independent semi-annual security report. This report can be reviewed by any customer upon request with the Cisco Security organization. For additional Cisco WebEx Connect security, refer to the Cisco WebEx Connect IM security white paper, available at

http://wwwin.cisco.com/csg/docs/CiscoWebExConnectSecurityWP.pdf

Firewall Domain White List

Access control lists should be set specifically to allow all communications from the webex.com and webexconnect.com domains and all sub-domains for both webex.com and webexconnect.com. The WebEx Connect Platform sends email to end-users for username and password communications. These email messages come from the mda.webex.com domain.

Logging Instant Messages

Cisco WebEx Connect instant messaging communications are logged on the local hard drive of the personal computer where the user is logged in. Instant message logging is a capability in Cisco WebEx Connect that can be enabled by means of policy through the Org Admin tool. If instant message logging is enabled for Cisco WebEx Connect, instant messages are logged and kept in the following path:

- For Windows XP

  C:\Documents and Settings\<*user*>\Local Settings\Application Data\WebEx Connect\Archive

- For Windows 7

  C:\Users\<*user*>\AppData\Local\WebEx Connect\Archive

The end-user can set logging specifics, whether to enable or disable logging, and how long the logs are kept. These message history settings are located under General in the Cisco WebEx Connect client preferences.

Customers looking for advanced auditing and e-discovery capabilities should consider third-party solutions. Currently Cisco does not provide support for advanced auditing of instant messaging communications. Cisco WebEx Connect, however, does allow for logging and archiving of instant messages exchanged between users. Archiving of the logs is possible though the use of third-party SaaS archiving services, or the logs can be delivered securely to an on-premises SMTP server.

For additional information on instant message archiving, refer to the *Cisco WebEx Connect Administrator's Guide*, available at

http://www.webex.com/webexconnect/orgadmin/help/index.htm

Capacity Planning for Cisco WebEx Connect

A single end-user requires only a 56 kbps dial-up Internet connection to be able to log in to WebEx Connect and get the basic capabilities such as presence, instant messaging, and VoIP calling. However, for a small office or branch office, a broadband connection with a minimum of 512 kbps is required in

order to use the advanced features such as file transfer, screen capture, PC-to-PC video calling, and team spaces. For higher quality video such as High Definition 720p, the minimum bandwidth connection recommendation is 2 Mbps.

For additional information on network and desktop requirements, refer to the *Cisco WebEx Connect Administrator's Guide*, available at

http://www.webex.com/webexconnect/orgadmin/help/index.htm

The Cisco Unified Communications integrations use Unified CM CTI Manager for click-to-call applications, as well as deskphone control mode with the Cisco Unified Client Services Framework. Therefore, observe the CTI limits as defined in the chapter on Call Processing, page 8-1. When Cisco UC Integration™ for WebEx Connect is operating in a softphone (audio on computer) mode, the Cisco Unified Client Services Framework is a SIP registered endpoint with Cisco Unified CM. When sizing a solution involving Cisco Unified Communications, you must include the CTI devices and the SIP endpoint devices utilizing resources on the Unified CM clusters.

Network Requirements

Cisco Webex Connect deployment network requirements are available at:

http://www.webex.com/webexconnect/orgadmin/help/17161.htm

High Availability for Cisco WebEx Connect

WebEx Connect is a Software-as-a-Service (SaaS) application. The end-user PC must be connected to the Internet for the end user to log in to WebEx Connect. A standard Internet connection is all that is required. If an end user is remote, it is not necessary for that user to be connected through the company VPN in order to log in to WebEx Connect. Cisco WebEx Connect can be deployed in a highly available redundant topology. Deployment of Cisco WebEx Connect Software-as-a-Service architecture consists of various network and desktop requirements described in this section.

High Availability

With the use of the multi-tenant Software-as-a-Service architecture, if any individual server in a group fails for any reason, requests can be rerouted to another available server in the Cisco WebEx Connect Platform.

The Cisco WebEx Network Operations Team provides 24x7 active monitoring of the Cisco WebEx Collaboration Cloud from the Cisco WebEx Network Operations Center (NOC). For a comprehensive overview of the Cisco WebEx technology, refer to the information at

http://www.cisco.com/en/US/prod/ps10352/collaboration_cloud.html

Redundancy, Failover, and Disaster Recovery

The Cisco WebEx Global Site Backup architecture handles power outages, natural disaster outages, service capacity overload, network capacity overload, and other types of service interruptions. Global Site Backup supports both manual and automatic failover. The manual failover mode is typically used during maintenance windows. The automatic failover mode is used in case of real-time failover due to a service interruption.

Global Site Backup is automatic and transparent to the end users, is available for all users, and imposes no limits on the number of users that can fail-over.

Global Site Backup consists of the following main components:

- Global Site Service — Is responsible for monitoring and switching traffic at the network level.
- Database Replication — Ensures that the data transactions occurring on the primary site are transferred to the backup site.
- File Replication — Ensures that any file changes are maintained in synchronization between the primary and the backup site.

Design Considerations for Cisco WebEx Connect

Cisco WebEx Connect is deployed as a Software-as-a-Service model, therefore design and deployment considerations are minimal. The Cisco WebEx Connect solution has client options available for the Windows and Mac desktop as well as the popular mobile devices such as Blackberry. Cisco WebEx Connect may also be deployed in a Citrix XenDesktop environment.

Design and deployment consists of interfacing with the Cisco WebEx Connect Platform, otherwise known as the Cisco Collaboration Cloud. Cisco WebEx Connect integrates with Cisco Unified Communications Manager and third-party applications. When deploying Cisco WebEx Connect, use the design considerations described in the following sections.

