

CHAPTER 4

Unified Contact Center Enterprise Desktop

Last revised on: October 29, 2008

The Cisco Unified Contact Center Enterprise (CCE) solution delivers a comprehensive set of desktop applications and services. This chapter covers the following major topics related to those desktop applications and services:

- [Desktop Components, page 4-1](#)
- [Desktop Solutions, page 4-6](#)
- [Deployment Considerations, page 4-16](#)
- [References to Additional Desktop Information, page 4-47](#)

What's New in This Chapter

[Table 4-1](#) lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

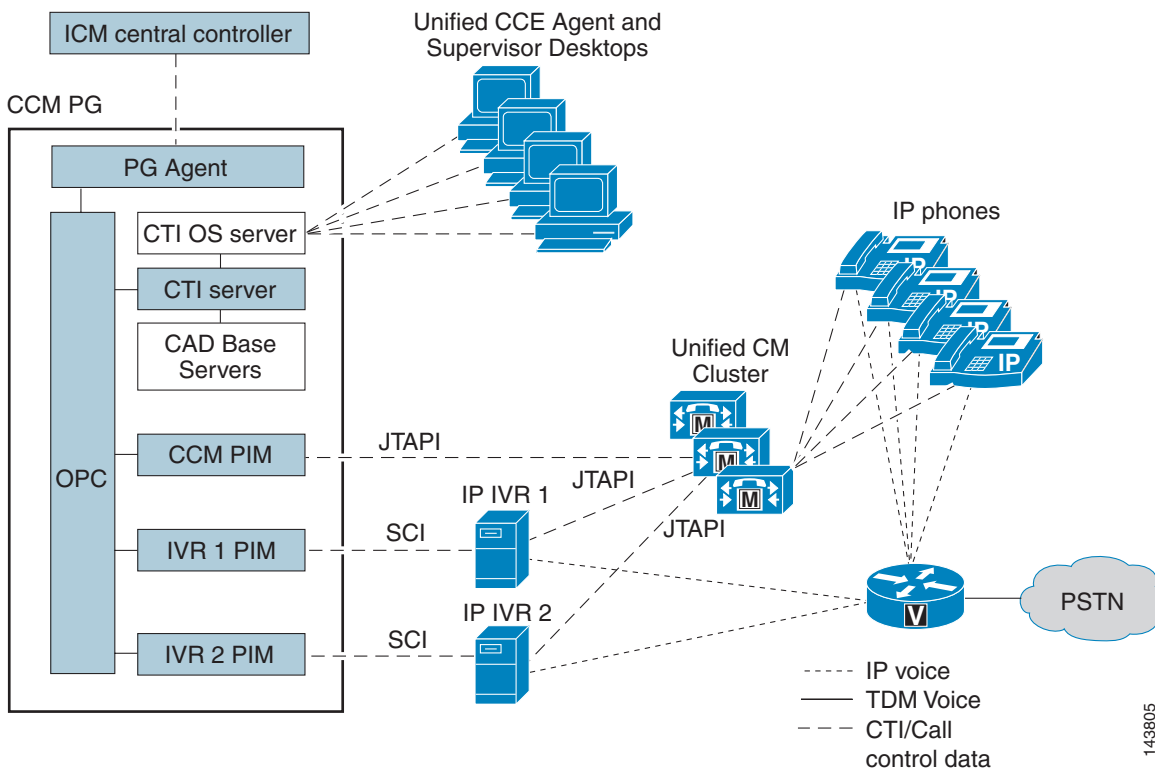
Table 4-1 *New or Changed Information Since the Previous Release of This Document*

New or Revised Topic	Described in:
Remote Silent Monitoring (RSM)	Cisco Remote Silent Monitoring, page 4-25

Desktop Components

The desktop applications themselves typically run on Agent, Supervisor, or Admin workstations. Services supporting the desktop applications typically run on the CCE Peripheral Gateway (PG) server. Within the CCE deployment, there may be one or more PG systems, and for each PG there is one set of active desktop services, which includes the CTI Object Server (CTI OS) and the Cisco Agent Desktop Base Services (for Cisco Agent Desktop deployments). [Figure 4-1](#) depicts the components within a Unified CCE deployment that support the various desktop applications.

Figure 4-1 Generic Unified CCE Desktop Components



In the Unified CCE solution, the Peripheral Gateway may be deployed in either a simplex or duplex configuration. Duplex configurations provide redundant desktop services for failover recovery support. These systems are typically identified as the primary, or A-side, and the backup, or B-side. For production deployments, a duplex configuration is required.

CTI Object Server

The CTI Object Server (CTI OS) is a high-performance, scalable, fault-tolerant, server-based solution for deploying CTI applications. CTI OS is a required component for CTI Toolkit desktop and Cisco Agent Desktop (CAD) solutions and is Cisco's latest version of the CTI implementation.

Communications from the desktop applications, such as agent state change requests and call control, are passed to the CTI OS server running on the Cisco Unified Peripheral Gateway. CTI OS serves as a single point of integration for CAD desktops, CTI Toolkit desktops, and third-party applications such as Customer Relationship Management (CRM) systems, data mining, and workflow solutions.

The CTI Object Server connects to CTI Server via TCP/IP and forwards call control and agent requests to CTI Server, which in turn forwards to the Open Peripheral Controller (OPC). From there, depending on the type of request, OPC will forward to either the CCM Peripheral Interface Manager (PIM) or to the CCE Central Controller.

Requests initiated from the desktop application that affect the agent state are sent to the CCE Central Controller, while requests initiated from the desktop application that affect call control are sent to the CCM PIM. The Unified CCE Central Controller monitors the agent state so that it knows when it can and cannot route calls to that agent and can report on that agent's activities.

Call control flows from the agent desktop application to Cisco Unified Communications Manager (Unified CM). Unified CM then performs the requested call or device control. The desktop services located on the PG keep the agent desktop application synchronized with the agent's IP phone state.

CTI Toolkit desktop configuration and behavior information is also managed at the CTI OS server, simplifying customization, updates, and maintenance, and supporting remote management.

CTI Object Server Services

- Desktop Security — Supports secure socket connections between the CTI Object Server on the PG and the agent, supervisor, or administrator desktop PC. Any CTI application built using the CTI Toolkit C++ Client Interface Library (CIL) Software Development Kit (SDK) can utilize the desktop security feature.



Note Desktop Security is not currently available in the .NET and Java CILs.

- Quality of Service (QoS) — Supports packet prioritization with the network for desktop call control messages.



Note QoS is not currently available in the .NET and Java CILs.

- Failover Recovery — Supports automatic agent login upon failover.
- Chat — Supports message passing and the text chat feature between agents and supervisors.
- Silent Monitoring — Supports VoIP monitoring of active calls. The CTI Object Server communicates with the Silent Monitor Service (SMS) to start/stop the VoIP packet stream forwarding.

The CTI Object Server is typically installed in duplex mode, with two CTI OS servers running in parallel for redundancy, one on PG side-A and one on PG side-B. The CTI Toolkit Desktop applications randomly connect to either server and automatically fail-over to the alternate server if the connection to the original CTI OS server fails. CTI OS can also run in simplex mode with all clients connecting to a single server, but Cisco does not recommend this configuration.

Agent capacity sizing for the PG is covered in the chapter on [Sizing Unified CCE Components and Servers, page 10-1](#).



Note

The CTI OS server interfaces to any desktop application built using the CTI Desktop Toolkit Software Development Kit. Cisco Agent Desktop (Release 6.0 and later) is built upon the C++ CIL Toolkit SDK and therefore does interface to CTI OS. Beginning with Cisco Agent Desktop Release 7.0(0), a single CTI OS server can support the use of both CAD and CTI Toolkit desktops concurrently. However, the agents and supervisors cannot be mixed between these desktop types.

CAD Base Services

Cisco Agent Desktop (CAD) is a software suite that provides a feature-rich packaged solution. CAD consists of user applications and the CAD Base Services, which can run co-resident on the Peripheral Gateway within a Unified CCE deployment and are required for CAD deployments only. The CAD Base Services provide redundancy and warm standby capabilities.

CAD Base Services

- Cisco Chat Service — Supports message passing and the text chat feature.
- Cisco Enterprise Service — Communicates with the Unified CCE components to provide call data to the user applications.
- Cisco Browser and IP Phone Agent Service — Provides services for CAD-BE and IPPA agent applications.
- Cisco Synchronization Service — Synchronizes the Unified CCE and CAD-specific configuration data.
- Cisco LDAP Monitor Service — Manages the storage and retrieval of CAD configuration data.
- Cisco Recording and Statistics Service — Manages the storage and retrieval of call recording, agent call, and agent state change data used in reports.
- Cisco Licensing and Resource Manager Service — Manages user licenses and controls failover behavior.
- Cisco Recording and Playback Service — Provides the call recording and playback feature.
- Cisco VoIP Monitor Service — Provides the voice streams for the call recording and silent monitoring features if server-based monitoring is used.

For more information on CAD, refer to the product documentation available at

http://www.cisco.com/en/US/products/sw/custcosw/ps427/tsd_products_support_series_home.html

Cisco Unified Contact Center Enterprise (CCE) supports a variety of desktop application choices for agents and supervisors, as described in the following sections.

Agent Desktops

An agent desktop application is a required component of a Unified CCE deployment. The contact center agent uses this application to perform agent state control (login, logout, ready, not ready, and wrap-up) and call control (answer, release, hold, retrieve, make call, transfer, and conference). In addition to these required features, the application can provide enhanced features that are useful in a contact center environment.

There are seven primary types of Unified CCE agent desktop applications available, as listed below.

Agent Desktop Applications Offered by Cisco

- Cisco Agent Desktop (CAD) — A packaged agent desktop solution supporting an embedded browser and scripted workflow automation.
- CTI Desktop Toolkit — A development toolkit that provides agent desktop applications and that supports full customization and integration with other applications, customer databases, and Customer Relationship Management (CRM) applications.
- CTI Driver for Siebel — A CTI driver for the Siebel Communication Server.
- Cisco Unified IP Phone Agent — An agent desktop solution provided through the Cisco Unified IP Phone display.
- Cisco Agent Desktop Browser Edition (CAD-BE) — A browser-based agent application that supports many of the features of the CAD windows-based agent application with lower platform requirements.

Agent Desktop Applications Offered Through Cisco Partners

- Partner Agent Desktops — Custom agent desktop applications are available through Cisco Technology Partners. These applications are based on the CTI Desktop Toolkit and are not discussed individually in this document.
- Prepackaged CRM integrations — CRM integrations are available through Cisco Unified CRM Technology Partners. They are based on the CTI Desktop Toolkit and are not discussed individually in this document.

Agent Mobility

Within the Unified CCE deployment, the agent desktop application is not statically associated with any specific agent or IP phone extension. Agents and phone extensions (device targets) are configured within the Unified CCE configuration and associated with a specific Unified CM cluster.

When logging in from an agent desktop application, the agent is presented with a dialog box that prompts for agent ID or login name, password, and the phone extension to be used for this session. At this time the agent ID, phone extension, and agent desktop IP address are dynamically associated. The association is released when the agent logs out.

