Cisco Collaboration Clients

Revised: November 19, 2013; OL-30952-01

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.

Cisco Collaboration Clients provide an integrated user experience and extend the capabilities and operations of Cisco Collaboration solutions. These clients enable collaboration both inside and outside the company boundaries by bringing together applications such as online meetings, presence notification, instant messaging, audio, video, voicemail, and many more.

Several Cisco collaboration clients are available. Third-party XMPP clients and applications can also be connected. Cisco Jabber clients integrate with underlying Unified Communication services through a common set of interfaces. In general, each client provides support for a specific operating system or device type. Use this chapter to determine which collaboration clients are best suited for your deployment. The client-specific sections of this chapter also provide relevant deployment considerations, planning, and design guidance around integration into the Cisco Unified Communications System.

The following collaboration clients are supported by the Cisco Unified Communications System:

- Cisco Jabber for Windows and Mac

  Cisco Jabber for Windows and Cisco Jabber for Mac are Unified Communications clients that provide robust and feature-rich collaboration capabilities including standards-based IM and presence, audio and video, visual voicemail, desktop sharing, deskphone control, Microsoft Office integration and contact management.

  Cisco Jabber for Windows and Cisco Jabber for Mac can be deployed to use on-premises services in which Cisco IM and Presence (formerly Cisco Unified Presence) and Cisco Unified Communications Manager provide client configuration, instant messaging and presence, and user and device management. Cisco Jabber for Windows and Cisco Jabber for Mac can also be deployed to use cloud-based services through integration with Cisco WebEx Messenger service.

  Cisco Jabber forms the basis of the current Cisco collaboration clients, which supersede Cisco Unified Personal Communicator and WebEx Connect in future Cisco Unified Communications System releases. Therefore, only Cisco Jabber for Windows and Cisco Jabber for Mac features and functionality are discussed in this chapter. Cisco Unified Personal Communicator and

WebEx Connect clients are still available and supported. For design guidance on Unified Personal Communicator and WebEx Connect clients, refer to the clients information in the *Cisco Unified Communications System 8.x SRND*, available at

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

- Cisco Jabber for Everyone

  Cisco Jabber for Everyone makes Cisco Jabber presence and instant messaging (IM) available at no additional cost for on-premises deployments. Jabber IM client applications and Cisco IM and Presence, zero-cost licenses are available to Cisco Unified Communications Manager customers on the following platforms: Windows, Mac, Android, BlackBerry, iPhone, iPad, and Cisco Jabber Web SDK. For more information on Jabber for Everyone, refer to the latest version of the *Jabber for Everyone Quick Start Guide*, available at

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

- Cisco Jabber for mobile devices

  Cisco provides collaboration clients for the following mobile devices: Android, BlackBerry, and Apple iOS devices such as iPhone and iPad. For more information on Cisco Jabber for mobile devices, see the chapter on Mobile Collaboration, page 23-1.

- Cisco Jabber Video for TelePresence

  Cisco Jabber Video for TelePresence (Jabber Video) extends the reach of TelePresence. Jabber Video works with a compatible PC or Mac and a webcam or Cisco TelePresence PrecisionHD camera to provide high-definition video communications to mobile workers, allowing them to connect to TelePresence systems. Cisco Jabber Video for TelePresence is a video-only client that is used with the Cisco TelePresence Video Communication Server (Cisco VCS) and does not leverage the same common set of interfaces as the other Jabber Clients, such as Jabber for Windows and Jabber for Mac. This document does not discuss details on deploying Cisco Jabber Video for TelePresence. For more information on Cisco Jabber Video for TelePresence, refer to the documentation at

  http://www.cisco.com/en/US/products/ps11328/tsd_products_support_series_home.html

- Cisco UC Integration™ for Microsoft Lync

  Cisco UC Integration™ for Microsoft Lync allows for integrated Cisco Unified Communications services with Microsoft Lync and Microsoft Office Communications Server (OCS) R2, 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 UC Integration™ for IBM Sametime

  Cisco UC Integration™ for IBM Sametime provides instant access to Cisco Unified Communications capabilities directly from IBM Sametime. The integration adds Cisco presence, softphone audio, and HD video capabilities for Sametime IM and presence users. It also includes Cisco desk phone control, integrated voicemail, and the conversation history.

- Third-party XMPP clients and applications

  Cisco IM and 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 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 the Cisco AJAX XMPP Library API). For additional information on the third-party open interfaces, see the chapter on Cisco IM and Presence, page 20-1.

- Cisco Virtualization Experience Media Engine

  The Cisco Virtualization Experience Media Engine (VXME) is an integral collaboration component to a thin client platform, and it extends the reach of the Virtual Desktop Infrastructure (VDI) to include collaboration as part of a fully integrated voice, video, and virtual desktop environment.

- Cisco IP Communicator

  Cisco IP Communicator is a Microsoft Windows-based soft-phone application that brings your work telephone to your personal computer. Unlike the Cisco Jabber Desktop Clients, Cisco IP Communicator does not have IM and Presence capabilities.

What's New in This Chapter

Table 21-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 21-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Cisco Virtualization Experience Media Engine (VXME)	Cisco Virtualization Experience Media Engine, page 21-29	November 19, 2013

Cisco Jabber Desktop Client Architecture

Cisco Jabber for Windows and Cisco Jabber for Mac use a common set of services to provide various Cisco collaboration features, including instant messaging and presence, audio, video, web collaboration, visual voicemail, and so forth. This common set of services provides a simplified client interface and an abstraction layer that allows access to the following underlying communications services:

- SIP-based call control for voice and video softphone clients from Unified CM
- Deskphone call control and "Click to Call" services from Unified CM's CTI interface
- Voice and video media termination for softphone clients
- Instant messaging and presence services using XMPP, from either the Cisco IM and Presence Service or Cisco WebEx Messenger service. Cisco WebEx Meeting Center also offers hosted collaboration services such as online meetings and events
- View scheduled audio, video and web conferencing services
- Desktop sharing using either, video desktop sharing (BFCP) or WebEx desktop sharing
- Visual voicemail services from Cisco Unity Connection using Internet Message Access Protocol (IMAP) or Representational State Transfer (REST)
- Contact management using:
  - Unified CM User Data Service (UDS) as a contact source (LDAP directory synchronization supported)

  - Directory access using Microsoft Active Directory or supported LDAP directories as a contact source
  - WebEx Messenger service
  - Jabber Desktop Client cache and contact list
- Microsoft Outlook Integration, which provides user availability status and messaging capabilities directly through the user interface of Microsoft Office applications such as Microsoft Outlook

The ability to communicate and abstract services and APIs, as shown in Figure 21-1, allows the Jabber Desktop Client 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. Depending on the deployment type, some features may not be supported.

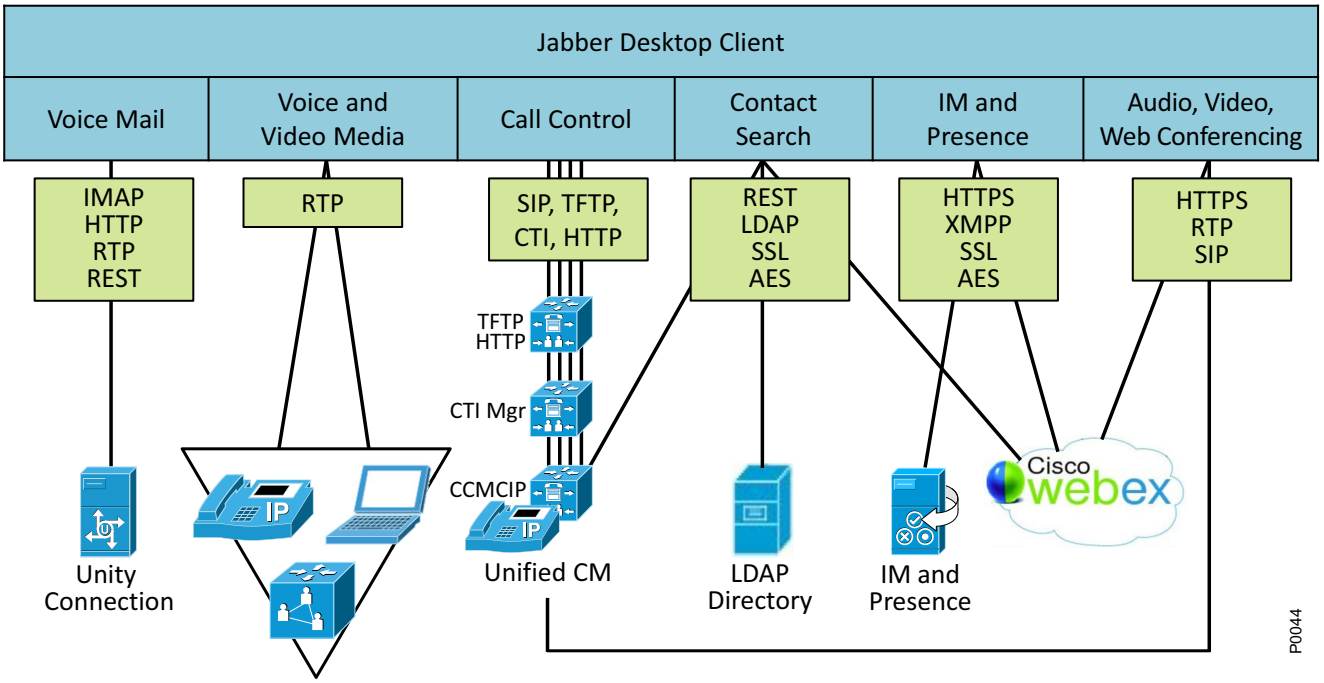
For specific protocol and software support, refer to the latest product documentation for the following Jabber Desktop clients:

- Cisco Jabber for Windows

  http://www.cisco.com/en/US/products/ps12511/index.html
- Cisco Jabber for Mac

  http://www.cisco.com/en/US/products/ps11764/index.html

Figure 21-1 Cisco Jabber Desktop Client Architecture



Cisco Unified Communications Services for Jabber Desktop Clients

The following sections discuss in more detail the underlying Cisco Unified Communications services with which the Cisco Jabber Desktop Clients integrate.

Jabber Desktop Clients – Instant Messaging and Presence Services

Instant messaging and presence services for Jabber clients are provided through an XMPP interface. Cisco offers instant messaging and presence services with the following products:

- Cisco IM and Presence
- WebEx Messenger service

The choice between Cisco IM and Presence or WebEx Messenger service for instant messaging and presence services can depend on a number of factors. WebEx Messenger service deployments use a cloud-based service that is accessible from the internet. On-premises deployments based on Cisco IM and Presence provide the administrator with direct control over their IM and presence platform and also allow presence federation using SIP/SIMPLE to other presence services.

For information on the full set of features supported by each IM and Presence platform, refer to the following documentation:

- Cisco IM and Presence

  http://www.cisco.com/en/US/products/ps6837/products_data_sheets_list.html
- WebEx Messenger service

  http://www.cisco.com/en/US/products/ps10528/index.html

  http://www.cisco.com/en/US/products/ps10528/prod_literature.html

Jabber Desktop Clients – Call Control

Cisco Jabber Desktop Clients can operate in one of two modes for call control:

- Softphone Mode — Using audio and video on a computer

  When a Jabber Desktop Client is in softphone mode, it is directly registered to Unified CM as a SIP endpoint for audio and video call control functionality, and it is configured on Unified CM as device type Client Services Framework.
- Deskphone Control Mode — Using a Cisco IP Phone for audio (and video, if supported)

  When a Jabber Desktop Client is in deskphone control mode, it does not register with Unified CM using SIP, but instead it uses CTI/JTAPI to initiate, monitor, and terminate calls, monitor line state, and provide call history, while controlling a Cisco Unified IP Phone. The Cisco CallManager Cisco IP Phone (CCMCIP) or UDS service on Unified CM is used by the Jabber Desktop Client to retrieve a list of devices associated with each user. This list of devices is used by a client in deskphone mode to choose which Cisco IP Phone it wishes to control.

Softphone Mode

When operating in softphone mode, the Jabber Desktop Client 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 Jabber Desktop Client supports a single line appearance for the user.

The SIP registered device of the Jabber Desktop Client 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. The Jabber Desktop Client in softphone mode uses the CCMCIP or UDS service to discover its device name for registration with Unified CM.

Deskphone Control Mode

When operating in deskphone control mode, the Jabber Desktop Client uses CTI/JTAPI to provide the ability to place, monitor, and receive calls using Cisco Unified IP Phones. When audio calls are received or placed in this mode, the audio path is through the Cisco Unified IP Phone. For video calls, the video stream can originate and terminate either on the Cisco IP Phone (if it has a camera) or on the computer using a approved camera. The Jabber Desktop Client uses the CCMCIP or UDS service on Unified CM to discover the associated devices of the user.

When using deskphone control mode for the Jabber Desktop Client, factor the CTI scaling numbers into the Unified CM deployment calculations. For additional information around capacity planning, see the chapter on Collaboration Solutions Design and Deployment Sizing Considerations, page 27-1.

Jabber Desktop Clients – Dial Plan Considerations

Dial plan and number normalization considerations must be taken into account when deploying the Jabber Desktop Client as part of any Unified Communications endpoint strategy. The Jabber Desktop 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, the need for additional dial rules is minimized because every lookup, resolution, and dialed event results in an E.164 formatted dial string.

If a deployment of Unified CM has implemented a private dial plan (for example, 5551212), then translation of the E.164 number to a private directory number needs to occur on Unified CM. Outbound calls can be translated by Unified CM translation patterns that allow the number being dialed (for example, +18005551212) to be presented to the endpoint as the private number (5551212 in this example). Inbound calls can be translated by means of directory lookup rules. This allows an incoming number of 5551212 to be presented for reverse number lookup caller identification as +18005551212.

Private numbering plan deployments may arise, where the dial plan used for your company and the telephone number information stored in the LDAP directory may require the configuration of translation patterns and directory lookup rules in Cisco Unified Communications Manager to manage number format differences. Directory lookup rules define how to reformat the inbound call ID to be used as a directory lookup key. Translation patterns define how to transform a phone number retrieved from the LDAP directory for outbound dialing.

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. Translation patterns are the recommended method for manipulating dialed numbers. For additional guidelines on translation pattern usage and dial plan management, see the chapter on Dial Plan, page 14-1.

Application Dialing Rules

Application dialing rules can be used as an alternative to translation patterns to manipulate numbers that are dialed. Application dialing rules can automatically strip numbers from, or add numbers to, phone numbers that the user dials. Application Dial Rules are configured in Unified CM and are downloaded to the client from Unified CM. Translation patterns are the recommended method for manipulating dialed numbers.

Directory Lookup Rules

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

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.

Jabber Desktop Clients – Audio and Video Media

A number of standard audio and video codecs for use in low bandwidth or high fidelity deployments are supported with the Jabber Desktop Client.

The Jabber Desktop Client 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 references the Jabber Desktop Client can use to determine the video frame rate for a call. The processing power and CPU used by the client play an important role in determining the video frame rate used. Another decision point is based on the Windows Experience Index (WEI) for the personal computer being used (see 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 client system requirements, video frame rates based on H.264 Level, and WEI encode and decode values, refer to the Client Application Release Notes, page 21-8.

Bandwidth utilization for audio and video calls from the Jabber Desktop Client can be maintained using the Unified CM regions and locations call admission control mechanisms. Administratively placing the Jabber Desktop Client in a Region provides the ability to control the per-call voice and video bandwidth usage and the preferred audio codecs to be used for calls within and between regions. Unified CM locations-based call admission control, and/or the use of RSVP, provides intra-location and inter-location audio and video bandwidth control. The Jabber Desktop Client requires the Unified CM region per-call bandwidth settings 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 session 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 for call admission control, see the chapter on Call Processing, page 9-1.

Quality of Service for Audio and Video Media from Softphones

An integral part of the Cisco Unified Communications network design recommendations is to classify or mark voice and video traffic so that it can be prioritized and appropriately queued as it traverses the network. There are a number of different methods to classify and remark traffic:

- Mapping identifiable media and signaling streams

  This method consists of assigning the Jabber client to use specific UDP and TCP ports and to re-mark the signaling and media based on these port ranges.

- Jabber for Cisco Media Services Interface (MSI) and metadata

  This method consists of using a PC product called Jabber for MSI, which informs the network of the traffic classifications of the media through metadata and allows Cisco switches and routers that support metadata to re-mark media based on these classifications.

- Trusted Relay Point (TRP),

  This method is a software function that uses a media termination point (MTP) provider and is dynamically inserted in a call flow by the Cisco Unified CM call processing agent. Cisco Unified CM inserts a trusted relay point (TRP) in front of the endpoint, and the media stream from the endpoint can be forced to flow through the TRP. The TRP re-marks the DSCP according to instructions from Cisco Unified CM, and the switch or router is configured to honor and trust media packets sent from the TRP.

Other methods do exist, such as Unified CM RSVP Agent. This method achieves both admission control and QoS enforcement and is discussed in detail in the chapter on Call Admission Control, page 13-1. However, audio and video QoS marking on PCs is likely not to be trusted given the wide range of applications and traffic generated by PCs. So re-marking of packets based on port and/or protocol is likely required. For more details on QoS recommendations, see the chapter on Network Infrastructure, page 3-1.