One Unified CM Integration per Managed Connect Domain

All end users on the same managed Cisco WebEx Connect domain have to use the same Unified CM integration. The creation of sub-groups of end users and the ability to assign a different Unified CM integration to different sub-groups, is currently not supported.

Unified CM CTI Manager

When integrating with Cisco Unified Communications for Cisco WebEx Connect, the Client Services Framework click-to-call is available from CTI. No other call flow and call control capabilities are available.

Refer to the chapter on Call Processing, page 8-1, for supported maximum CTI limits. The CTI numbers are key when using CTI WebDialer with the Cisco Unified Communications Widgets for Cisco WebEx Connect, as well as for desk phone control mode with the Cisco Unified Communications Integration™ for Cisco WebEx Connect.

Third-Party XMPP Clients Connecting to Cisco WebEx Connect Platform

Although Cisco does not officially support any other XMPP clients to connect to the Cisco WebEx Connect Platform, the nature of the XMPP protocol is to allow end users to connect to presence clouds with various XMPP clients using their WebEx Connect credentials. A list of XMPP software clients is available at

http://xmpp.org/software/clients.shtml

Organization policies cannot be enforced on third-party XMPP clients, and features such as end-to-end encryption, desktop share, video calls, PC-to-PC calls, and teleconferences are not supported with third-party clients. To allow non-WebEx Connect XMPP IM clients to authenticate to your Connect domain(s), DNS SRV records must be updated. The specific DNS SRV entry can be found in the Cisco WebEx Connect site administration space, under Configuration and IM Federation.

The use of non-Connect XMPP clients in the Cisco WebEx Connect site administration space, under Configuration and XMPP IM Clients, must be explicitly allowed.

For additional information on enabling third-party XMPP clients to connect to the WebEx Connect platform, refer to the *Cisco WebEx Connect Administrator's Guide*, available at

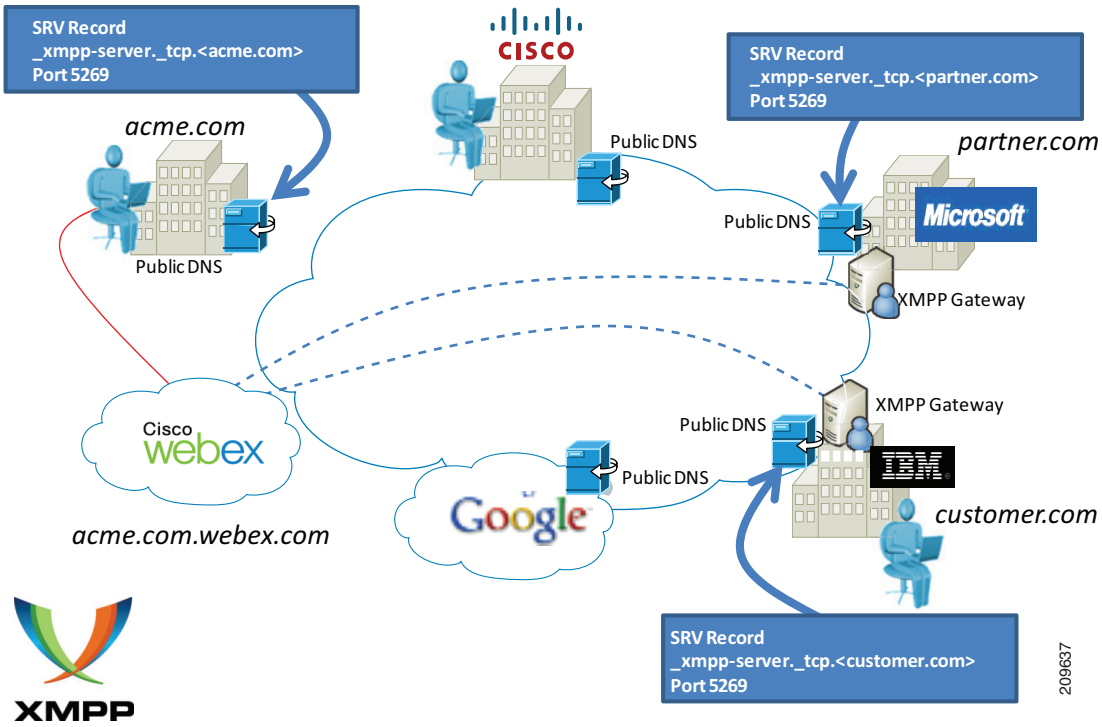
http://www.webex.com/webexconnect/orgadmin/help/index.htm

Instant Message and Presence Federation Using Third-Party XMPP Clients

The Cisco WebEx Connect network can federate with XMPP-based instant messaging networks such as GoogleTalk and Jabber.org. (See Figure 24-9.) A list of public instant messaging networks based on XMPP is available at

http://xmpp.org/

Figure 24-9 Inter-Domain Federation



WebEx Connect can federate with IBM Lotus Sametime through the IBM Lotus Sametime XMPP gateway and with Microsoft Office Communications Server through the Microsoft Office Communications Server XMPP gateway. When using these third-party XMPP gateways, the configuration must be enabled at the back end of the IBM Lotus Sametime and Microsoft Office Communications Server deployments. Cisco does not officially support these configurations, nor does Cisco guarantee interoperability between clients.

Currently WebEx Connect does not interoperate with Yahoo! Messenger and Windows Live Messenger, but it can federate with AIM through a federation gateway.