This mechanism enables an agent to work (or *hot-desk*) at any workstation. It also enables agents to take their laptops to any Cisco Unified IP Phone and log in from that device (assuming the phone has been configured in the Unified ICM and in Unified CM to be used in the Unified CCE deployment). Agents can also log in to other phones using the Cisco Extension Mobility feature. For more information on Extension Mobility, refer to the Extension Mobility section of the *Cisco Unified Communications Manager Features and Services Guide*, available at

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

Supervisor Desktops

In addition to the agent desktop application, a supervisor desktop application is also available. The contact center supervisor uses this application to monitor agent state for members within their team. The supervisor desktop also enables Silent Monitoring of agents during active calls.

The available types of Unified CCE supervisor desktop applications are listed below.

Supervisor Desktop Applications Offered by Cisco

- Cisco Supervisor Desktop (CSD) — A packaged supervisor desktop solution.
- CTI Desktop Toolkit — A development toolkit that provides a supervisor desktop application and supports customization and integration with other applications, customer databases, and Customer Relationship Management (CRM) applications.

Supervisor Desktop Applications Offered Through Cisco Partners

- Prepackaged CRM integrations — CRM integrations are available through Cisco Unified CRM Technology Partners. They are based on the CTI Desktop Toolkit and are not discussed individually in this document.

Desktop Solutions

Depending on the requirements of the contact center, a particular type of desktop might be better suited to the solution. Table 4-2 contains an abbreviated list of the functionality available in the various desktop applications. It is intended to provide a starting point to determine the desktop that best meets specific solution requirements. Further information is available for each of the Cisco desktops in the sections below and in their respective product specifications at <http://www.cisco.com>.

Table 4-2 Features Supported by Cisco Desktop Solutions

Desktop Functionality	Cisco Agent Desktop	Cisco Agent Desktop Browser Edition	CTI Desktop Toolkit	CTI Driver for Siebel	IP Phone Agent
Turn-key desktop applications	Yes	Yes	Yes	Yes	Yes
Custom desktop development using C++, .NET, and Java			Yes		
Desktop Security	Yes		Yes		
Workflow Automation	Yes	Yes			
Mobile (Remote) Agents	Yes	Yes	Yes		
Siebel Integration				Yes	
Silent Monitoring	Yes	Yes	Yes		Yes
Integrated Recording Capability	Yes	Yes			Yes
Monitor Mode Applications			Yes		
Outbound Calls	Yes		Yes		
Microsoft Terminal Services Support	Yes		Yes		
Citrix Presentation Server Support	Yes		Yes		
Agent Mobility	Yes	Yes	Yes		Yes
IP Phone Solution (no soft desktop)					Yes
Specific capability or integration not offered by Cisco					

Cisco Agent Desktop Solution

The Cisco Agent Desktop (CAD) solution is a suite of packaged desktop applications and services. The CAD solution offers a rich set of features for the contact center environment, including:

- Lightweight Agent Desktop

Cisco Agent Desktop Browser Edition (CAD-BE) is a java-based agent application that runs in a browser window on the agent's desktop. It offers a similar look-and-feel as the Cisco Agent Desktop application, with many of the same features. CAD-BE can run in any supported browser on any supported operating system.

- **Workflow Automation**

The workflow automation feature allows an administrator to customize the agent environment and how the user applications interact with that environment. Workflow automation enables data processing actions to be scheduled based on telephony events (for example, popping data into a third-party application on the answer event and sending email on the dropped event). Workflow automation interfaces with applications written for Microsoft Windows browsers and terminal emulators. Some customizations can be as simple as using keystroke macros for screen pops.
- **On-Demand Recording**

The supervisor (and, if enabled, the agent) can record a customer phone call for later review by a supervisor.
- **Unified IP Phone Agent**

With this service, agents using Cisco Unified IP Phones with XML services can log in and use their phone to perform most of the agent functions found in an agent desktop application.
- **Collaboration**

A supervisor can text-chat directly with agents or agent teams. Agents can text-chat with supervisors or other team members (if enabled). The supervisor can push web pages to agents and send team messages to agent desktops. Interactive collaboration enables the contact center to communicate better, increase productivity, improve customer responsiveness, and coach or train agents.
- **Task Automation**

Routine agent tasks, such as email, conference to knowledge workers, launching other applications, high-priority chat, and so forth, can be configured as task buttons on the agent's toolbar to reduce call duration and improve customer responsiveness.
- **Silent Monitoring**

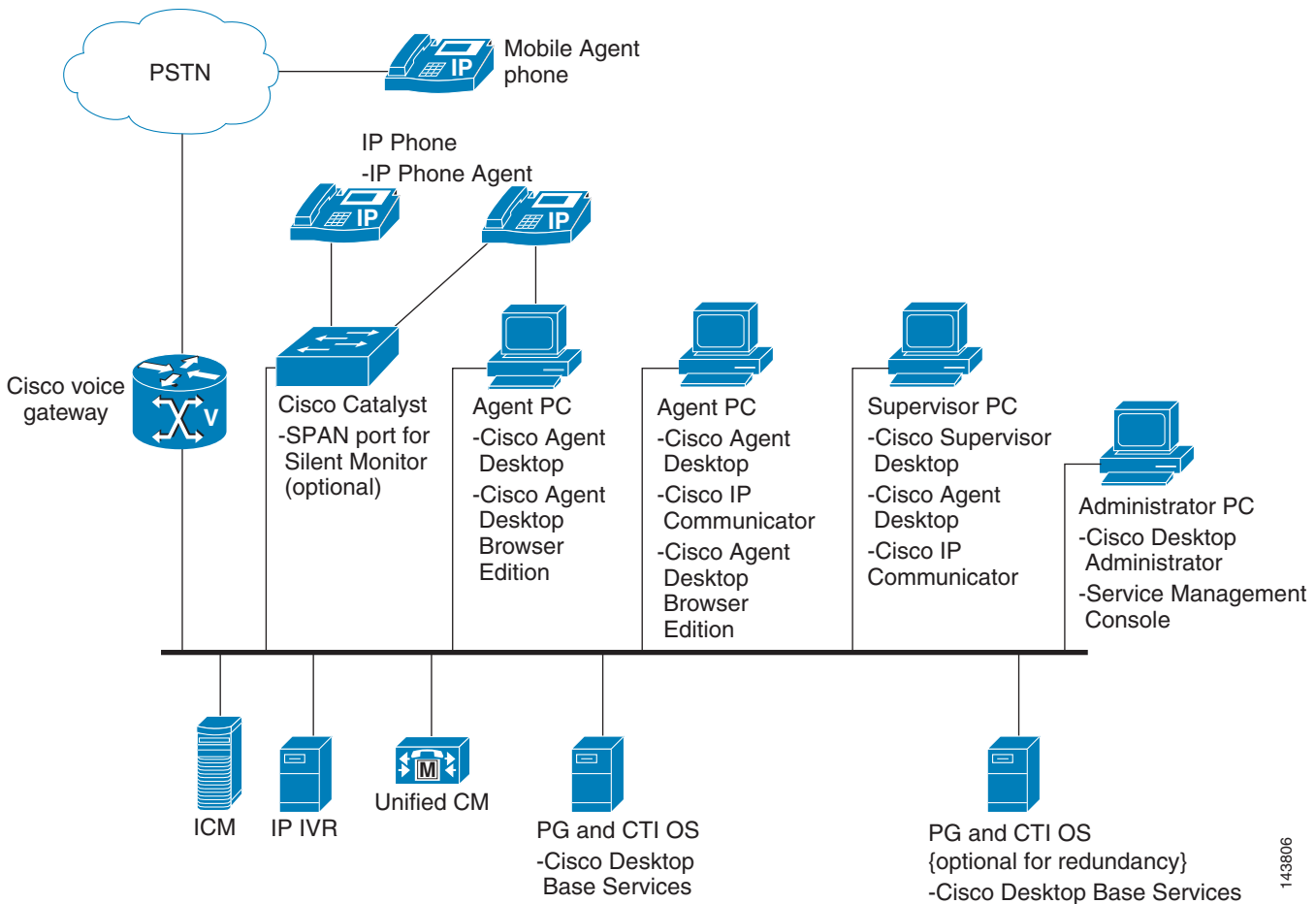
Supervisors can initiate a silent monitor session with an agent within their team.

CAD User Applications

The CAD user applications include the following applications for call center agents, supervisors, and administrators. There are three types of agent applications included in the CAD suite. (See [Figure 4-2](#).)

- **Cisco Agent Desktop (CAD)** — A Windows Agent application
- **Cisco Agent Desktop Browser Edition (CAD-BE)** — A Java-based agent application
- **Cisco IP Phone Agent (IPPA)** — An IP phone service agent application
- **Cisco Supervisor Desktop (CSD)** — A Windows supervisor application
- **Cisco Desktop Administrator (CDA)** — A Windows application that allows configuration of the agent and supervisor applications
- **Cisco Services Management Console (SMC)** — A Java-based applet that allows administrators to monitor the health of the CAD base services

Figure 4-2 Cisco Agent Desktop System Configuration and Components



143806

CAD Application Features

Table 4-3 compares some of the more important features in CAD that can be used to help select the agent application that would work best for a particular deployment.

Table 4-3 Features Supported by CAD User Applications

Feature	CAD	CAD-BE	IPPA
Call Control	Yes	Yes	N/A ¹
VPN/Remote Agent Support	Yes	Yes	Yes
Support for Cisco IP Communicator	Yes	Yes	N/A
Mobile agent support	Yes	Yes	N/A
Outbound Option	Yes	No	N/A
Integrated browser	Yes	Yes	N/A
Call Event Workflow automation	Yes	Yes	N/A
Citrix/Terminal Services support	Yes	N/A	N/A

Table 4-3 Features Supported by CAD User Applications (continued)

Feature	CAD	CAD-BE	IPPA
Agent state workflow automation	Yes	N/A	N/A
Desktop monitoring	Yes	N/A	N/A

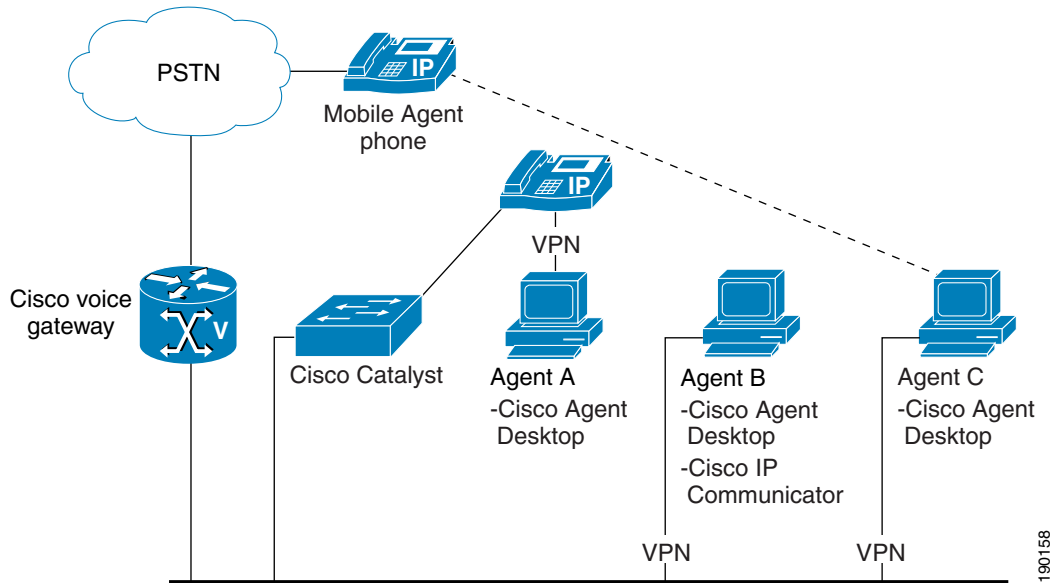
1. Call control actions are performed by using the IP phone's call control softkeys.