Client Application Release Notes

- Cisco Jabber for Windows

  http://www.cisco.com/en/US/products/ps12511/prod_release_notes_list.html

- Cisco Jabber for Mac

  http://www.cisco.com/en/US/products/ps11764/prod_release_notes_list.html

Jabber Desktop Clients – Audio, Video and Web Conferencing Services

Access to scheduled conferencing services for clients can be provided through an HTTP interface. Cisco audio, video and web-based scheduled conferencing services can be provided by using the cloud-based WebEx Meeting Center service or a combination of on-premises MeetingPlace audio and video conferencing services and WebEx cloud-based web conferencing services. For more information, refer to the following documentation:

- Cisco Unified MeetingPlace

  http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_data_sheets_list.html

- WebEx Meeting Center

  http://www.psimeeting.com/pdf/WebEx_Meeting_Center.pdf

Jabber Desktop Clients – Contact Management

The Jabber Desktop Client can use one of the following contact sources for contact search and information:

- Cisco Unified CM User database via the User Data Service (UDS)
- LDAP directory integration
- WebEx Messenger service

Contacts can also be stored and retrieved locally using either of the following:

- Jabber Desktop Client Cache
- Local address books and contact lists such as Microsoft Outlook

The Jabber Desktop Client uses reverse number lookup to map an incoming telephone number to a contact, in addition to photo retrieval. The Jabber Desktop Client contact management allows for up to five search bases to be defined for LDAP queries.

Cisco Unified CM User Data Service (UDS)

UDS provides clients with a contact search service on Cisco Unified Communications Manager. You can synchronize contact data into the Cisco Unified CM User database from Microsoft Active Directory or other LDAP directory sources. Clients can then automatically retrieve that contact data directly from Unified CM using the UDS REST interface.

LDAP Directory

You can configure a corporate LDAP directory to satisfy a number of different requirements, including the following:

- User provisioning — You can provision users automatically from the LDAP directory into the Cisco Unified Communications Manager database using directory integration. Cisco Unified CM synchronizes with the LDAP directory content so that you avoid having to add, remove, or modify user information manually each time a change occurs in the LDAP directory.
- User authentication — You can authenticate users using the LDAP directory credentials. Cisco IM and Presence synchronizes all the user information from Cisco Unified Communications Manager to provide authentication for client users.
- User lookup — You can enable LDAP directory lookups to allow Cisco clients or third-party XMPP clients to search for contacts in the LDAP directory.

WebEx Directory Integration

WebEx Directory Integration is achieved through the WebEx Administration Tool. WebEx imports a comma-separated value (CSV) file of your enterprise directory information into its WebEx Messenger service. For more information, refer to the documentation at

http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?17444.htm

Jabber Desktop Client Cache

The Jabber Desktop Client maintains a local cache of contact information derived from previous directory queries and contacts already listed, as well as the local address book or contact list. If a contact for a call already exists in the cache, the Jabber Desktop Client does not search the directory. If a contact does not exist in the cache, the Jabber Desktop Client performs a directory search.

Directory Search

When a contact cannot be found in the local Jabber Desktop Client cache or contact list, a search for contacts can be made. The WebEx Messenger user can utilize a predictive search whereby the cache, contact list, and local Outlook contact list are queried as the contact name is being entered. If no matches are found, the search continues to query the corporate directory (WebEx Messenger database).

Deploying Jabber Desktop Clients

Cisco recommends using the Bulk Administration Tool for the deployment of Jabber Desktop Clients. 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 Jabber Desktop Clients

Cisco Jabber Desktop Clients operate as either a SIP endpoint registered to Unified CM or as a deskphone controller of a Cisco Unified IP Phone using a CTI connection to Unified CM. When planning a deployment of the Jabber Desktop Client, 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 and CTI controlled devices. The following additional items must be considered for a Jabber Desktop Client deployment:

- Device Configuration

  When configured in softphone mode, a Jabber Desktop Client configuration file is downloaded through TFTP or HTTP 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 or HTTP to Jabber Desktop Client devices.

  The Jabber Desktop Client uses the Cisco CallManager Cisco IP Phone (CCMCIP) or UDS service to gather information about the devices associated with a user, and it uses this information to provide a list of IP phones available for control by the client in deskphone control mode. The Jabber Desktop Client in softphone mode uses the CCMCIP or UDS service to discover its device name for registration with Unified CM.

- Deskphone Mode

  When configured in deskphone mode, the Jabber Desktop Client establishes a CTI connection to Unified CM upon login and registration to allow for control of the IP phone. Unified CM supports up to 40,000 CTI connections. If you have a large number of clients operating in deskphone mode, make sure that you evenly distribute those CTI connections across all Unified CM subscribers running the CTIManager service. This can be achieved by creating multiple CTI Gateway profiles, each with a different pair of CTIManager addresses, and distributing the CTI Gateway profile assignments across all clients using deskphone mode.

- Voicemail

  When configured for voicemail, the Jabber Desktop Client updates and retrieves voicemail through an IMAP or REST connection to the mailstore.

- Authentication

  Client login and authentication, contact profile information, and incoming caller identification are all handled through a query to the LDAP directory, unless stored in the local Jabber Desktop Client cache. Authentication for voicemail can be set to use the same authentication as IM and Presence; however, when using WebEx Messenger, users need to enter their credentials manually.

- Contact Search

  There are several contact sources that can be used with the Jabber Desktop Client. For example, the UDS service can be used by clients to search for contacts in the Unified CM User database. Alternatively, LDAP integration can be used. If the requested contact cannot be found in the local Jabber Desktop Client cache, UDS or LDAP contact searches take place. When using the WebEx Messenger service, contact search uses the WebEx database.

High Availability for Jabber Desktop Clients

Cisco Jabber Desktop Clients use primary and secondary servers for each of the following configuration components: TFTP server, HTTP server, CTIManager, CCMCIP server, voicemail server, UDS server, and LDAP server. When operating in softphone mode, the Jabber Desktop Client is registered with Cisco Unified CM as a SIP endpoint, and it supports all of the registration and redundancy capabilities of a registered endpoint of Unified CM. When operating in deskphone mode, the Jabber Desktop Client is controlling a Cisco Unified IP Phone using CTI, and it supports configuration of a primary and secondary CTIManager in the CTIManager Profile. For additional details on CTI deployment, see the chapter on Call Processing, page 9-1.

Design Considerations for Jabber Desktop Clients

Observe the following design considerations when deploying the Cisco Jabber Desktop Client:

- The administrator must determine how to install, deploy, and configure the Jabber Desktop Client in their organization. Cisco recommends using a well known installation package such as Altiris to install the application.
- The userid and password configuration of the Jabber Desktop Client user must match the userid and password of the user stored in the LDAP server or local database 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 translation patterns or application dialing rules and directory lookup rules.
- 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 purposes, you must consider the port usage required for Jabber Desktop Clients and corresponding applications being integrated.
- 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 Jabber Desktop Client rather than a top-level search base for the entire deployment.

- Utilize the DNS SRV infrastructure for Service Discovery to automatically discover required services for Jabber and reduce user intervention. For details, refer to the *Cisco Jabber DNS Configuration Guide*, available at

  http://www.cisco.com/web/products/voice/jabber.html

Common Deployment Models for Jabber Clients

Cisco Jabber for Windows and Jabber for Mac clients support the following deployment models:

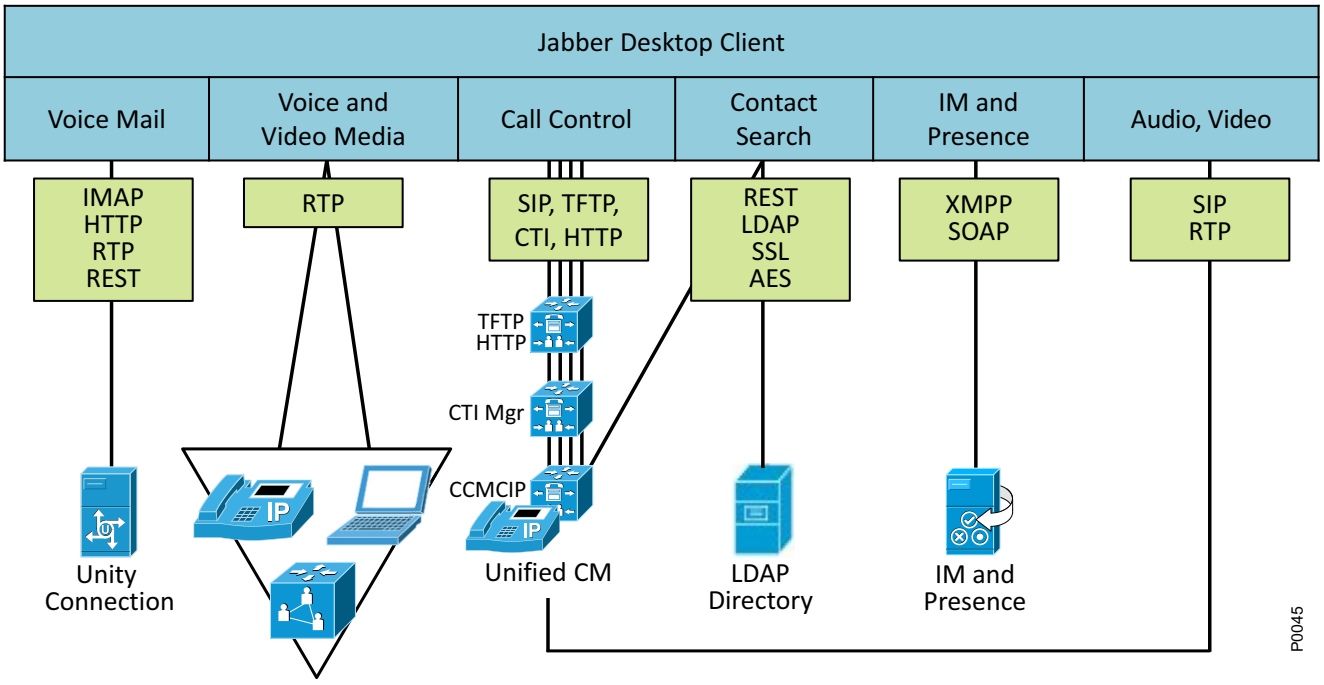
- On-Premises Deployment Model, page 21-12
- Cloud-Based Deployment Model, page 21-14
- Hybrid Cloud-Based and On-Premises Deployment Model, page 21-15

Your choice of deployment will depend primarily upon your product choice for IM and presence and the requirement for additional services such as voice and video, voicemail, and deskphone control.

On-Premises Deployment Model

The on-premises deployment model is one in which all services are set up and configured on an enterprise network that you manage and maintain. (See Figure 21-2.)

Figure 21-2 Jabber On-Premises Deployment Model



The on-premises deployment model for Cisco Jabber for Windows relies on the following components:

- Cisco Unified Communications Manager provides all user and device configuration capabilities.
- Cisco Unified Communications Manager and Cisco conferencing devices provide audio and video conferencing capabilities.
- Cisco Unity Connection provides voicemail capabilities.
- Cisco IM and Presence provides instant messaging and presence services.
- Microsoft Active Directory or another supported LDAP directory provides contact sources.

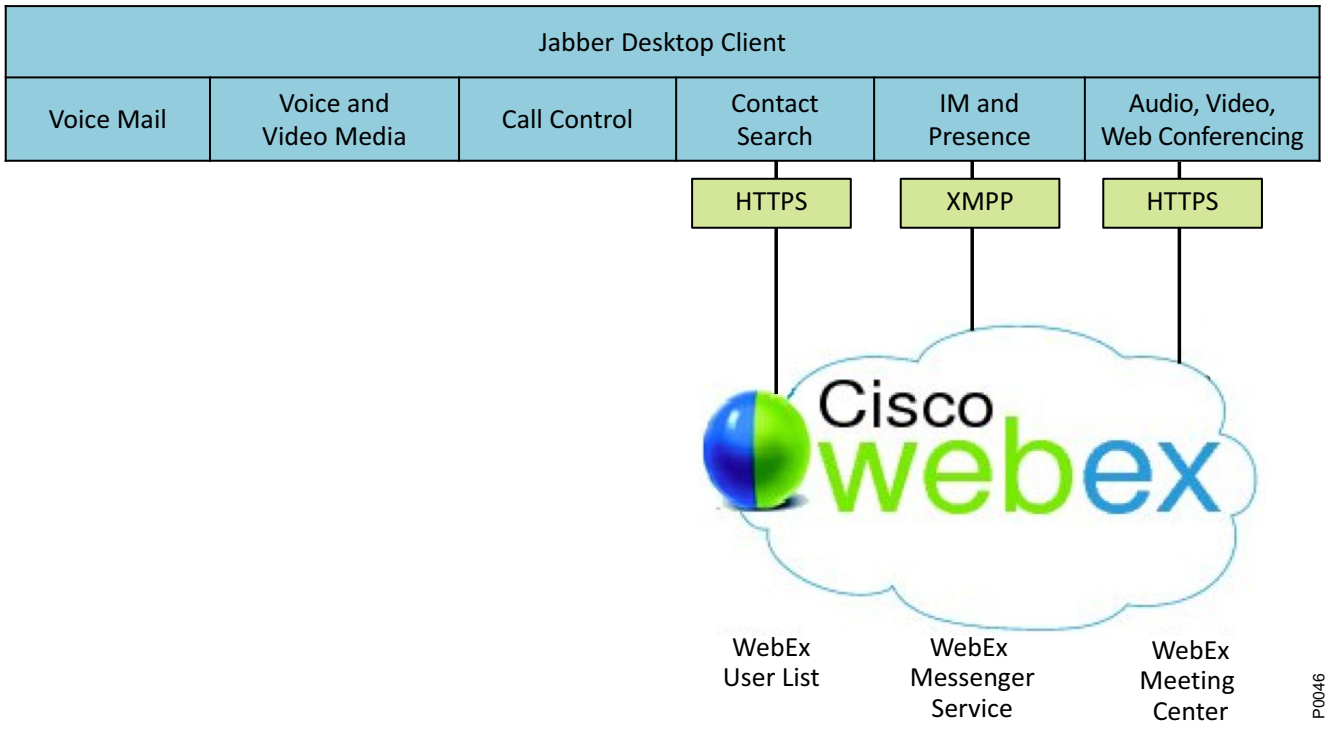
These components are the essential requirements to achieve a base deployment of Cisco Jabber clients. After you set up and configure a base deployment, you can set up and configure additional deployment options such as:

- Voice — Provides audio call capabilities.
- Video — Provides capabilities to enable users to transmit and receive video calls.
- Voicemail — Provides voicemail capabilities that users can retrieve directly in the Cisco Jabber client user interface or when users dial their voicemail number.
- Desktop sharing — Enables users to share their desktops via Binary Flow Control Protocol (BFCP).
- Microsoft Office integration — Provides user availability status and messaging capabilities directly through the user interface of Microsoft Office applications such as Microsoft Outlook.

Cloud-Based Deployment Model

The cloud-based deployment model is one in which all, or most, services are hosted in the cloud using Cisco WebEx. When implementing a cloud-based deployment model using Cisco WebEx, you manage and monitor your cloud-based deployment with the Cisco WebEx Administration Tool. (See Figure 21-3.)

Figure 21-3 Jabber Cloud-Based Deployment Model (WebEx)



The cloud-based deployment model for Cisco Jabber for Windows relies on Cisco WebEx Messenger service for the following services:

- Instant messaging and chat capabilities
- Presence capabilities for users
- Native desktop sharing
- User configuration and contact sources

These services are the essential components required to achieve a base deployment of Cisco Jabber for Windows. After you set up and configure a base deployment, you can set up and configure additional deployment options such as:

- Cisco WebEx Meeting Center — Offers hosted collaboration features such as online meetings and events.
- Microsoft Office integration — Provides user availability status and messaging capabilities directly through the user interface of Microsoft Office applications such as Microsoft Outlook. This integration is set up by default.

- Calendar integration — Calendar integration with WebEx Meeting Center, Outlook, and IBM Lotus Notes is also supported.