Other Resources and Documentation

The *Cisco WebEx Connect Administrator's Guide* is available at

http://www.webex.com/webexconnect/orgadmin/help/index.htm

The Cisco WebEx Connect end-user guide is available at

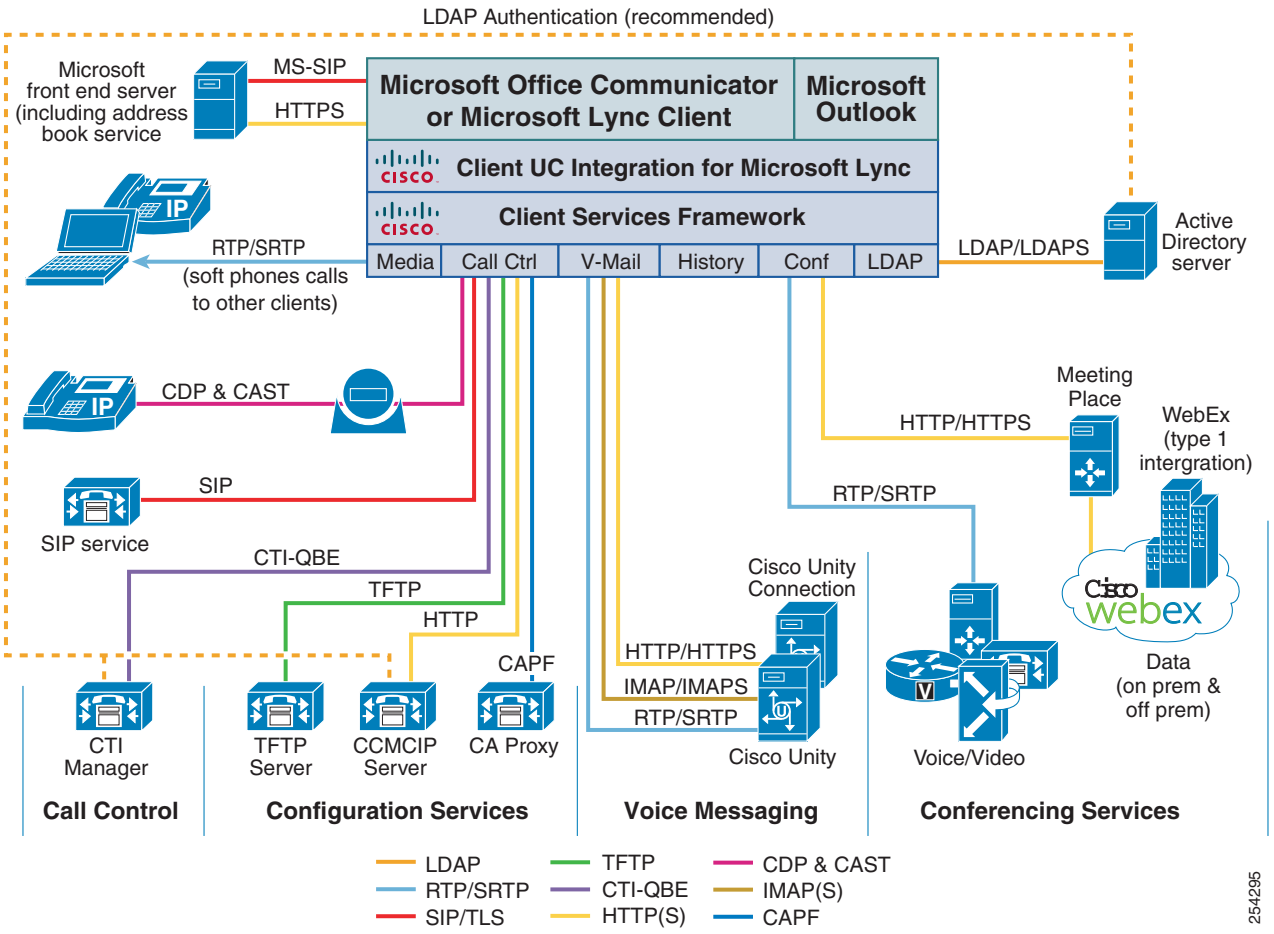
http://www.webex.com/webexconnect/help/wwhelp/wwhimpl/js/html/wwhelp.htm

Cisco UC Integration™ for Microsoft Lync Architecture

Cisco UC Integration™ for Microsoft Lync allows for tightly integrated Cisco Unified Communications services for Microsoft Lync using the Cisco Unified Client Services Framework, while delivering a consistent user experience. The solution extends the presence and instant messaging capabilities of Microsoft Lync by providing access to a broad set of Cisco Unified Communications services, including standards-based audio and video, unified messaging, web conferencing, deskphone control, and telephony presence.

The solution architecture for a Cisco UC Integration™ for Microsoft Lync deployment, shown in Figure 24-10, includes Cisco Unified Communications Manager for audio and video services, Microsoft Office Communications Server 2007 for presence and instant messaging services, Microsoft Active Directory for user account information, Cisco Unified Client Services Framework for PC audio or deskphone control, and Microsoft Lync.

Figure 24-10 Cisco UC Integration™ for Microsoft Lync



With a deployment of Cisco UC Integration™ for Microsoft Lync, the client utilizes user information from the Office Communications Server Address Book that gets downloaded to the client. The address book is generated and delivered to the clients from the Office Communications Server once the user is enabled for presence and instant messaging. Cisco recommends that administrators populate the user

directory number information with an E.164 value (for example, +18005551212) and enable LDAP synchronization and authentication on Unified CM for user account consistency. Cisco UC Integration™ for Microsoft Lync connects to both Cisco Unified CM and Microsoft Active Directory and provides for account credential synchronization rules.