For more information on CAD agent applications, refer to the appropriate user guide, available at http://www.cisco.com/en/US/products/sw/custcosw/ps427/tsd_products_support_series_home.html

Cisco Agent Desktop

Cisco Agent Desktop is a Microsoft Windows application that runs on an agent's PC and works with either a hardware IP phone or the Cisco IP Communicator software phone. Cisco Agent Desktop interfaces with the CTI OS service for call control and agent state change events. For all other features, it communicates directly with the CAD services. Cisco Agent Desktop includes support for desktop monitoring, which captures the voice stream on the agent's IP phone to support the silent monitoring and call recording features. Figure 4-3 shows the types of supported CAD agents.

Figure 4-3 CAD Agents and Components



Agent A in Figure 4-3 shows a CAD agent that uses a hardware IP phone. The IP phone is shown directly connected to the agent's PC via a network cable, which is the configuration required for desktop monitoring. The VPN label designates that CAD supports a VPN connection between the agent's PC and the call center network.

Agent B shows a CAD agent that uses the Cisco IP Communicator softphone. This configuration also supports a VPN connection to the call center network. It is the most common configuration for remote agents.

Agent C shows CAD being used with the new Mobile Agent feature. Mobile agents are agents whose phones are not directly controlled by Unified CM. The agent may use their home phone or cell phone as their agent device. In this case, the agent provides a CTI port to associate with their remote phone when they log in. ACD calls for the logged-in agent are sent to the CTI port, which causes the call to appear at the mobile agent's device. There is a logical relationship (shown as a dashed line) between the CAD agent and the mobile phone. The VPN label indicates that CAD will support a VPN connection to the call center network. CAD mobile agents cannot be silently monitored or recorded.

For more information on Cisco Agent Desktop, refer to the *Cisco Agent Desktop User Guide*, available at http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_user_guide_list.html

Cisco Agent Desktop Browser Edition

Cisco Agent Desktop Browser Edition (CAD-BE) is a java applet that runs in Microsoft Internet Explorer on the Agent's PC. CAD-BE is related to the IP Phone Agent in that it interfaces to the IP Phone Agent Service for all of its agent state and call control. However, whereas the IPPA service is limited in features due to the size and graphical features of the IP phone's display, CAD-BE can use the abilities and features of any java applet. This allows CAD-BE to have a small footprint on the agent's desktop and yet offer many features that are also found in the CAD agent Windows application.

CAD-BE Limitations and Features

CAD-BE does not support all the features of CAD. Some of its limitations are related to the limitations of the IPPA application. Some of the main features include:

- Support for both hardware and software IP phones
- Support for mobile agents

Some of the limitations include:

- Desktop monitoring is not supported. A VoIP Monitor service must be used for the silent monitoring and recording feature.
- CAD-BE agents cannot be run from a Citrix/MTS environment.
- Advanced reporting and workflows are not supported at this time.
- Outbound Option is not supported with CAD-BE.

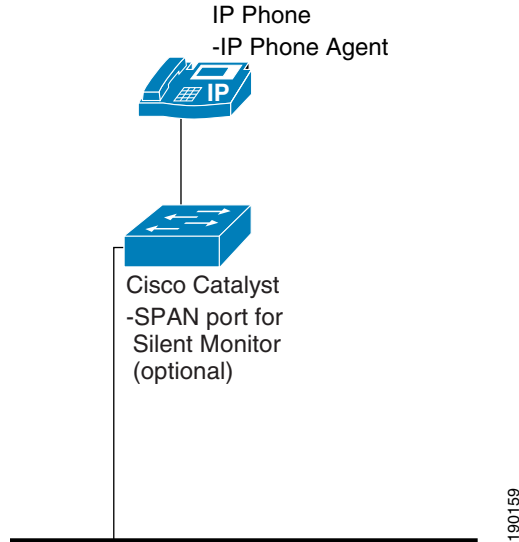
Cisco Unified IP Phone Agent

Cisco Unified IP Phone Agent (IPPA) runs as an IP phone XML service and does not require the agent to have a PC. The IPPA application allows all the basic features required by a call center agent, as well as some advanced features such as reason codes and call recording.

The IPPA application is a CAD-based agent interface and does not communicate with the CTI OS service. Therefore, IP Phone Agent cannot be used as a backup agent interface for CTI OS-based agents. With IP Phone Agent, agent state control (login, logout, ready, not ready) is done through the IP Phone Agent XML application executing on the Cisco IP Phone. IP Phone Agent call control is done using the normal call control functions on the IP Phone.

A VoIP Monitor service must be used to silently monitor or record calls for IPPA agents.

Figure 4-4 illustrates the components used by IP Phone agents.

Figure 4-4 Cisco IP Phone Agent Components

For more information on IP Phone Agent, refer to the *Cisco IP Phone Agent User Guide*, available at http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_user_guide_list.html

Cisco Supervisor Desktop

Cisco Supervisor Desktop provides a graphical view of the agent team being managed by the supervisor. An expandable navigation tree control, similar to Windows Explorer, is used to navigate to and manage the team's resources.

Supervisors are able to view real-time information about the agents in a team as well as interact with these agents. A supervisor can select an agent to change the agent's state, view information specific to that agent, silently monitor or record the agent's calls, barge in or intercept an agent's call, chat with the agent, or push a web page to the agent's desktop.

When Cisco Supervisor Desktop is installed, an instance of Cisco Agent Desktop is installed as well. Cisco Agent Desktop is needed to enable a supervisor to take calls and barge in, intercept, and retrieve skill group statistics.

The Supervisor Work Flow module within Cisco Supervisor Desktop enables configurable actions to be triggered when specific events occur in the contact center. For example, a supervisor work flow can be set up so that, whenever more than 10 calls are in queue for a specific skill group, an audible alert sounds and the skill group name is highlighted in red on the supervisor's desktop. This module enables contact centers to tailor the CAD installation to meet their specific needs.

This version of CAD has added the email alert action to supervisor work flows. This action can be triggered by skill group events (number of calls in queue or longest call in queue) and will send an email to one or more configured email addresses. The email contains information related to the condition that caused the event as well as custom text.

Cisco Supervisor Desktop now contains an integrated web browser that gives supervisors the ability to push web pages to particular agents in their team.

For more information on Cisco Supervisor Desktop, refer to the *Cisco Supervisor Desktop User Guide*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_user_guide_list.html

Cisco Desktop Administrator

Cisco Desktop Administrator enables an administrator to configure the CAD services, Cisco Supervisor Desktop, and CAD agent applications. Individual workflow groups containing agents and supervisors can be configured separately to provide specific functionality to particular groups of agents.

Using Cisco Desktop Administrator, an administrator can configure the following items:

- Enterprise data fields and layouts
- Desktop and server monitoring
- Dial strings
- Phone books available to agents
- Reason codes and wrap-up data
- Toolbar buttons for CAD and CAD-BE agents
- Appearance and behavior of the CAD and CAD-BE integrated browser
- Workflow groups
- Workflows for each agent type
- Number of browser tabs and default pages for each tab for CAD and CAD-BE agents that have integrated browser support

For more information on Cisco Desktop Administrator, refer to the *Cisco Desktop Administrator User Guide*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_user_guide_list.html

Cisco Desktop Monitoring Console

The Cisco Desktop Monitoring Console is a Java application that monitors the status of the CAD services. It provides a convenient interface for an administrator to use to get real-time information about the CAD system.

CTI Desktop Toolkit Solution

The CTI Desktop Toolkit provides a Software Development Kit (SDK) for custom development of desktop applications. The CTI Desktop Toolkit supports C++, Java, and .NET development Client Interface Libraries (CILs) and provides sample applications for customization.

Additionally, the CTI Desktop Toolkit ships complete with pre-built, ready-to-run agent desktop, supervisor desktop, and call center monitoring applications. These applications can be used as-is or can be customized further to meet the particular needs of a call center.

The CTI Desktop Toolkit also offers advanced tools for integrating desktop applications with a database, Customer Relation Management (CRM) applications, or other contact center applications.

The CTI Toolkit Desktop solution offers a rich set of features for the contact center environment, including:

- Collaboration — A supervisor can text-chat directly with agents, and agents can text-chat with supervisors or other team members (if enabled). Interactive collaboration enables the contact center to communicate better, increase productivity, improve customer responsiveness, and coach or train agents.

- Secure Desktop Connection — Desktop security is provided between the agent desktop and the CTI OS server.
- Silent Monitoring — A supervisor can initiate a silent monitor session with an agent within their team.

CTI Toolkit Software Development Kits and User Applications

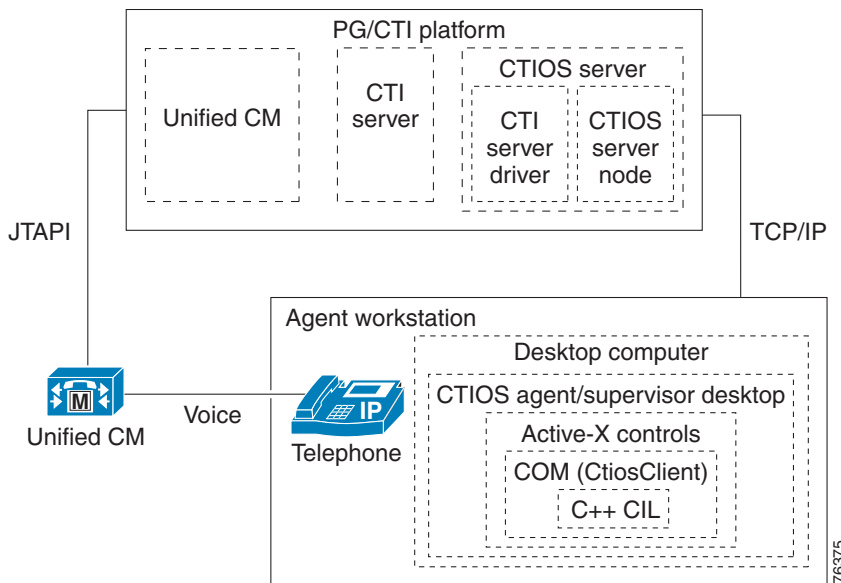
The CTI Desktop Toolkit provides the following user tools and applications:

- C++ CIL API — A Windows software development kit for developing C++ CTI applications
- Java CIL API — A cross-platform library for developing Java CTI applications
- .NET CIL API — A Windows software development kit for developing custom .NET framework CTI applications
- COM CIL API — A set of COM Dynamic Link Libraries (COM DLL) for building a Visual Basic 6.0 CTI application
- ActiveX Controls — A set of Windows GUI controls for custom desktop development using Microsoft Visual Basic 6.0
- CTI OS Runtime Callable Wrappers — A set of .NET assemblies that allows the use of COM CIL and ActiveX controls in native .NET applications
- CTI Toolkit Agent Desktop — A Windows Visual Basic application built upon the COM CIL and Active-X controls, providing agent desktop functionality
- CTI Toolkit Supervisor Desktop — A Windows Visual Basic application built upon the COM CIL and Active-X controls, providing supervisor desktop functionality
- CTI Toolkit Outbound Desktop — A Windows Visual Basic application built upon the COM CIL and Active-X controls, supporting outbound call center campaigns in addition to standard agent desktop functionality
- CTI Toolkit Combo Desktop — A Windows agent and supervisor application based on the .NET CIL, which combines support for agent, supervisor, and outbound functionality
- CTI Toolkit All-Agents Monitor — A Windows Admin application based on the C++ CIL, providing call center agent status monitoring
- CTI Toolkit All-Calls Monitor — A Windows Admin application based on the C++ CIL, providing call center call status monitoring

Figure 4-5 illustrates the architecture of the CTI Desktop Toolkit. For more information regarding the CTI Desktop Toolkit, refer to the *CTI OS Developer's Guide for Cisco ICM/IPCC Enterprise and Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps14/products_programming_reference_guides_list.html

Figure 4-5 CTI Desktop Toolkit Architecture

**C++ CIL API**

The CTI Desktop Toolkit C++ CIL provides a set of header files and static libraries for building C++ CTI applications using Microsoft Visual Studio .NET. The C++ CIL also supports a secure desktop connection between the agent PC and the CTI Object Server on the PG.

Java CIL API

The CTI Desktop Toolkit Java CIL provides a powerful cross-platform library for developing Java CTI applications.

.NET CIL API

The CTI Desktop Toolkit .NET CIL provides native .NET class libraries for developing native .NET Framework applications. The .NET Combo Desktop is provided as a sample application built using the .NET CIL.

COM CIL API

The CTI Desktop Toolkit COM CIL provides a set of COM Dynamic Link Libraries for building Visual Basic 6.0 CTI applications. The CTI Toolkit Agent and Supervisor Desktops are provided as sample applications built with Visual Basic 6.0 and using the COM CIL.

ActiveX Controls

The CTI Toolkit includes a set of ActiveX controls to enable rapid application development. The ActiveX controls are UI components that enable easy drag-and-drop creation of custom CTI applications in a variety of container applications. Container applications include Microsoft Visual Basic 6.0, Microsoft Internet Explorer, Microsoft Visual C++ 7.0, Borland Delphi, Sybase Powerbuilder, and other applications supporting the OC96 ActiveX standard.

The ActiveX Controls include:

- Agent State Control
- Chat Control
- Emergency Assist Control
- Alternate Control
- Answer Control
- Bad Line Control
- Call Appearance Control
- Conference Control
- Hold Control
- Make Call Control
- Reconnect Control
- Status Bar Control
- Record Control
- Transfer Control
- Agent Statistics Control
- Skill Group Statistics Control
- Agent Select Control
- Supervisor Control
- Silent Monitor Control

CTI Toolkit Agent Desktop

The CTI Toolkit Agent Desktop is a Microsoft Windows application that runs on an agent's desktop PC and works with either a hardware IP phone or the Cisco IP Communicator software phone. The CTI Toolkit Agent Desktop interfaces with the CTI OS server for call control and agent state change events.

The CTI Toolkit Agent Desktop includes support for desktop monitoring, which captures the voice stream on the agent's IP phone to support the silent monitoring and call recording features.

CTI Toolkit Supervisor Desktop

The CTI Toolkit Supervisor Desktop is a Microsoft Windows application that runs on a supervisor's desktop PC. The CTI Toolkit Supervisor Desktop interfaces with the CTI OS server for agent state change events and real-time statistics updates. The CTI Toolkit Supervisor Desktop provides the contact center supervisor with the ability to manage a team of agents. Supervisors are able to view real-time information about the agents in a team as well as interact with these agents. A supervisor can select an agent to change the agent's state, view information specific to that agent, silently monitor the agent's call, barge in or intercept the agent's call, or chat with the agent.

A supervisor may also receive emergency assistance requests from agents on their team through the supervisor desktop.

In the Unified CCE, supervisors may also be configured to act as agents. When this is done, the standard set of agent phone controls are available on the Supervisor Desktop.

CTI Toolkit Outbound Desktop

The CTI Toolkit Outbound Desktop is a Microsoft Windows application that runs on an agent's desktop PC and works with either a hardware IP phone or the Cisco IP Communicator software phone. The CTI Toolkit Outbound Desktop interfaces with the CTI OS server for call control and agent state change events. In addition to the standard set of agent controls present in the CTI Toolkit Agent Desktop, the Outbound Desktop provides a set of controls for managing outbound call campaigns. Outbound calls are automatically managed by the Unified CCE, and the agent utilizes the additional controls to accept the next outbound call.

CTI Toolkit Combo Desktop

The CTI Toolkit Combo Desktop is a Microsoft Windows .NET application that runs on an agent's desktop PC and works with either a hardware IP phone or the Cisco IP Communicator software phone. The CTI Toolkit Combo Desktop interfaces with the CTI OS server for call control and agent state change events.

The Combo Desktop integrates the functionality of the Toolkit Agent, Supervisor, and Outbound desktops into a single .NET application. The Combo Desktop source code is also provided as a starting point for custom desktop development using the Microsoft .NET Framework.

CTI Toolkit All-Agents Monitor

The CTI Desktop Toolkit ships complete with a ready-to-run All-Agents Monitor application. This application provides a call center administrator with the ability to monitor agent login and state activity within the call center.

CTI Toolkit All-Calls Monitor

The CTI Desktop Toolkit ships complete with a ready-to-run All-Calls Monitor application. This application provides a call center administrator with the ability to monitor call activity within the call center.

CTI Driver for Siebel Solution

The Cisco CTI Driver for Siebel is an installable component developed by Cisco that enables integration of the Cisco Unified CCE with the Siebel CRM Environment. In this solution, the Siebel Agent Desktop provides the agent state and call control interface. The Siebel Desktop utilizes the Cisco CTI Driver for Siebel, which is built on top of the CTI Desktop Toolkit C++ CIL to communicate with the CTI Object Server.

For more information on the capability of the Siebel eBusiness solution, refer to the Siebel website at

<http://www.siebel.com/index.shtm>

Deployment Considerations

This section covers the following deployment considerations:

- [Citrix and Microsoft Terminal Services \(MTS\)](#), page 4-17
- [Silent Monitoring](#), page 4-18
- [NAT and Firewalls](#), page 4-43
- [Co-Residency of CTI OS and CAD Services on the PG](#), page 4-45
- [Support for Mix of CAD and CTI OS Agents on the Same PG](#), page 4-45

- [Support for IP Phones and IP Communicator, page 4-45](#)
- [Miscellaneous Deployment Considerations, page 4-46](#)

Citrix and Microsoft Terminal Services (MTS)

This section discusses deploying Cisco Agent Desktop and Cisco Toolkit Desktop in a Citrix or Microsoft Terminal Services (MTS) environment.

Cisco Agent Desktop

Cisco Unified CCE supports running Cisco Agent Desktop within a Citrix terminal services environment. When planning to use Citrix terminal services for CAD, take the following considerations into account:

- Cisco Supervisor Desktop (CSD) and Cisco Desktop Administrator (CDA) are not supported in a Citrix terminal services environment.
- Desktop monitoring (for silent monitoring and recording) is not supported with Citrix terminal services. SPAN port monitoring must be used instead.
- Macros work only if they involve applications running on the Citrix server, and not those running on the client PC.
- Only one Citrix user name is supported per CAD application login.
- The login ID and extension that appear by default in the login dialog box when CAD is started, are those associated with the last login by any user.
- The Citrix web client is not supported.
- Only Citrix 4.0 running on Windows 2000 Server or Windows 2003 Server are supported.

For implementation details, refer to *Integrating CAD into a Citrix MetaFrame Presentation Server or Microsoft Terminal Services Environment*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_implementation_design_guides_list.html

Cisco Toolkit Desktop

Cisco Unified CCE supports running CTI Toolkit Desktop within the Citrix and Microsoft Terminal (MTS) Services environments. When planning to use Citrix terminal services with the CTI Toolkit Desktop, take into account the following considerations:

- Versions of Citrix MetaFrame Presentation Server prior to Version 4.0 are not supported. Earlier versions have limitations for publishing Microsoft .NET applications.
- CTI OS Java CIL client applications are supported only on Citrix MetaFrame Presentation Server 4.0 for the Windows platform. There is no planned support for Citrix MetaFrame Presentation Server 4.0 on UNIX.
- Silent Monitoring is supported within a Citrix or MTS environment.
- CTI OS Client Desktop sounds such as dial tones and DTMF tones are not audible.

For implementation details, refer to *Integrating CAD into a Citrix MetaFrame Presentation Server or Microsoft Terminal Services Environment*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps427/products_implementation_design_guides_list.html

Silent Monitoring

Silent monitoring enables supervisors to monitor the conversations of agents within their team. Supervisors are not able to participate actively in the conversation, and the agent(s) and caller(s) are unaware they are being monitored. Both the Cisco Agent Desktop and the CTI Desktop Toolkit provide solutions support for silent monitoring. CAD Server-based monitoring supports Agent Desktops, IP Phone Agents, and Mobile Agents. Desktop monitoring supports only desktop agents. CTI OS releases 7.2 and later support two types of silent monitors: CTI OS silent monitor and Unified CM silent monitor.

CTI OS silent monitoring is accomplished via one or more VoIP monitoring services located either on the agent's desktop (desktop monitoring) or on a separate VoIP monitor server (server-based monitoring). CTI OS uses server-based silent monitoring to support mobile agents and desktop-based silent monitoring to support traditional (non-mobile) Unified CCE agents.

Unified CM accomplishes silent monitoring with a call between the supervisor's (monitoring) device and agent's (monitored) device. The agent's phone mixes and sends the agent's conversation to the supervisor's phone, where it is played out to the supervisor. Unified CM silent monitoring can be initiated by any of the CTI OS supervisor desktops (out-of-the-box, Java, or .NET). Any Unified CCE agent desktop, including Siebel, can be silently monitored using Unified CM silent monitoring, provided the following requirements are met:

- The agent to be silently monitored is using a Cisco Unified IP Phone 7941, 7961, or 7971
- The contact center is using Cisco Unified CM 6.x
- Phones are configured to use RTP streams (SRTP streams cannot be silently monitored)

Unified CM silent monitoring does not support mobile agents.