For information on WebEx Messenger service configuration for Jabber Clients, refer to the WebEx administration guide available at

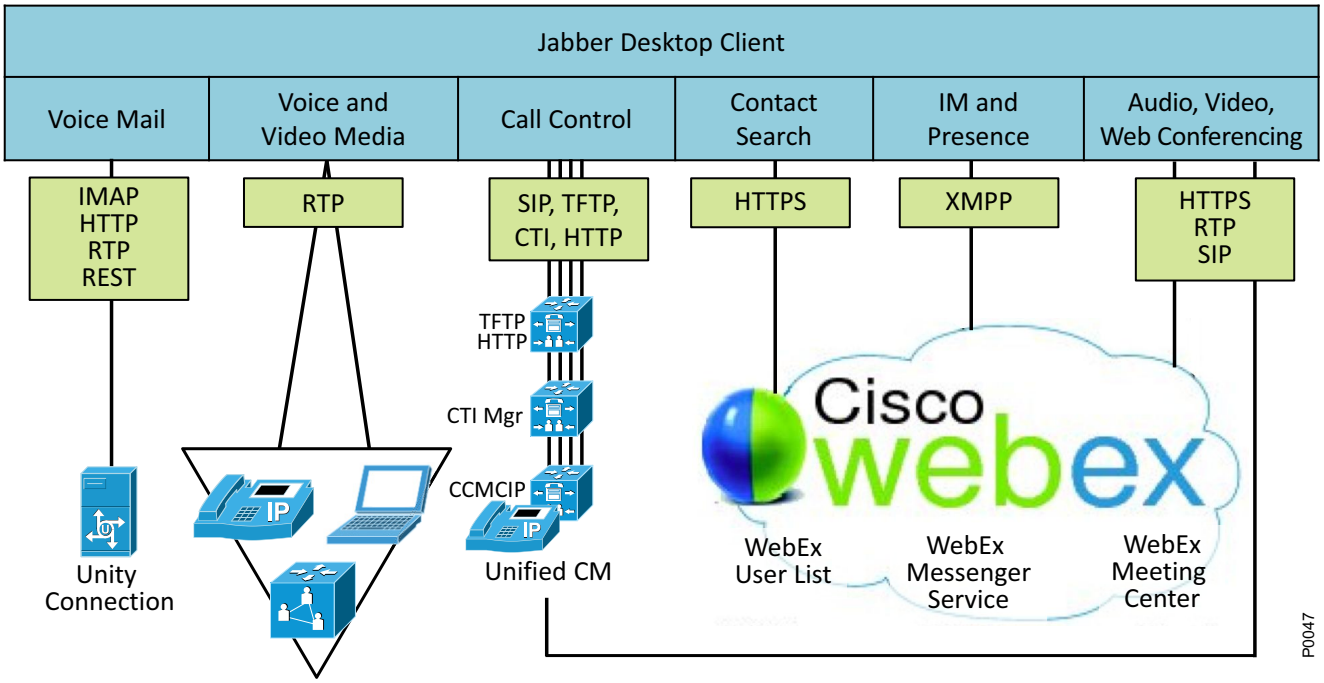
http://www.webex.com/webexconnect/orgadmin/help/index.htm

Hybrid Cloud-Based and On-Premises Deployment Model

A hybrid deployment is one in which the cloud-base services hosted on Cisco WebEx Messenger service are combined with the following components of an on-premises deployment (see Figure 21-4):

- Cisco Unified Communications Manager provides user and device services.
- Cisco Unity Connection provides voicemail services.

Figure 21-4 Jabber Hybrid Cloud -Based and On-Premises Deployment Model



Integration with Cisco WebEx Messenger service, Cisco Unified Communications Manager, and Cisco Unity Connection lets you extend your cloud-based deployment and enable the following deployment options:

- Voice — Provides audio calls managed through Cisco Unified Communications Manager.
- Video — Provides capabilities to enable users to transmit and receive video calls.
- Voicemail — Provides voicemail capabilities that users can retrieve directly in the Cisco Jabber for Windows user interface or when users dial their voice mailbox number.
- Desktop Sharing — Enables users to share their desktops.

Client-Specific Design Considerations

The following sections discuss design considerations that are specific to Cisco Jabber for Windows and Jabber for Mac. For common design considerations for these client types, use the design guidance provided in the section on Cisco Jabber Desktop Client Architecture, page 21-3.

Cisco Jabber for Windows

Cisco Jabber for Windows is a Unified Communications client that provides robust and feature-rich collaboration capabilities that include the following:

- Chat over XMPP, including:
  - Rich text formatting
  - File transfer
  - Screen capture
  - Group chat
  - Emoticons
- Desk phone control
- Software phone calling
- High definition video
- Desktop sharing
- Deskphone video
- Visual voicemail
- Microsoft Office integration
- Lotus Notes calendar integration
- Contact search
- Extend and Connect
- Support for custom embedded tabs to render HTML content

Jabber for Windows clients support on-premises, cloud-based, and hybrid deployment models.

Client Launch Sequence

The following steps describe, at a high level, the initial Cisco Jabber for Windows launch sequence for on-premises deployment:

1. Retrieve the presence server type (WebEx or Unified IM and Presence) from jabber-bootstrap.properties in the installation directory.
2. Authenticate with the presence server.
3. Retrieve profile details and connect to available services such as:
   - HTTP servers
   - CTI gateway servers
   - User Data Service (UDS) servers

- Voicemail servers
- Directory servers

4. Retrieve Cisco Jabber for Windows configuration files. These XML files are loaded from the HTTP server and can contain additional configuration information such as:
   - Client configuration parameters for automatic updates, password reset URL, and so forth
   - Client policy parameters to allow/disallow screen captures, files transfers, and so forth
   - Directory service information such as directory type and directory attribute mappings
   - Application dial rules and directory look up rules

The high-level launch sequence for WebEx cloud deployment is as follows:

1. The client securely authenticates to the WebEx Messenger service.
2. The client retrieves profile details and User Contact list, WebEx Meeting Center URL, server information (such as Unified CM servers and voicemail servers), and pilot number.

Contact Sources

Cisco Jabber for Windows defaults to using Enhanced Directory Integration (EDI), which uses preconfigured directory attribute mappings for integration with Microsoft Active Directory. For integration with an LDAP directory that requires custom attribute mapping, these attribute mappings can be created in a configuration file that can be downloaded to the client from a Unified CM HTTP server. Cisco Jabber for Windows does *not* use directory settings that are specified in the Cisco IM and Presence Service configuration.

Jabber for Windows also supports the Unified CM User Data Service (UDS), which allows a client to search for contacts using the Unified CM user database (which may be synchronized with an LDAP directory). In addition, Jabber for Windows supports Microsoft Outlook local contact, which allows users to search for contacts that are in the user's Microsoft Outlook client.

Video Rate Adaptation and Resolution

Cisco Jabber for Windows uses the Cisco Precision Video Engine and ClearPath technology to optimize video media. The Cisco Precision Video Engine uses fast video rate adaptation to negotiate optimum video quality based on network conditions. Video rate adaptation dynamically scales video quality upward when video transmission begins. Cisco Jabber for Windows also saves history so that subsequent video calls begin at the optimal resolution. ClearPath technology improves resolution on sub-optimal networks by reducing the effects of packet loss.

Jabber for Windows supports desktop sharing using either WebEx Desktop Share or Video Desktop Share (using BFCP). Jabber for Windows also supports deskphone video. When deskphone video is enabled, sufficient bandwidth must be provisioned.

For more information on the configuration options and administration of a Jabber for Windows client, refer to the latest version of the *Cisco Jabber for Windows Installation and Configuration Guide*, available at

http://www.cisco.com/en/US/products/ps12511/prod_installation_guides_list.html

Also refer to the Jabber for Windows Release Notes, available at

http://www.cisco.com/en/US/products/ps12511/prod_release_notes_list.html

For specific details about Jabber for Windows client features, refer to the Jabber for Windows data sheet, available at

http://www.cisco.com/en/US/products/ps12511/products_data_sheets_list.html

Extend and Connect

Jabber for Windows supports Extend and Connect, which enables users to make and receive calls from Jabber using third-party phones. This allows users to utilize their existing third-party PBX phones while taking advantage of Cisco Collaboration features. There are several modes within Extend and Connect, and each mode requires different trunk usage. The dial plan must be designed carefully for Extend and Connect. For more details on dial plan design, see the chapter on Dial Plan, page 14-1.

Cisco Jabber for Mac

Cisco Jabber for Mac is a Unified Communications client that provides robust and feature-rich collaboration capabilities that include the following:

- Chat over XMPP, including:
  - Rich text formatting
  - File transfer
  - Screen capture
  - Group chat
  - Emoticons
- Desk phone control
- Software phone calling
- Visual voicemail
- Contact search

Cisco Jabber for Mac clients support on-premises, cloud-based, and hybrid deployment models.

Client Launch Sequence

The following steps describe, at a high level, the initial Cisco Jabber for Mac launch sequence for on-premises deployment:

1. Retrieve the presence server type (WebEx or Cisco IM and Presence) from jabber-bootstrap.properties in the installation directory.
2. Authenticate with the presence server.
3. Retrieve profile details and connect to available services such as:
   - TFTP servers
   - CTI gateway servers
   - Cisco CallManager Cisco IP Phone (CCMCIP) servers
   - Voicemail servers
   - Directory servers

4. Retrieve Cisco Jabber for Mac configuration files. These XML files are loaded from the TFTP server and can contain additional configuration information such as application dial rules and directory look up rules.

The high-level launch sequence for WebEx cloud deployment is as follows:

1. The client securely authenticates to the WebEx Messenger service.
2. The client retrieves profile details and User Contact list, WebEx Meeting Center URL, server information (such as Unified CM servers and voicemail servers), and pilot number.