Deploying Cisco UC Integration™ for Microsoft Lync

When deploying Cisco UC Integration™ for Microsoft Lync, observe the guidelines presented in this section.

Configuration Settings

Cisco UC Integration™ for Microsoft Lync reads its configuration settings from a series of registry entries that the administrator must configure. Cisco recommends pushing these registry configuration settings from Microsoft Active Directory by means of Group Policy to distribute the configuration settings automatically to the client computer. Although Group Policy is the recommended installation mechanism, there are other methods available as well, including third-party software deployment tools, batch files, Vbscript, or manual configuration.

Microsoft Active Directory group policies can be extended using administration templates, and the Cisco UC Integration™ for Microsoft Lync provides an administrative template that the administrator can add to provide the group policy support. After the administrative template is loaded, a Cisco UC Integration™ configuration policy can be created by the administrator for the registry configuration settings (TFTP servers, CTI servers, CCMCIP Servers, Voicemail, and LDAP Servers). The registry location where these settings are stored is:

HKCU\Software\Policies\Cisco Systems, inc.\Client Services Framework\AdminData

The Group Policy Management Console can be used to control how and where these group policies are applied to different organizational units. From a client policy perspective, when deploying Cisco UC Integration™ for Microsoft Lync, Cisco recommends setting the Microsoft Telephony Mode Policy to **IM and Presence Only** and **DisableAVConferencing**. These client policy changes will allow for only a single set of call options to be displayed in the Microsoft Lync user experience.

A Cisco UC Integration™ for Microsoft Lync deployment also allows for custom presence states to be defined and deployed in the cisco-presence-states-config.xml file that gets installed. However, Cisco recommends that administrators relocate this file to a HTTPs location, such as the Microsoft Office Communications Server, to allow Microsoft Lync to use this custom presence state file based on the following registry location:

HKLM\Software\Policies\Microsoft\Communicator\CustomStateURL

Software Installation

The software installation can be handled a number of different ways and is designed to be deployed using desktop management tools such as Microsoft Active Directory Group Policy, Systems Management Server (SMS), Altiris, or self-extracting executable with script/batch file. Because customer topologies vary, there is no recommendation about which method to use. For details on the software deployment method, refer to the Cisco UC Integration™ for Microsoft Lync documentation available at

http://www.cisco.com/en/US/products/ps10317/index.html

Capacity Planning for Cisco UC Integration™ for Microsoft Lync

Cisco UC Integration™ for Microsoft Lync uses Unified CM CTI Manager for click-to-dial applications, as well as deskphone control mode with the Cisco Unified Client Services Framework. Therefore, observe the CTI limits as defined in the chapter on Call Processing, page 8-1. When Cisco UC Integration™ for Microsoft Lync is operating in a softphone (audio on computer) mode, the Cisco Unified Client Services Framework is a SIP registered endpoint with Cisco Unified CM. When sizing a solution involving Cisco Unified Communications, you must include the CTI devices and the SIP endpoint devices utilizing resources on the Unified CM clusters.

High Availability for Cisco UC Integration™ for Microsoft Lync

Cisco Unified Client Services Framework provides primary and secondary servers for each of the configuration components, TFTP Server, CTI Manager, CCMCIP Server, Voicemail Server, and LDAP Server. When operating in softphone (audio on computer) mode, the Client Services Framework is a SIP registered endpoint with Cisco Unified CM and it supports all of the registration and redundancy capabilities of a registered endpoint of Unified CM. When operating in deskphone mode, the Client Services Framework is controlling a Cisco Unified IP Phone using CTI, and it supports configuration of a primary and secondary CTI Manager. For additional details on CTI deployment refer to the chapter on Call Processing, page 8-1. The Client Services Framework does not rely on Microsoft Lync being online to support high availability.

Microsoft Lync provides primary and secondary servers with the configuration of enterprise pools for an Office Communications Server deployment. For additional details, refer to the Microsoft Office Communications Server 2007 deployment documentation available at

http://technet.microsoft.com/en-us/library/dd425168%28office.13%29.aspx

Design Considerations for Cisco UC Integration™ for Microsoft Lync

Observe the following design considerations when deploying Cisco UC Integration™ for Microsoft Lync:

- The administrator must determine how to install, deploy, and configure the Cisco UC Integration™ for Microsoft Lync in their organization. Cisco recommends using a well known installation package such as Altiris to install the application, and use Group Policies to configure the user registry settings for the required components of TFTP Server, CTI Manager, CCMCIP Server, Voicemail Pilot, LDAP Server, LDAP Domain Name, and LDAP search contexts.
- Cisco UC Integration™ for Microsoft Lync connects to both Cisco Unified CM and Microsoft Active Directory; therefore, Cisco recommends enabling LDAP Synchronization and LDAP Authentication on Unified CM to allow for integration of the Unified Communications and back-end directory components.
- The address book generated by the Microsoft Office Communications Server and distributed to the clients is used by Cisco UC Integration™ for Microsoft Lync to initiate voice and video calls. Before enabling the user for Microsoft Office Communications Server instant messaging and presence, Cisco recommends configuring the user with an E.164 telephone number in Microsoft Active Directory.