Supervisors can use any Cisco IP Phone, including Cisco IP Communicator, to silently monitor.

CTI Toolkit Silent Monitor

A given CTI OS Server can be configured to use either CTI OS silent monitor or Unified CM silent monitor, or to disable silent monitoring. When supervisor desktops connect to the CTI OS Server, this configuration is downloaded. The supervisor desktop uses this information to invoke the configured type of silent monitor when the Start Silent Monitor button is pressed. The initial message from the supervisor desktop is used by the CTI OS Server to drive either the CTI OS or Unified CM silent monitor.

For details regarding the configuration of silent monitoring, system administrators can refer to the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_installation_guides_list.html

Developers implementing either the CTI OS or Unified CM silent monitor should refer to the *CTI OS Developer's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps14/products_programming_reference_guides_list.html

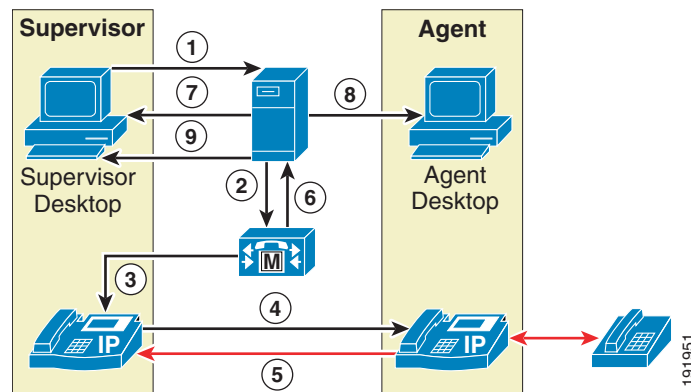
Unified CM Silent Monitor

This section describes how CTI OS accomplishes silent monitoring when the CTI OS Server is configured to use the Unified CM silent monitor.

Unified CCE 7.2(1) adds support for the silent monitoring functionality available in Unified CM 6.x. [Figure 4-6](#) illustrates the following message flow, which occurs when the Unified CM silent monitor is initiated by the supervisor desktop:

1. The supervisor initiates silent monitoring by sending the Agent.SuperviseCall() message to Unified CCE.
2. Unified CCE sends the Call.startMonitor() message to Unified CM.
3. Unified CM instructs the supervisor's phone to call the built-in-bridge in the agent's phone.
4. The supervisor's phone places the call to the built-in-bridge in the agent's phone.
5. The agent's phone forwards a mix of the agent's and customer's voice streams.
6. Call events for the silently monitored call are sent from Unified CM to Unified CCE.
7. CTI OS sends a SilentMonitorStarted event to the supervisor desktop.
8. CTI OS sends a SilentMonitorStarted event to the agent desktop.
9. CTI OS sends call events for the silently monitored call to the supervisor desktop.

Figure 4-6 Unified CM Silent Monitoring for Unified CCE



Unified CM silent monitoring works the same as other call control functionality provided by Unified CM (such as conference, transfer, and so forth). When Unified CM is used for silent monitoring, a message is sent from the desktop, through Unified CCE, through Unified CM, and out to the phones where silent monitoring is executed.

The messaging through Unified CCE and Unified CM impacts Unified CCE performance. For further details regarding the impact of Unified CM silent monitoring on Unified CCE sizing, see the chapter on [Sizing Unified CCE Components and Servers](#), page 10-1.

Unified CM silent monitoring is supported only for agents who are connected to Unified CCE on the LAN; it does not support mobile agents and remote agents (agents connected to Unified CCE across a WAN).

**Note**

Starting with Unified CM 5.1, G.722 is used as the default codec for regions that are configured for G.711 on devices that support G.722. G.722 does not work with Unified CM silent monitoring. To disable this default, in Unified CM Administration go to Enterprise Parameters and set "Advertise G.722 Codec" to disabled.

CTI OS Silent Monitor

This section describes how CTI OS accomplishes silent monitoring when the CTI OS Server is configured to use the CTI OS silent monitor.

The silent monitoring solution provided by CTI Toolkit in Release 7.0 and earlier was integrated in the CIL. The CIL had components to capture and forward voice packets as well as components to play back a stream of forwarded voice packets to the supervisor's sound card. This feature limited silent monitoring support to IPCC agent desktops deployed behind a Cisco IP Phone and IPCC supervisor desktops deployed on the supervisor's desktop.

In Release 7.1 of CTI OS, two new deployment types were introduced: Citrix and Mobile Agent. In these two deployments, the CIL is not deployed where it has access to the voice stream. In Citrix, the CIL is located on the Citrix Server. Agents and supervisors use a Citrix client to run the desktop. When this is done, the desktop runs on the Citrix server. The Citrix client merely displays the UI of the desktop. Because it is the agent's Citrix client that is deployed behind the IP phone, the CIL no longer has access to the voice path. Similarly, it is the supervisor's Citrix client that has the sound card. In this case, the CIL is running on the Citrix server and does not have access to the sound card.

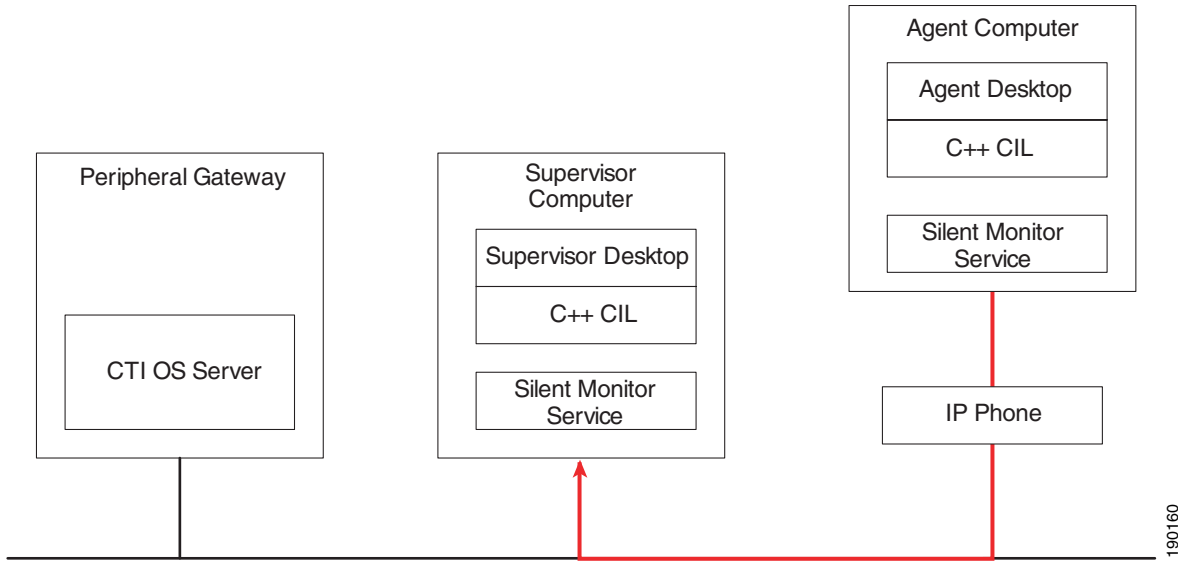
In Mobile Agent deployments, the CIL is deployed on an agent's remote PC. When the agent uses an analog phone, the CIL does not have access to the voice stream.

To support these two deployment models, it was necessary to break the silent monitor components out of the CIL and put them on a separate service. This allows the service to be deployed where it has access to the agent's voice stream or the supervisor's sound card.

The following figures show where the silent monitoring service should be deployed for each deployment model. The red line in each diagram illustrates the path of the monitored voice stream.

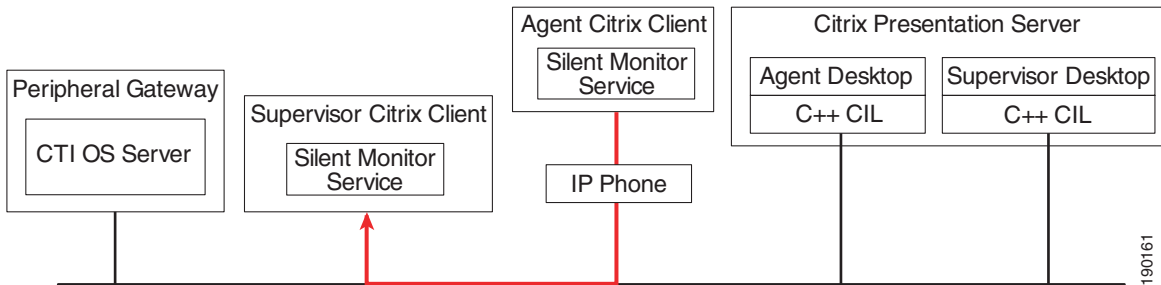
[Figure 4-7](#) and [Figure 4-8](#) illustrate deployments where the agent uses an IP phone. In these deployments, silent monitoring is configured the same way regardless of whether the agent is mobile or not.

Figure 4-7 Silent Monitoring for Cisco Unified CCE When a Mobile or Local Agent Uses an IP Phone



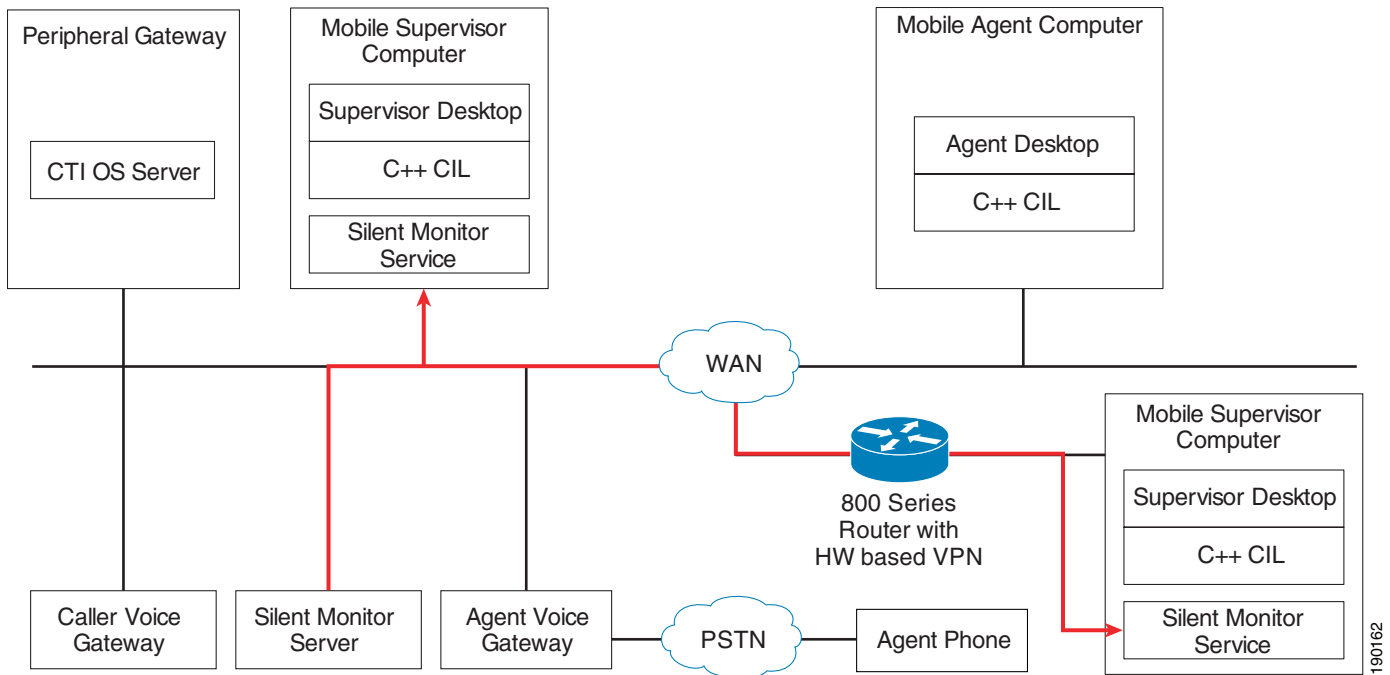
The deployment in [Figure 4-7](#) is very similar to CTI OS Release 7.0 and earlier deployments. The only difference is that the silent monitoring service is running alongside the CIL to provide silent monitoring functionality.