Contact Sources

Cisco Jabber for Mac supports LDAP directory integration. With Cisco IM and Presence, Jabber for Mac supports the following directory server types: Microsoft Active Directory, iPlanet, Sun ONE, and OpenLDAP. When one of these directory server types is selected, the presence server populates the LDAP attribute map with Cisco Jabber user fields and LDAP user fields. These default mappings can be modified to support the attribute mappings of other LDAP directory servers. For Cisco Jabber for Mac clients using the Cisco IM and Presence Service, you must configure the LDAP server and attribute mappings for your environment (**Application > Legacy Clients > Settings**).

Jabber for Mac does *not* support Unified CM UDS contact searches.

Jabber for Mac supports desktop sharing using WebEx Desktop Share.

For more information on the configuration options and administration of a Jabber for Mac client, refer to the *Cisco Jabber for Mac Installation and Configuration Guide*, available at

http://www.cisco.com/en/US/products/ps11764/prod_maintenance_guides_list.html

Also refer to the Jabber for Mac Release Notes, available at

http://www.cisco.com/en/US/products/ps11764/prod_release_notes_list.html

For specific details about Jabber for Mac client features, refer to the Jabber for Mac data sheet, available at

http://www.cisco.com/en/US/products/ps11764/products_data_sheets_list.html

Cisco Jabber Instant Messaging and Presence Deployments

Instant messaging and presence services for Jabber clients can be provided through the Cisco Jabber XMPP interface. Cisco offers instant messaging (IM) and presence services with the following products:

- Cisco IM and Presence, page 21-19
- Cisco WebEx Messenger Service, page 21-22

The following sections discuss the architecture and design considerations for Cisco IM and Presence and WebEx Messenger service.

Cisco IM and Presence

The main component of the Cisco IM and Presence solution is the Cisco IM and Presence Service, which supports SIP/SIMPLE and Extensible Messaging and Presence Protocol (XMPP) for collecting information regarding a user's availability status and communications capabilities. The user's availability status indicates whether or not the user is actively using a particular communications device. The user's communications capabilities indicate the types of communications that user is capable of using, such as

video conferencing, web collaboration, instant messaging, or basic audio. The architecture of Cisco IM and Presence and the design guidance for deployments are discussed in detail in the chapter on Cisco IM and Presence, page 20-1.

The following sections discuss aspects of Cisco IM and Presence design that are relevant to Jabber clients using a Cisco IM and Presence cluster.

Client Scalability

The Cisco IM and Presence Service hardware deployment determines the number of users a cluster can support. Cisco Jabber client deployments 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**.

High Availability for Jabber Clients

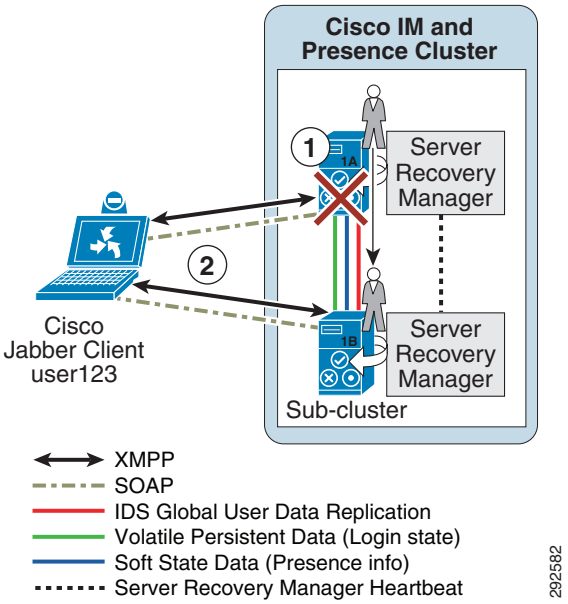
All users in the Cisco IM and Presence cluster must be assigned to a server prior to any exchange of information. By default, Cisco IM and Presence allows for automatic user assignment that is equally balanced across all servers in the cluster. If desired, the administrator can control where users are 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 Jabber clients can be provisioned with a basic deployment (not high availability), a highly available deployment for automatic redundancy, and an IM and presence only deployment. In a Cisco IM and 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 Jabber client high availability is supported only within a Cisco IM and Presence subcluster.

As illustrated in Figure 21-5, the server recovery manager monitors the various services on Cisco IM and Presence to determine if a service has failed and then 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. The Cisco Jabber client determines that 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 21-5 Cisco Jabber Client XMPP Failover



Third-Party XMPP Clients Connecting to Cisco IM and Presence

Cisco IM and Presence supports standards-based XMPP to enable third-party XMPP client applications to integrate with IM and Presence for availability and instant messaging (IM) services. Third-party XMPP clients must comply with the XMPP standard as outlined in the Cisco Software Development Kit (SDK). A list of XMPP software clients is available at

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

To allow users of the XMPP client applications to search and add contacts from an LDAP directory, configure the LDAP settings for XMPP clients on IM and Presence. The domain name on the XMPP client, specifically the XMPP connection attempt domain name, must match the domain on IM and Presence. You must enable DNS SRV in your deployment when you integrate XMPP clients with IM and Presence. The XMPP client performs a DNS SRV query to find an XMPP server (IM and Presence) to communicate with, and then performs a record lookup of the XMPP server to get the IP address.

For additional information on enabling third-party XMPP clients to connect to Cisco IM and Presence, refer to the latest version of the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*, available at

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

Cisco WebEx Messenger Service

Cisco WebEx Messenger service is a multi-tenant software-as-a-service (SaaS) platform for synchronous and asynchronous collaboration. The WebEx Messenger 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 information on the Cisco WebEx Messenger service, refer to the documentation available at

http://www.cisco.com/en/US/products/ps10528/index.html

For more information on the Cisco WebEx Cloud, refer to the documentation available at

http://www.cisco.com/en/US/solutions/ns1007/collaboration_cloud.html

Logging Instant Messages

Cisco WebEx Messenger service 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 Messenger service that can be enabled by means of policy through the Org Admin tool. The end-user can set logging specifics, whether to enable or disable logging, and how long the logs are kept.

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 Messenger service, 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.

Capacity Planning for Cisco WebEx Messenger Service

A single end-user requires only a 56 kbps dial-up Internet connection to be able to log in to WebEx Messenger service 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, desktop sharing, and screen capture.

Cisco Webex Messenger service deployment network requirements are available at

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

High Availability for Cisco WebEx Messenger Service

WebEx Messenger is a Software-as-a-Service (SaaS) application. The end-user device must be connected to the Internet for the end user to log in to the IM client. 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 the WebEx Messenger service. Cisco WebEx Messenger service IM clients can be deployed in a highly available redundant topology.

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 Messenger service, for a seamless user experience. Deployment of the Cisco WebEx Messenger service Software-as-a-Service architecture involves various network and desktop requirements. For additional details, see the chapter on Cisco IM and Presence, page 20-1.

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/solutions/ns1007/collaboration_cloud.html

Third-Party XMPP Clients Connecting to Cisco WebEx Messenger Service

Although Cisco does not officially support any other XMPP clients to connect to the Cisco WebEx Messenger service, the nature of the XMPP protocol is to allow end users to connect to presence clouds with various XMPP clients. Users can connect with third-party software by using their WebEx Messenger service 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 Messenger service XMPP IM clients to authenticate to your WebEx Messenger service domain(s), DNS SRV records must be updated. The specific DNS SRV entry can be found in Cisco WebEx administration, under Configuration and IM Federation.

The use of non-Messenger service XMPP clients in Cisco WebEx administration, under Configuration and XMPP IM Clients, must be explicitly allowed.