Cisco IP Phone Messenger Application Architecture

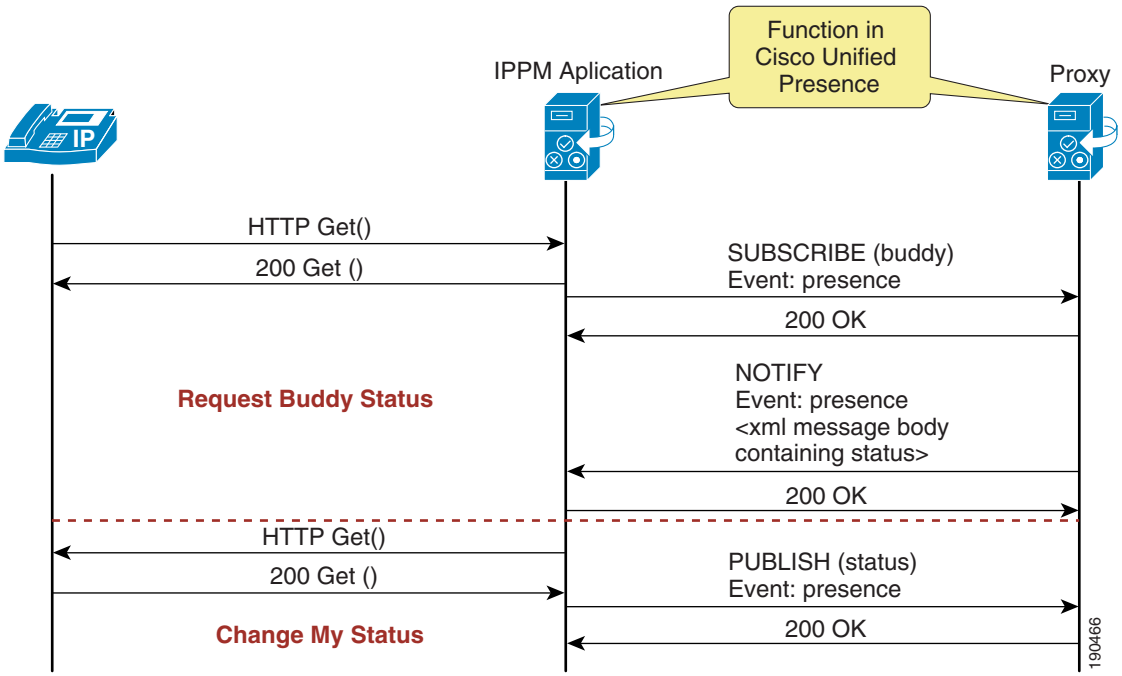
Cisco IP Phone Messenger is a Cisco Unified IP Phone Service that provides users with the ability to create a buddy list, watch their buddies' aggregated presence information, and exchange instant messages with their buddies' Cisco Unified IP Phone or compliant SIP or SIMPLE client or gateway.

The Cisco IP Phone Messenger (IPPM) application, which is a component of Cisco Unified Presence, serves as a protocol translator between HTTP and SIP messaging. The IPPM application communicates with the Cisco Unified IP Phones using XML over HTTP (http://www.cisco.com/go/apps), and it communicates with the SIP Proxy/Registrar Server using SIP. The IPPM application can distinguish between two devices with the same directory number in different partitions and can also function when the user is logged in through Extension Mobility. However, it does rely on the availability of the Cisco Unified Presence publisher for new user logins.

The IPPM application provides the following presence functionality (see Figure 24-11):

- Shows aggregated presence status of a buddy.
- Supports overriding the presence status manually (Available, Busy, Do Not Disturb).
- Upon phone login, SUBSCRIBE to all phone buddies' presence statuses. Upon phone logout, SUBSCRIBE with Expires=0 (terminate subscription).
- Update buddy presence status in the IPPM application upon receipt of a NOTIFY message from the presence engine.
- Manage the contact list from both the phone (Phone Messenger Service) and the web user interface (http://<*cup_server_address*>/ccmuser).

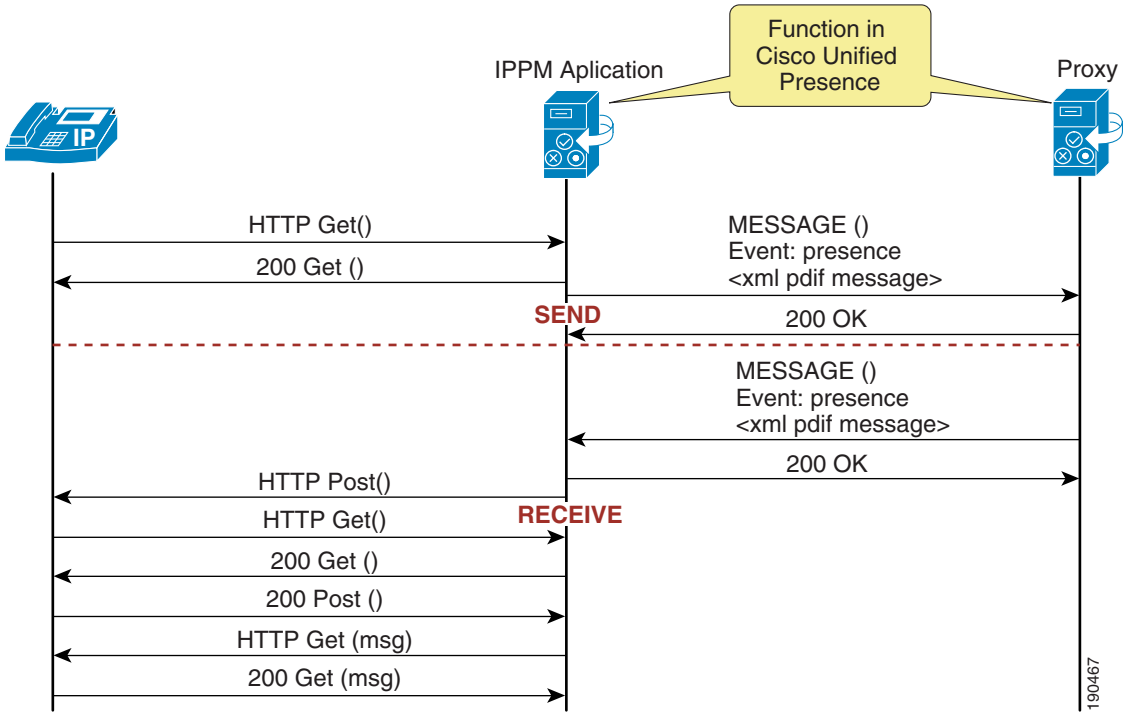
Figure 24-11 IPPM Protocol Translation Presence