Figure 4-8 Silent Monitoring for Cisco Unified CCE with Citrix When a Mobile or Local Agent Uses an IP Phone



In the deployment model in [Figure 4-8](#), the silent monitoring service is deployed on Citrix clients, where it has access to the agent's voice stream and the supervisor's sound card. The CIL makes a connection to the silent monitoring service and sends it instructions over a TCP connection in order to start and stop silent monitoring sessions.

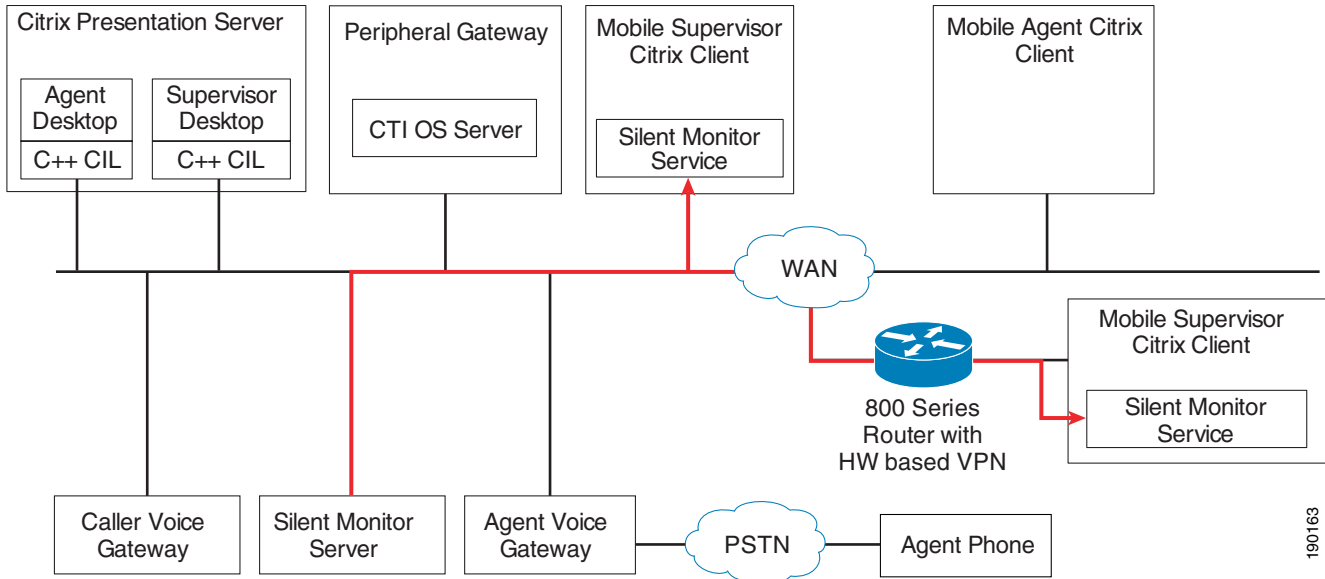
Figure 4-9 Silent Monitoring for a Mobile Agent Using a PSTN Phone



In the deployment model in [Figure 4-9](#), one silent monitoring service is deployed on a switch's SPAN port in order to gain access to voice traffic passing through the agent gateway. This silent monitoring service is used by agents to forward their voice streams to supervisor silent monitoring services.

Supervisors running locally are deployed the same as IPCC supervisors. Supervisors running remotely are also deployed the same as IPCC supervisors, but a Cisco 800 Series Router with hardware-based VPN is required in order for the supervisor to receive agent voice streams.

Figure 4-10 Silent Monitoring for a Mobile Agent Using a PSTN Phone with Citrix or Microsoft Terminal Services



In the deployment model in [Figure 4-10](#), one silent monitoring service is deployed on a switch's SPAN port in order to gain access to voice traffic passing through the agent gateway. This silent monitoring service is used by agents to forward their voice streams to supervisor silent monitoring services. Mobile agents need to run only their Citrix clients. Agent desktops running on the Citrix server will connect to the silent monitoring server.

Supervisors running locally are deployed the same as Citrix IPCC supervisors. Supervisors running remotely are also deployed the same as Citrix IPCC supervisors, but a Cisco 800 Series Router with hardware-based VPN is required in order for the supervisor to receive agent voice streams.

In the two mobile agent deployments above ([Figure 4-9](#) and [Figure 4-10](#)), calls whose voice traffic does not leave the agent gateway cannot be silently monitored. This includes agent-to-agent calls as well as agent consultations with other agents. The only calls that can be reliably monitored in this case are calls between agents and customers. This is because the mobile agent solution requires separate gateways for callers and agents to ensure that voice traffic is put on the network.

Clusters

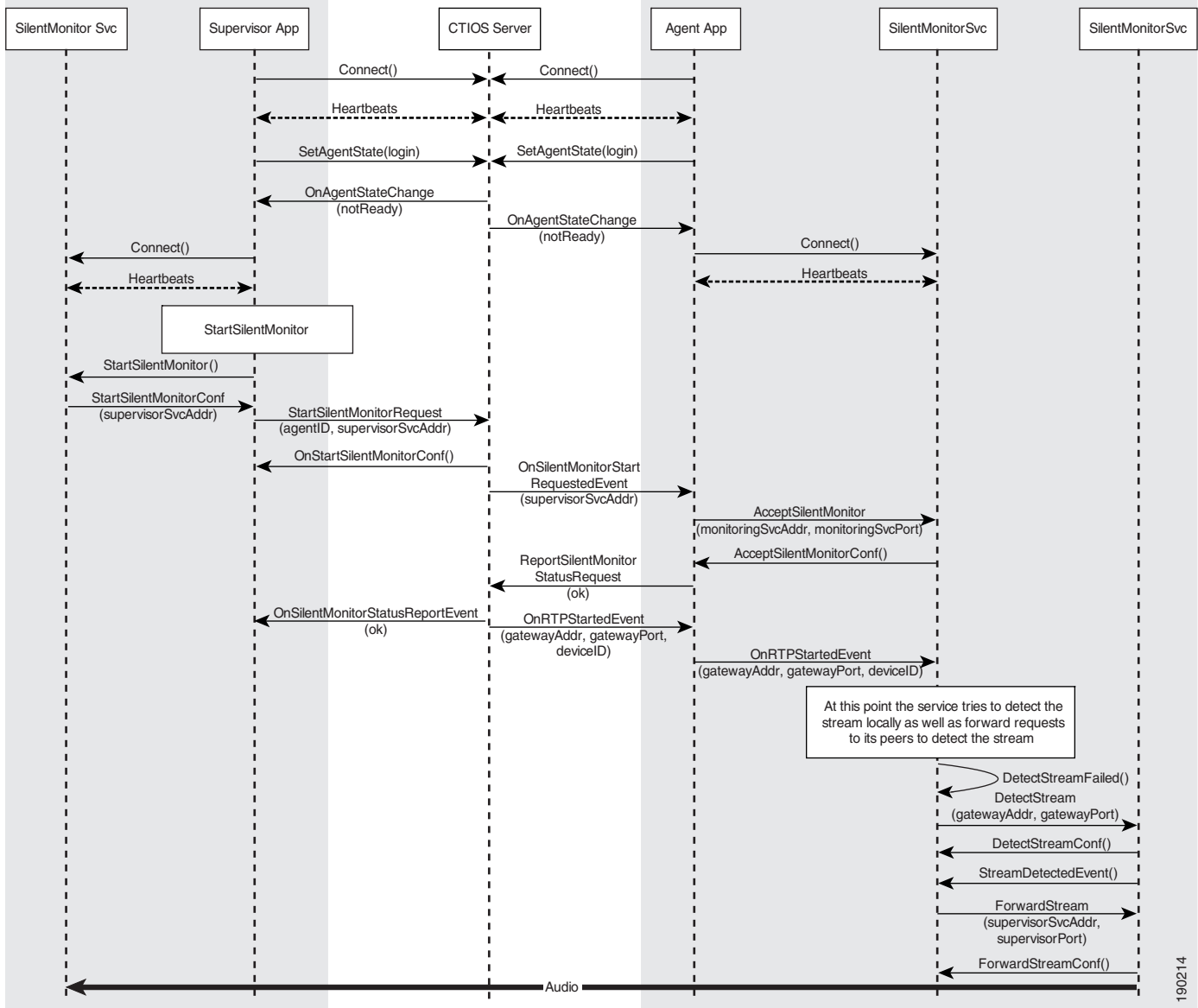
If a mobile agent's login can be handled by one of two gateways, it is possible to cluster two silent monitoring servers together to provide silent monitoring functionality regardless of the gateway that handles the call. When a request to silent-monitor the agent is received, the silent monitoring server that receives the request from the agent desktop will forward the request to its peer, and then both silent monitoring servers will attempt to detect the stream. Once the agent's voice stream is detected, it is forwarded to the supervisor's silent monitoring service by the silent monitoring server that detected the stream.

For more information regarding deployment and configuration of the silent monitoring service, refer to the *CTI OS System Manager's Guide* for Release 7.1, available on <http://www.cisco.com>.

Message Flow

Figure 4-11 illustrates the messaging that occurs between the desktops, CIT OS Server, and silent monitoring services when a silent monitor session is initiated. Note that messaging between the desktops and the CTI OS Server has not changed from CTI OS Release 7.0.

Figure 4-11 Message Flow Between Desktops, CTI OS Server, and Silent Monitoring Service



190214

Connection Profiles

In mobile agent deployments, agent desktops learn where and how to connect to their silent monitoring server using a CTI OS connection profile. When an agent logs in, the agent desktop uses the following algorithm to determine where the silent monitoring service is located:

1. If a silent monitoring service is present in the connection profile, attempt to connect to it.
2. If no silent monitoring service is present, determine if the desktop is running under Citrix.
3. If the desktop is running under Citrix, connect to the silent monitoring service running at the Citrix client's IP address.
4. If the desktop is not running under Citrix, connect to the silent monitoring service running at **localhost**.