Other Resources and Documentation

For additional information on WebEx, refer to the Cisco WebEx administrator's guide available at

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

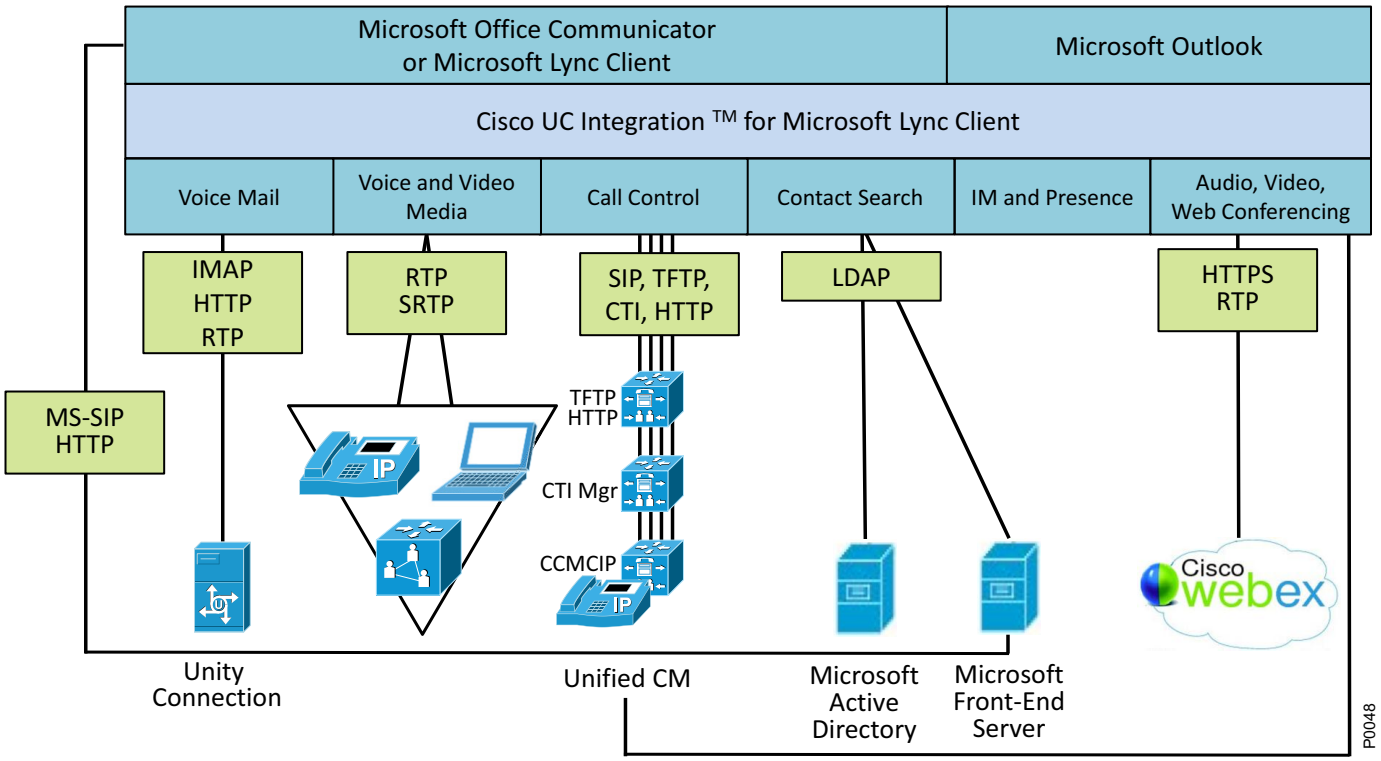
Cisco UC Integration™ for Microsoft Lync Architecture

Cisco UC Integration™ for Microsoft Lync clients support a variation of the on-premises deployment models, where IM and presence services are provided by Microsoft Applications instead of Cisco IM and Presence.

Cisco UC Integration™ for Microsoft Lync allows for tightly integrated Cisco Unified Communications services for Microsoft Lync by integrating with underlying Unified Communications services. 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, while delivering a consistent user experience.

The solution architecture for a Cisco UC Integration™ for Microsoft Lync deployment, shown in Figure 21-6, 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 Communications services for PC audio or deskphone control, and Microsoft Lync.

Figure 21-6 Cisco UC Integration™ for Microsoft Lync Architecture



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.

Note With Cisco UC Integration™ for Microsoft Lync, instant messaging and presence services are provided by Microsoft rather than by Cisco Unified Communications services.

Deploying Cisco UC Integration™ for Microsoft Lync

When deploying Cisco UC Integration™ for Microsoft Lync, observe the guidelines presented in this section. Cisco Unified Communications Manager provides the call control, while Microsoft Lync provides the instant messaging and presence.

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 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™ for Microsoft Lync configuration policy can be created by the administrator for the registry configuration settings (TFTP servers, CTI servers, CCMCIP servers, voicemail, and LDAP servers).

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 you deploy 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 an 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

Capacity Planning for Cisco UC Integration™ for Microsoft Lync

Cisco UC Integration™ for Microsoft Lync uses Unified CM CTIManager for click-to-dial applications, as well as deskphone control mode by integrating with underlying Cisco Unified Communications services. Therefore, observe the CTI limits as defined in the chapter on Call Processing, page 9-1. When Cisco UC Integration™ for Microsoft Lync is operating in softphone (audio on computer) mode, the client 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

The Cisco UC Integration™ for Microsoft Lync Client provides primary and secondary servers for each of the configuration components: TFTP server, CTIManager, CCMCIP server, voicemail server, and LDAP server. When operating in softphone (audio on computer) mode, the client 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 is controlling a Cisco

Unified IP Phone using CTI, and it supports configuration of a primary and secondary CTIManager. For additional details on CTI deployments, refer to the chapter on Call Processing, page 9-1. The client 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 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 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, CTIManager, 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 UC Integration™ for IBM Sametime Architecture

Cisco UC Integration™ for IBM Sametime clients supports a variation of the on-premises deployment models, where IM and presence services are provided by IBM Sametime instead of Cisco IM and Presence.

The integration takes the form of an Eclipse plug-in that provides a standardized way (within the IBM IM and presence architecture) of enhancing the Sametime client's abilities above and beyond its own native feature set.

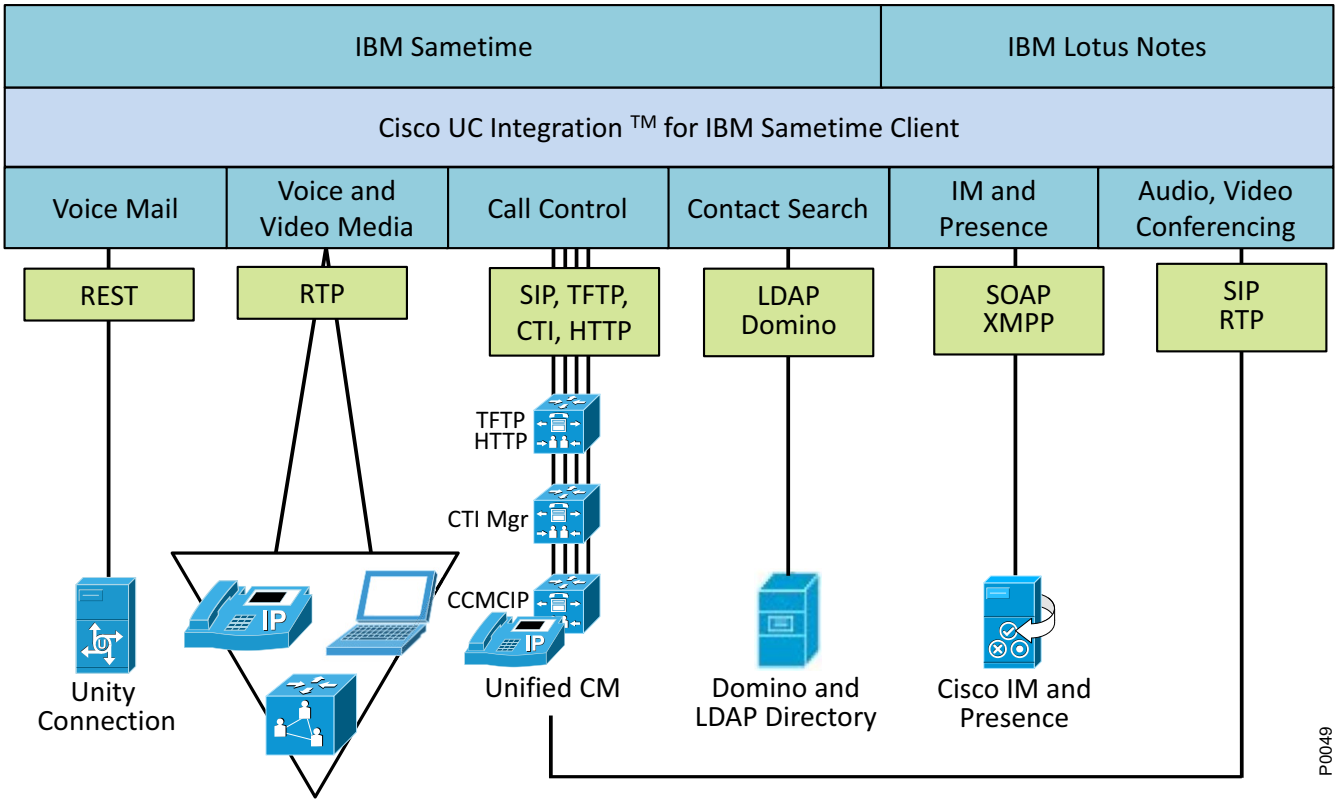
Cisco UC Integration™ for IBM Sametime provides instant access to Cisco Unified Communications capabilities directly from IBM Sametime. The integration enhances productivity by adding Cisco presence, softphone audio, and HD video capabilities for Sametime IM and presence users. It also includes Cisco desk phone control, integrated voicemail, and the conversation history. The integration allows access to the same Cisco Unified Communications services for both standalone and Notes-embedded Sametime clients.