The IPPM application provides the following instant messaging (IM) functionality (see Figure 24-12):

- Translates HTTP instant messages from the phone to outbound SIP MESSAGE messages.
- Translates inbound SIP MESSAGE messages to HTTP instant messages to the phone.
- Provides the ability to dial-back a buddy from either the buddy information screen or the IM screen.
- Manages the message history from the phone (Phone Messenger Service).
- Provides the ability to configure canned system-wide and personal IM responses as well as the ability to compose messages.

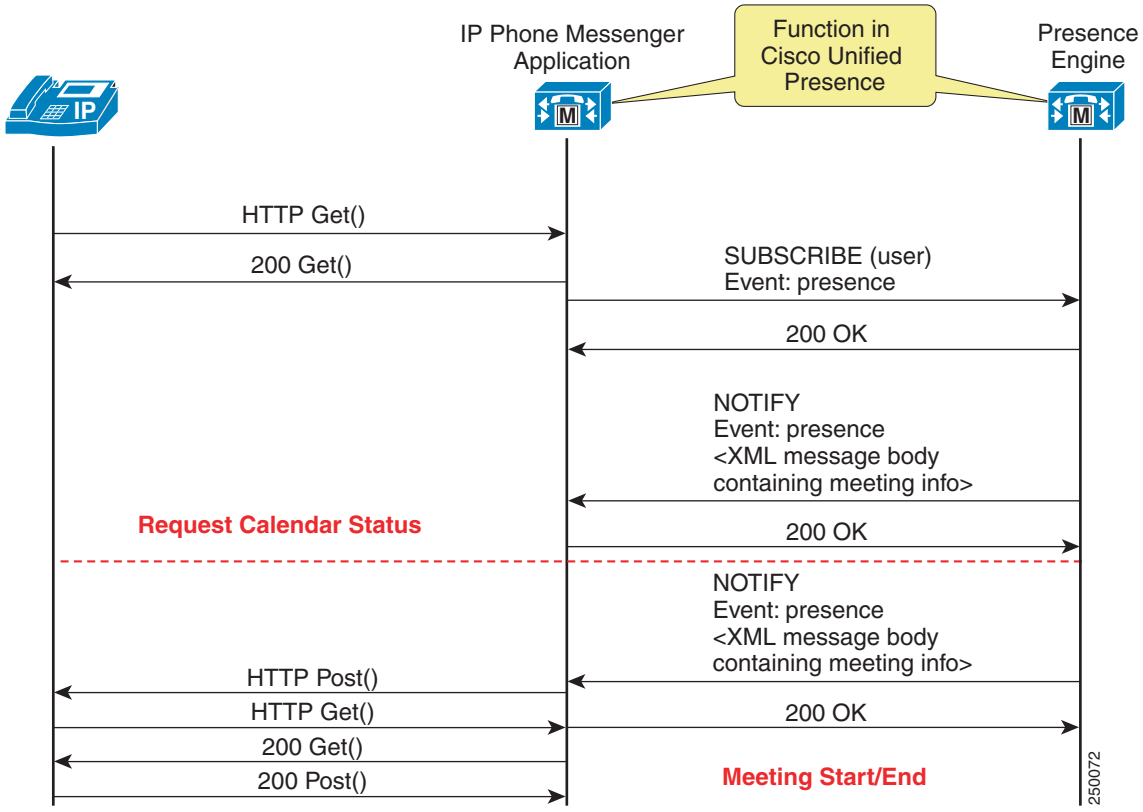
Figure 24-12 IPPM Protocol Translation Instant Message



The IPPM application provides the following meeting notification functionality (see Figure 24-13):

- Meeting reminders can be sent from Cisco Unified Presence to registered IPPM phones without requiring the user to log in to their desktop calendar clients.
- Provides the ability to join a meeting from the IPPM service (through join, dial, or callback).
- Users can control whether to block the meeting reminder feature by means of the end-user configuration page.
- Users can browse the meeting roster list inside the meeting detail screen. The IPPM module will then send a SUBSCRIBE message per participant to the Presence Engine for their presence status. Meeting reminders and instant messages can then be sent to the users on the roster list, based on current availability.

Figure 24-13 IPPM Protocol Translation Meeting Notification



For a listing of the phone models that support Cisco IP Phone Messenger, consult the *Hardware and Software Compatibility Information for Cisco Unified Presence*, available at

http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

High Availability for Cisco IP Phone Messenger

Current IP Phone Services in the Cisco Unified Communications System are configured with either an IP address or DNS A record entry for the HTTP Service URL, which can result in a single point of failure if no IP Phone Service redundancy is configured.

Without IP Phone Services redundancy, the IP Phone Messenger deployment should be load-balanced by means of configuration across both the Cisco Unified Presence publisher and subscriber.