Supervisor desktops use the following algorithm to find their silent monitoring service:

1. If the desktop is running under Citrix, connect to the silent monitoring service running at the Citrix client's IP address.
2. If the desktop is not running under Citrix, connect to the silent monitoring service running at **localhost**.

If the `IPCCSilentMonitorEnabled` key is set to 0 in the connection profile, no attempt is made to connect to a silent monitoring service.

Cisco Remote Silent Monitoring

This section covers Cisco Remote Silent Monitoring. Remote Silent Monitoring (RSM) is a new feature available for Cisco Unified Contact Center Enterprise Release 7.2 and later that allows for the real-time monitoring of agents as a dial-in service.

The RSM solution consists of three components:

- VLEngine
- PhoneSim
- Callflow Script(s) for Unified CVP and IP IVR

For a further description of these components, refer to the *Cisco Remote Silent Monitoring Installation and Administration Guide*, available at <http://www.cisco.com>.

Hardware Considerations

The RSM solution is highly integrated part of a Cisco Unified Contact Center Enterprise environment. Because of this, the functioning of RSM requires resources from various other components of the platform as a whole. To properly integrate RSM, then, requires an understanding of its interactions with the rest of the environment so that capacity can be properly planned, provisioned, and managed.

Platform Considerations

In particular, RSM interacts mainly with the following components in the environment:

Unified CM Cluster

The RSM server has two tie-ins with each Unified CM cluster in the environment that it is configured to use:

Simulated Phones: RSM's PhoneSim component requires that a Cisco Unified IP Phone 7941 device entry be created on the Unified CM cluster for each of the simulated phones (or "simphones") it is configured to manage. For instance, a RSM system that is configured to handle up to 100 dialed-in supervisors monitoring agents on a particular Unified CM cluster will need to have at least of these 100 simphones. To the Unified CM cluster itself, these simphones appear as normal Cisco Unified IP Phone 7941 SIP phones; however, in reality they are homed to and controlled by PhoneSim instead of being an actual physical phone device.

When compared with the usage profile of a normal phone, the simphone usually puts a lighter load on the Unified CM cluster. This is because it exhibits only a small set of behaviors, consisting of:

- Registering with the Unified CM cluster when PhoneSim is started.
- Making a "monitoring call" to an agent's phone when a dialed-in supervisor requests to monitor that agent. The agent's phone then forks off a copy of the conversation the agent is having to the simphone.

JTAPI: When RSM is integrated into the environment, a JTAPI user is created and associated with each agent phone device that can be monitored, as well as with each simphone device that was created on the cluster.

When an agent is to be monitored, a JTAPI monitor request call is made from the RSM server to the Unified CM cluster that manages that agent's phone. Also, while RSM is in use, a JTAPI CallObserver is kept attached to each simphone device. It is also attached to an agent phone device, but only while the JTAPI monitor request is being issued to that device.

JTAPI connections may optionally be encrypted. However, this will induce a slight performance penalty on the server itself when higher agent loads are utilized. For more information on enabling JTAPI connection security, refer to the *Cisco Remote Silent Monitoring Installation and Administration Guide*, available at <http://www.cisco.com>.

AXL: AXL usage is relatively light; it is used by RSM only to resolve an agent DN to an associated device name whenever a caller requests to monitor to an agent. All AXL communications are encrypted (via being run over HTTPS).

CTI OS Server

RSM makes a persistent "monitor-mode" connection to each CTI OS server it is configured to use. Through this connection certain platform events such as call start, call end, agent on hold, and so forth, are streamed in real-time.

Besides this, RSM will make an additional, short-lived "agent-mode" connection to possibly each CTI OS server when a supervisor dials in and authenticates. The purpose of this connection is to validate the supervisor's entered credentials by performing a corresponding login into CTI OS. Note that, if the built-in authentication mechanisms of the RSM callflow (for example, the checkCredentials API call) are not used, this connection is not made. If the login is successful, that supervisor's team membership is requested by the RSM server. Once returned, a logout is called and the connection is terminated.

Note that the total supervisor count in Unified CCE must be spread across CTI OS desktop users and RSM. For example, in a 2000 agent configuration, up to 200 agents can be supervisors. This means that the total supervisor count between CTI OS and RSM must not exceed 200.

CTI OS connections may be optionally encrypted (via use of IP Sec configurations). However, this will induce a significant performance penalty on the server itself when higher agent loads are utilized. For more information on enabling CTI OS connection security, refer to the *Cisco Remote Silent Monitoring Installation and Administration Guide*, available at <http://www.cisco.com>.

VRU

The RSM platform does not directly media-terminate inbound calls. Instead, supervisors dial into a Unified CVP or IP IVR-based VRU system, which runs call flow script logic that interacts with services hosted on the RSM server via HTTP. Thus, if a given RSM installation is to support up to 40 dialed-in supervisors, there must be a VRU present (as well as the necessary PRI/network resources) that can offer this same level of support.

Furthermore, a caller accessing RSM will often place a higher load on the VRU's processor(s) and memory than a caller accessing some more traditional IVR-type callflow. This is because, in a more traditional IVR callflow, shorter, oftentimes cached or non-streamed prompts are played, separated by periods of caller input gathering and silence. With RSM, however, the predominant caller activity is monitoring an agent's call, and to the VRU this looks like the playback of a long streaming audio prompt, which is an activity that requires a relatively high level of VRU processor involvement.

With Unified CVP deployments, supported VXML gateway models are listed in the *Hardware and System Software Specification for Cisco Unified Customer Voice Portal (Unified CVP)*, otherwise known as Unified CVP Bill of Materials (BOM), available at <http://www.cisco.com>.

When provisioning a VRU for use by RSM, a good rule of thumb is to count each RSM call as 1.3 non-RSM calls on a processor/memory-usage basis. So for a VRU that can normally handle 40 concurrent calls, plan for it to be able to handle only 30 RSM calls. $(40 * 1.3) = 30$

Also note that RSM makes extensive use of VXML Voice Browser functionality under both Unified CVP and IP IVR.

Agent Phones

Use of RSM to monitor an agent requires that that agent's phone be a third generation of newer Cisco Unified IP Phone 79x1, 79x2, 79x5, 7970 or newer. This is because these phones include extra DSP resources in the form of a Built-in-Bridge (BiB). The BiB allows the phone to fork off a copy of the current conversation stream to the RSM server.

Cisco Unified Contact Manager provides for a maximum of one active monitoring session per agent because the agent's phone can handle only one active monitoring session and one active recording session at any given time.

So, if a third-party recorder is recording the agent's conversations, the agent can still be monitored by a supervisor using supervisor desktop or RSM. However, if both a RSM-based supervisor and a supervisor-desktop-based supervisor both tried to monitor the agent during the same time period, the request would fail with the last one to try because it would exceed the above-mentioned monitoring limit.

Note that RSM will set up only one monitoring session through Unified CM for a single monitored agent, even if two or more RSM users are requesting to monitor the agent's call at the same time. In this case, RSM forks the stream to cover all RSM users. This allows more than two RSM-based supervisors to monitor the same agent, for instance. However, if there are multiple RSM servers in the environment that monitor the same agent, they will each make a separate monitoring call to that agent.

If the monitoring call limit has been reached for a specific agent and a dialed-in supervisor then attempts to monitor this same agent, the supervisor's request will be denied via an audio prompt feedback from the system stating that the agent cannot be monitored.

RSM Hardware Considerations

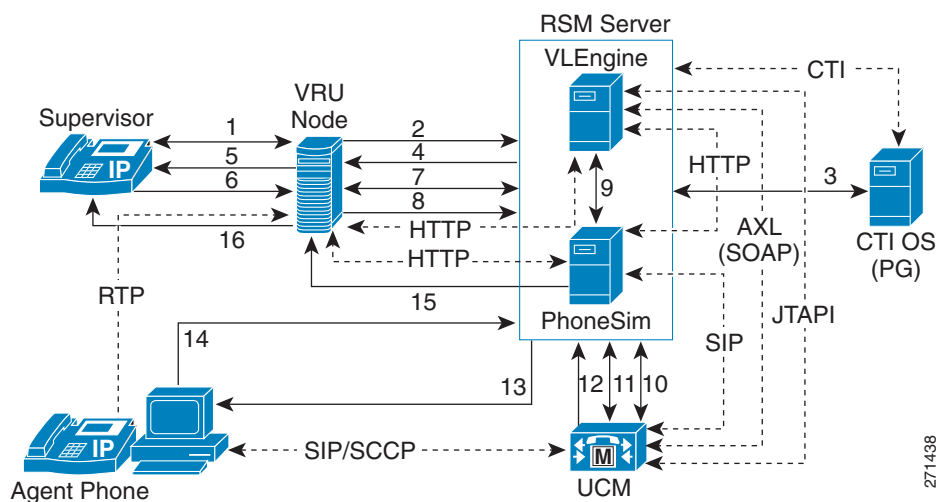
RSM is supported in installations where the number of agents in the enterprise is less than 8,000 and the number of maximum concurrent number supervisors using the system is less than 80. In all supported RSM configurations, the VLEngine and PhoneSim components are installed on the same physical server.

For more information, refer to the RSM Requirements section of the *Cisco Remote Silent Monitoring Installation and Administration Guide*, available at <http://www.cisco.com>.

RSM Component Interaction

Figure 4-12 illustrates the types of interactions that occur when a supervisor dials into an RSM-enabled platform and monitors an agent.

Figure 4-12 Remote Silent Monitor Enabled Call Flow



RSM Call Flow

Figure 4-12 shows the following call flow steps:

1. Supervisor calls in, and the call is media-terminated on the VRU (Unified CVP or IP IVR). The VRU runs the RSM callflow script to handle the call. The call begins by the user being asked to authenticate himself or herself. The user then enters his or her credentials.
2. After the user enters his or her credentials, the VRU makes a login request to RSM over HTTP.
3. The VLEngine component in RSM interacts with the CTI OS server to validate the authentication credentials.
4. VLEngine replies back to the VRU node via HTTP with the authentication result.
5. If the supervisor is successfully authenticated, the script in the VRU will play the main menu prompt. From here, the supervisor will be allowed to monitor an agent.
6. The supervisor chooses to monitor a single agent from the main menu, and enters a Directory Number (DN) of an agent to be monitored.

7. The VRU checks with VLEngine if the given agent can be monitored. VLEngine then checks whether the agent with that DN is logged in, is in talking state, and is in the supervisor's team, using previously cached event feed information from the CTI OS server. If so, it replies back to the VRU node.
8. The VRU node then sends a monitor request to PhoneSim to monitor the entered DN.
9. VLEngine works internally using HTTP.
10. VLEngine resolves the device name of the agent phone from the entered directory number (DN) using an AXL request to Unified CM and gets a response.
11. Following that, VLEngine sends a JTAPI request to Unified CM to monitor the agent's phone, and it gets a JTAPI success response.
12. The PhoneSim component will then receive a SIP-based instruction from Unified CM for a simulated phone that it manages, to establish a monitoring call with the agent's phone.
13. The chosen simulated phone establishes the monitoring call with the agent's phone based on Unified CM's above request.
14. After the establishment of a monitoring call from RSM server to agent, the agent phone's Built-in-Bridge (BiB) forwards the call conversation to PhoneSim in the form of RTP packets.
15. In turn, PhoneSim strips the RTP headers and streams this data to the VRU node over HTTP as a response to the request made earlier in step 8.
16. The VRU then plays the data to the supervisor as if it were a streaming audio prompt.