The solution architecture for a Cisco UC Integration™ for IBM Sametime deployment, shown in Figure 21-7, includes:

- Cisco Unified Communications Manager for audio and video services
- Cisco Unified Communications Manager IM and Presence for injection of phone status into Sametime

- Cisco Unity Connection for visual voicemail capabilities
- IBM Lotus Sametime for desktop presence and instant messaging services
- LDAP or native Domino Directory for user account information
- Cisco Unified Communications services for PC audio/video and desk phone control

Figure 21-7 Cisco UC Integration™ for IBM Sametime Architecture



With a deployment of Cisco UC Integration™ for IBM Sametime, the client utilizes user information from the Sametime server's directory. The LDAP lookup capability of the plug-in is used to perform the following tasks:

- Deliver additional click-to-call phone numbers above and beyond the single number provided by the native Sametime Business Card service
- Provide a number to Sametime Contact resolution service for incoming CTI notifications, during softphone calls, for voice messages and for call history
- Look up a predetermined attribute from the Sametime directory that matches any given person's Unified Communications Manager IM and Presence username

Note With Cisco UC Integration™ for IBM Sametime, instant messaging and presence services are provided by IBM rather than by Cisco Unified Communications services.

Deploying Cisco UC Integration™ for IBM Sametime

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

Configuration Settings

Cisco UC Integration™ for IBM Sametime is provisioned using a configuration tool that is provided by Cisco. The tool is intended to allow a system administrator to configure the necessary system parameters for Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence, Cisco Unity Connection, and the Sametime (LDAP/Domino) directory to enable the correct plug-in operation. The Cisco UC Integration™ plug-in cannot be deployed without first generating its configuration. If the system's Sametime credentials match those of the Cisco platforms, then the tool can be used to program the plug-in to use the Sametime credentials to automatically log into the Cisco servers. However, if the logon credentials between Sametime and the Cisco UC applications are different, then users will need to manage their Cisco username and password locally within the client after the Cisco UC Integration™ plug-in is provisioned. After the tool's configuration is saved, it will be uploaded automatically into the plug-in's update site folder. The Cisco UC Integration™ plug-in can be pushed automatically or pulled manually into the Sametime client. The specific IBM provisioning mechanisms used for automatic deployment will vary depending on whether the Sametime client is implemented in standalone mode or as an integrated Lotus Notes sidebar.

Capacity Planning for Cisco UC Integration™ for IBM Sametime

Cisco UC Integration™ for IBM uses Unified CM CTI Manager for click-to-dial applications, as well as deskphone control mode with the underlying Cisco Unified Communications services Therefore, observe the CTI limits as defined in the chapter on Call Processing, page 9-1. When Cisco UC Integration™ for IBM is operating in a softphone (audio/video on computer) mode, the client 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 IBM Sametime

Cisco UC Integration™ for IBM Sametime provides primary and secondary servers for the following configuration components: TFTP server, CTIManager, CCMCIP server, and the Cisco IM and Presence. Cisco Unity Connection and the Directory configuration support only a single server entry. When operating in softphone (audio/video on computer) mode, the Cisco UC Integration™ for IBM 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 desk phone mode, the Cisco UC Integration™ for IBM is controlling a Cisco Unified IP Phone using CTI, and it supports configuration of a primary and secondary CTIManager. For additional details on CTI deployments, refer to the chapter on Call Processing, page 9-1.

Design Considerations for Cisco UC Integration™ for IBM Sametime

Observe the following design considerations when deploying Cisco UC Integration™ for IBM Sametime:

- Identify which type of directory the Sametime Server uses because it might be different than the directory used for Cisco Unified CM synchronization. Identify the directory attribute values that are used for the Cisco username and the Sametime username. Identify if the Cisco and IBM passwords are synchronized between the two platforms. If they are not, end users will have to manage their Cisco credentials manually within the Cisco UC Integration™ for IBM Sametime client. If the passwords are synchronized, the Sametime credentials can be used to log on automatically to the Cisco Unified Communications platforms.
- Based upon the above username comparison, carefully plan the presence integration design approach, which will normally utilize a Sametime business card attribute or a Sametime directory lookup, to be able to map to a Sametime contact's phone status.
- Gather all the other system parameters needed for the Cisco UC Integration™ for IBM Sametime configuration tool, and program it using the Cisco documentation.
- Ensure that Cisco Unified Communications Manager, Cisco IM and Presence, and Cisco Unity Connection are also appropriately configured for the Cisco UC Integration™ for IBM.
- Identify if Sametime has been deployed as a standalone client or whether it is deployed as an integrated sidebar in Lotus Notes.
- If Sametime is deployed as a standalone client, then request that the IBM administrator use the Sametime Server's HTTP-based plug-in provisioning tools to distribute the Cisco UC Integration™ for IBM Sametime plug-in automatically to the Sametime client population.
- If Sametime is deployed as an integrated notes sidebar, then work with the IBM administrator to create a "Notes Widget" for the Cisco UC Integration™ for IBM Sametime plug-in and then request that the IBM administrator make use of Domino's desktop settings and policy tools to provision the Cisco UC Integration™ for IBM Sametime automatically into the Notes clients.

Cisco Virtualization Experience Media Engine

The Cisco Virtualization Experience Media Engine (VXME) provides an integral collaboration software component by extending the Cisco Jabber collaboration experience to a Virtual Desktop Infrastructure (VDI) environment. VXME is a software package installed on a local platform (a thin client), and it allows users to enhance their VDI sessions to include locally terminated voice and video real-time communications, bypassing real-time media routing through the virtual desktop while allowing for a fully integrated user experience. The hosted virtual desktop is supported with Citrix XenDesktop, Citrix XenApp Published Desktop, or VMware View, through locally installed Citrix Receiver or VMware View Client, respectively. Regardless of the host VDI platform, a user has a consistent voice, video, and virtual desktop experience using Cisco Jabber on the virtual desktop with fully integrated accessories enabled for Unified Communications and seamless integration with VXME.

For more information on Cisco Virtualization Experience Media Engine (VXME), refer to the data sheet and product documentation at

http://www.cisco.com/en/US/products/ps12862/tsd_products_support_series_home.html

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

The Cisco VXME 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. A thin client can operate as VDI-only using Jabber on the Virtual desktop for deskphone control mode of a Cisco Unified IP Phone, or the thin client can operate in a fully integrated voice, video, virtual desktop deployment using VXME.

No additional configuration is required for Cisco Virtualization Experience Media Engine, if the network is set up for Medianet or Dual VLAN. If the network is not set up for either, Cisco VXME will be placed in the data VLAN (given that display protocol VDI interaction consumes as much bandwidth as available). Likewise, QoS traffic marking is not performed, and traffic traverses the network as best-effort. 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 Media Engine

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

A Cisco Virtualization Experience Media Engine 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 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 UC Integration™ for Microsoft Lync (see High Availability for Cisco UC Integration™ for Microsoft Lync, page 21-25). The endpoint registered to Unified CM can be either a Cisco Unified IP Phone when using thin clients or Cisco VXME. 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 Cisco VXME.

Design Considerations for Cisco Virtualization Experience Media Engine

The following design considerations apply to the Cisco Virtualization Experience Media Engine:

- CTI guidelines must be observed when deploying Cisco Virtualization Experience Media Engine in a fully integrated voice, video, and virtual desktop environment.
- With Cisco VXME, QoS is handled by Medianet or Dual VLAN, if configured. If not configured, QoS is best-effort and the thin client 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

Cisco IP Communicator

Cisco IP Communicator is a Microsoft Windows-based application that endows computers with the functionality of IP phones. This application enables high-quality voice calls on the road, in the office, or from wherever users can access the corporate network. It is a solution for remote users and telecommuters when IM and Presence capabilities are not required.

Because Cisco IP Communicator is a standalone device that supports both SCCP and SIP, the design guidelines for IP phones in the various Collaboration deployment models still hold true for Cisco IP Communicator. See the chapter on Collaboration Deployment Models, page 10-1, for details.

When deploying Cisco IP Communicator, it is important to deploy QoS too. If QoS is not deployed, packet drops and excessive delay and jitter can occur, leading to impairments of the telephony services. When media packets are subjected to drops, delay, and jitter, the quality of audio is compromised. When signaling packets are subjected to the same conditions, users can experience unresponsiveness to user input, continued ringing upon answer, call termination, and other undesirable behaviors on the client. For more information on implementing QoS, refer to the chapter on Network Infrastructure, page 3-1.

For more information about Cisco IP Communicator, refer to the data sheets and product documentation at

http://www.cisco.com/en/US/products/sw/voicesw/ps5475/index.html