On Unified CM, configure two phone services for IP Phone Messenger, one that uses the Cisco Unified Presence publisher and one that uses the Cisco Unified Presence subscriber, as illustrated in the following example:

- PhoneMessenger1:

  http://publisher.cups.com:8081/ippm/default?name=#DEVICENAME#

- PhoneMessenger2:

  http://subscriber.cups.com:8081/ippm/default?name=#DEVICENAME#

With Cisco IP Phone Messenger, you can deploy the Cisco Unified IP Phones in either of the following ways:

- Single phone service

  With the single phone service, you configure half of the Cisco Unified IP Phones to point to the Cisco Unified Presence publisher (PhoneMessenger1 in the example above), while the other half is configured to point to the Cisco Unified Presence subscriber (PhoneMessenger2 in the example above).

  Advantage — The administrator load-balances the IP Phone Messenger users by means of configuration.

  Disadvantage — If the Cisco Unified Presence server running that phone service fails, the IP Phone Messenger service is unavailable to the users.

- Dual phone service

  With the dual phone service, you configure all Cisco Unified IP Phones to have two IP Phone Messenger services (both PhoneMessenger1 and PhoneMessenger2 in the above example).

  Advantage — If the Cisco Unified Presence server running the phone service fails, the user can try using the IP Phone Messenger service running on the second server.

  Disadvantage — This method relies on the phone user to pick the IP Phone Messenger service to use from the Services menu. This method potentially leads to one Cisco Unified Presence server being selected more than the other, thus resulting in a disproportionate number of users on one particular Cisco Unified Presence server.

With IP Phone Services redundancy (see High Availability for IP Phone Services, page 19-5), IP Phone Messenger can be configured on Unified CM as a single phone service by using the server load balancer (SLB) IP address, as illustrated in the following example:

- PhoneMessenger:

  http://*slb_ip_address*:8081/ippm/default?name=#DEVICENAME#

Capacity Planning for Cisco IP Phone Messenger

The user message history and contact list are both stored in the Cisco Unified Presence database and have the potential to contain large quantities of data. Every user login to the IP Phone Messenger application will download the message history and contact list. Therefore, if bandwidth might be a concern, you can limit the message history size and contact list size through Cisco Unified Presence administration by setting the **Max Instant Message History Size** and **Max Contact List Size** under the IP Phone Messenger settings.

The user has the ability to set a Session Timer parameter for controlling the amount of time the user is logged into the current session and a Refresh Interval parameter for controlling the rate at which presence status updates occur. The administrator currently has no control over these parameters; therefore, the default settings (Session Timer = 480 minutes and Refresh Interval = 30 seconds) are most likely to be used.

Cisco Virtualization Experience Client Architecture

Cisco Virtualization Experience Client (VXC) endpoints enable the end users to have secure real-time access to content and business applications as well as a rich collaborative user experience. These endpoints provide access to collaboration services that are part of the larger Cisco Virtualization Experience Infrastructure (VXI) solution. For information on a complete end-to-end VXI solution design, refer to the documentation available at

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns1100/landing_vxi.html

Deploying Cisco Virtualization Experience Clients

Cisco Virtualization Experience Clients (VXC) are endpoints in the Cisco Unified Communications portfolio; however, they are more than just simple endpoints because they interact with a user's working environment by providing voice, video, and virtual desktop capability and functionality. A user's work environment can assume various profiles (for example, task worker, knowledge worker, or mobile worker), and Cisco has various Virtualization Experience Clients to meet those different needs.

The Cisco VXC 2111 and VXC 2112 provide an integrated form factor that is paired with a Cisco Unified IP Phone 8961, 9951, or 9971 for a fully integrated voice, video, and virtual desktop environment. The Cisco VXC 2211 and VXC 2212 provide a standalone form factor that can be used as simply a virtual desktop (for a task worker) or can be paired with an IP phone for a fully integrated user environment. The Cisco VXC 4000 provides a software-only solution by using a repurposed PC to provide the user with voice and virtual desktop functionality, while the Cisco VXC 6215 provides a Linux-based thin client for fully integrated voice, video, and virtual desktop in a single device. For the mobile worker, Cisco Cius provides a fully secure and integrated voice, video, and virtual desktop environment.

Cisco Virtualization Experience Client Manager

Cisco Virtualization Experience Client (VXC) Manager is a critical and mandatory component of any Virtualization Experience Client deployment. Cisco VXC Manager uses industry standard protocols to manage network intelligent devices simply, efficiently, remotely, and securely using a component-based architecture. As a required component of any VXC deployment, VXC Manager is used to easily manage, organize, upgrade, control, and support various Cisco VXC devices running Independent Computing Architecture (ICA) or PC over IP (PCoIP) protocol.

Note Cisco VXC 4000 is installed on Microsoft Windows only, thus is not managed by VXC Manager. The VXC 4000 Windows installer can be deployed using any common software deployment utility.

Power Over Ethernet

The Cisco Virtualization Experience Client 2111 and 2112 integrated form factor receives power from the spine connector on the unit, which attaches to the Key Expansion port on the Cisco Unified IP Phone 8961, 9951, and 9971. Power to the Cisco Unified IP Phone 8961, 9951, and 9971 is provided through a PWR-CUBE-4 or through 802.3at inline power.

The Cisco Virtualization Experience Client 2211 and 2212 standalone form factor receives power from one of three sources: the PWR-CUBE-4, 802.3at inline power, or 802.3af inline power.

Cisco Cius media station can receive power from the PWR-CUBE-4 or 802.3at inline power.

The Cisco Virtualization Experience Client 4000 and 6215 do not support inline power over ethernet.

Network Considerations (Call Admission Control, Quality of Service, and Bandwidth)

Cisco VXC zero clients (VXC 2111, 2112, 2211, and 2212) provide a virtual desktop environment through display protocol interaction between the zero client and the connection broker datacenter back end. Quality of Service (QoS) is best-effort, and the Cisco VXC zero clients should be placed in the data VLAN. Display protocols inherently use as much bandwidth as a link provides; therefore, bandwidth controls can be put in place at the network port level, or they can be configured through the back-end Citrix or VMware connection broker settings. When a Cisco Unified IP Phone is paired with a VXC zero client, follow existing Unified Communications call admission control, QoS, and bandwidth guidelines.

Cisco VXC 4000 is a software-only solution that uses applications running locally on the PC for a fully integrated solution that includes a thick Virtual Desktop Infrastructure (VDI) client (Citrix Receiver 3.0 or VMware View Client 5.0) and the VXC 4000 software application. With the VXC 4000, QoS is best-effort, and the VXC 4000 should be placed in the data VLAN because all the traffic, voice, and virtual desktop will originate from the local PC resource.

The Cisco VXC 6215 thin client provides a fully integrated software appliance running locally on the device, and it provides display protocol interaction through standard APIs with the hosted virtual desktop environment when used in a fully integrated Unified Communications deployment. The VXC 6215 can operate as a VDI-only endpoint, similar to a Cisco VXC zero client deployment, or it can operate in a fully integrated voice, video, virtual desktop deployment. In both deployments, QoS is best-effort, and the Cisco VXC 6215 should be placed in the data VLAN. Call admission control for voice and video follow existing Cisco Unified IP Phone guidelines, and bandwidth controls for the virtual desktop are provided through the connection broker settings.

Capacity Planning for Cisco Virtualization Experience Clients

All Cisco Virtualization Experience Clients are deployed with a Virtual Desktop Infrastructure (VDI) component, while some of the deployments may also contain a Unified Communications component. Capacity planning and datacenter resource utilization for VDI when using the Cisco Virtualization Experience Clients is covered as part of the Virtualization Experience Infrastructure (VXI) sizing. For details, refer to the VXI documentation available at

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns1100/landing_vxi.html

Capacity planning for the Unified Communications components depends on which Virtualization Experience Client is deployed:

- Cisco VXC 2111 and 2112 integrated form factor zero clients are paired with a Cisco Unified IP Phone 8961, 9951, or 9971. The Cisco client running in the user's virtual desktop uses the deskphone control mode of the Cisco Unified IP Phone; therefore, Computer Telephony Integration (CTI) planning guidelines must be followed for each client deployed.
- Cisco VXC 2211 and 2212 standalone form factor zero clients can be deployed as VDI-only or as a fully integrated voice, video, and virtual desktop with a number of different Cisco Unified IP Phones. When deployed in a Unified Communications environment, the Cisco client running in the user's virtual desktop uses the deskphone control mode of the Cisco Unified IP Phone; therefore, CTI planning guidelines must be followed for each client deployed.
- Cisco VXC 4000 software appliance is a software-only VXC deployment option. The Cisco client running in the user's virtual desktop uses the deskphone control mode of the VXC 4000; therefore, CTI planning guidelines must be followed for each VXC 4000 deployed.

- Cisco VXC 6215 thin client running in VDI-only mode follows VDI capacity planning; however, when the VXC 6215 is deployed as a fully integrated voice, video, and virtual desktop, additional Unified Communications capacity must be accounted for. The Cisco client running in the user's virtual desktop uses the deskphone control mode of the VXC software appliance running locally on the Linux thin client; therefore, CTI planning guidelines must be followed for each client deployed. The VXC software appliance is a SIP line-side registered device on Cisco Unified CM; therefore, for each VXC 6215 thin client running as a fully integrated voice, video, and virtual desktop, a SIP line device and CTI connection is used.

High Availability for Cisco Virtualization Experience Clients

A Cisco Virtualization Experience Client deployment has several aspects that involve high availability: the Virtual Desktop Infrastructure (VDI), the Cisco client running within the hosted virtual desktop (HVD), and the Unified Communications endpoint registered to Unified CM. A user's desktop virtualization environment can be deployed according to Citrix or VMware high availability guidelines. The Cisco client running within the user's virtual desktop supports high availability according to the guidelines listed for Cisco Unified Personal Communicator (see High Availability for Cisco Unified Personal Communicator, page 24-13) and Cisco UC Integration™ for Microsoft Lync (see High Availability for Cisco UC Integration™ for Microsoft Lync, page 24-28). The Unified Communications endpoint registered to Unified CM can be either a Cisco Unified IP Phone when using the Cisco VXC 2111, 2112, 2211, and 2212 zero clients, or the VXC software appliance if using the Cisco VXC 4000 or 6215. These Unified CM registered endpoints support failover for the devices as part of their call control group assignment.

Note CTI failover is not supported with Cisco Virtualization Experience Clients. Survivable Remote Site Telephony (SRST) is supported with the Cisco Unified IP Phones, but SRST is not supported with the VXC software appliance.

Design Considerations for Cisco Virtualization Experience Clients

The following design considerations apply to the Cisco Virtualization Experience Clients:

- Cisco VXC Manager is a required component to manage, configure, and upgrade Cisco Virtualization Experience Clients.
- Cisco Virtualization Experience Clients provide end-user access as part of the larger Cisco Virtualization Experience Infrastructure deployment. Cisco VXI end-to-end solution deployment design guidance is tested and documented as a Cisco Validated Design.
- CTI guidelines must be observed when deploying Cisco Virtualization Experience Clients in a fully integrated voice, video, and virtual desktop environment.
- With the Cisco VXC Software Appliance, QoS is best-effort and the VXC 6215 should be placed in the data VLAN. For details on traffic marking, refer to the *Enterprise QoS Solution Reference Network Design Guide*, available at

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