Figure 4-13 also illustrates the various protocol interfaces that RSM has into the rest of the system:

- **HTTP(S):** As stated previously, HTTP is used as the carrier protocol for VRU-based requests into the RSM system. A request takes standard URL form and may look like one of the following URLs:

```
http://rsmserver:8080/vlengine/checkUserCredentials?supervisorID=1101&pin=1234&outputFormat=plain
```

```
http://rsmserver:8080/vlengine/canMonitorAgentID?supervisorID=1101&agentID=1001&outputFormat=vxml
```

The first request above is for the checkUserCredentials API call, while the second is for the canMonitorAgentID API call. Parameters to these requests are passed via the GET method. The return data (as an HTTP response) is either plaintext or encapsulated in VoiceXML, depending on the API call being used and on the value specified for the outputFormat parameter (if available for that call).

- **SOAP (AXL):** The Unified CM AXL interface is used by RSM to resolve an agent DN to an associated device name whenever a dialed-in supervisor requests to monitor an agent. The AXL API is encapsulated in SOAP messages, which themselves are encapsulated in HTTP(S).
- **CTI OS:** The RSM server makes several connections to CTI OS. One of these connections is for receiving platform events. (In the language of CTI OS, it is a monitor-mode connection.) The other(s) are what CTI OS calls agent mode connections and are used to authenticate logging-in supervisors if the standard authentication facilities are being utilized.
- **JTAPI:** The request to start monitoring an agent's phone is made through JTAPI. This requires a JTAPI application user to be defined on each Unified CM cluster in the environment, and to be associated to all agent phones.
- **RTP:** While a dialed-in supervisor is monitoring an agent, there will be a monitoring call in progress from the BiB (built-in-bridge) of that agent's phone to the RSM server. While the signaling data for this call is run through Unified CM (just like any other call), the RTP traffic will flow between the agent phone and the RSM server.

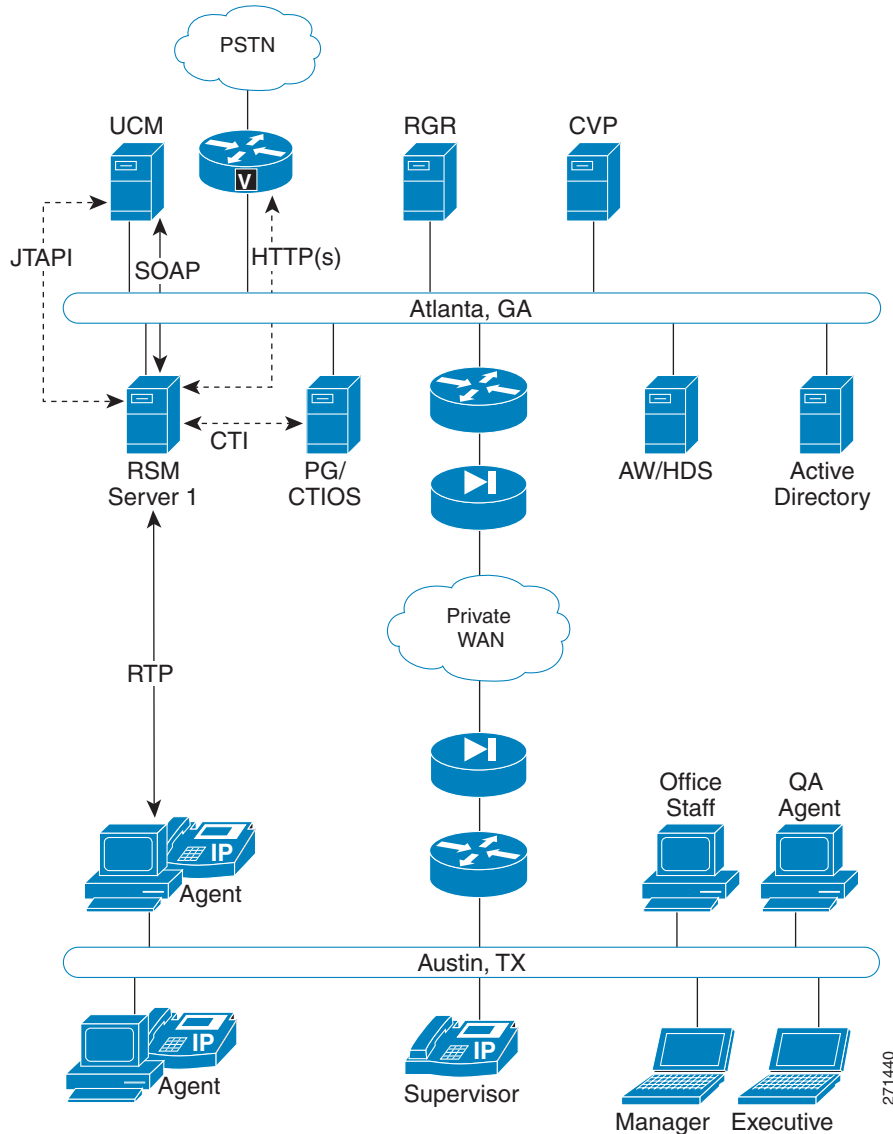
Multisite WAN

The following scenarios depict basic supported configurations for the RSM product in a multi-site deployment.

Single Cluster, Single VRU

Figure 4-14 depicts a simple multi-site setup involving a single Unified CM cluster and a single VRU.

Figure 4-14 Multi-Site Deployment with a Single UCM Cluster and Single VRU



In this case, the Unified CM and Unified CE environment is co-located in Atlanta, and the Austin location contains the entire end-user population. The VRU is a VXML Gateway/voice gateway in Atlanta, controlled by a Unified CVP Call Server also in Atlanta.

The supervisor in Austin could possibly have two ways of dialing into the RSM system:

- Through the PSTN — Here the supervisor would dial an E.164 number, and the call would be hairpinned through the voice gateway. The Unified CVP RSM callflow application would handle the call as normal from that point.
- As a VoIP extension — In this case, Unified CM would have a trunk configuration set up to the VRU. The call would remain VoIP all the way through, and the call would likewise be handled by the Unified CVP RSM callflow application.

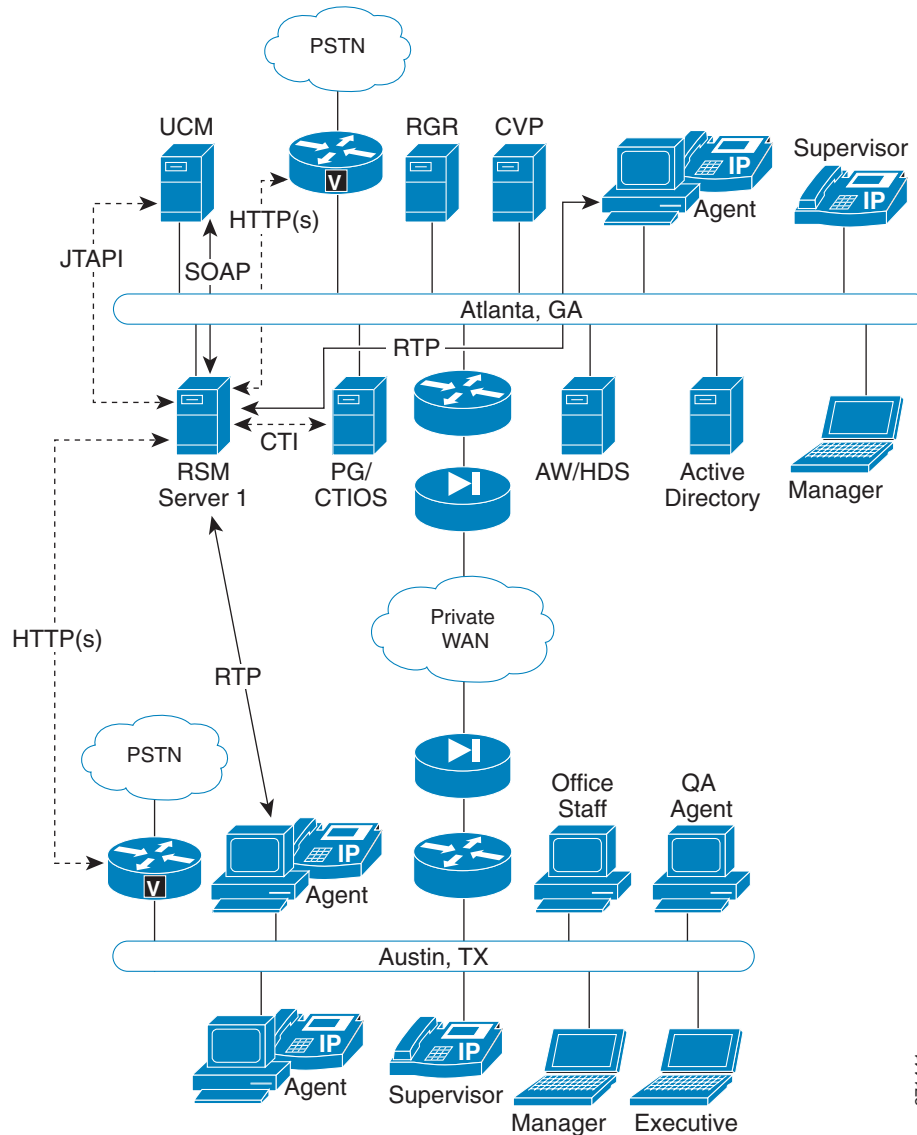
In this scenario, all RSM traffic is confined to the Atlanta site except:

- The RTP traffic of the agent being monitored (signified as a red dotted line)
- The actual supervisor call into the platform

Single Cluster, Multiple VRUs

Figure 4-15 depicts a multi-site deployment with a single Unified CM cluster and multiple VRUs.

Figure 4-15 Multi-Site Deployment with a Single Unified CM Cluster and Multiple VRUs



271441

This scenario is similar to the previous one, with the addition of PSTN access at the Austin site. This scenario also adds personnel to the Atlanta site.

With the addition of a PSTN egress point in Austin, a call from a supervisor at the Austin location to the RSM system could be backhauled across the WAN (if VoIP end-to-end) or sent across the PSTN if the Atlanta DID associated with the RSM application was dialed.

In this example, Unified CVP is still used as well as the Unified CVP Call Server. However, there are two VXML Gateways, one at each site. The environment is configured so that a supervisor dialing RSM from Austin will be routed to the RSM callflow application on the Austin VXML Gateway, while a supervisor dialing in from Atlanta will be routed to the Atlanta VXML Gateway.

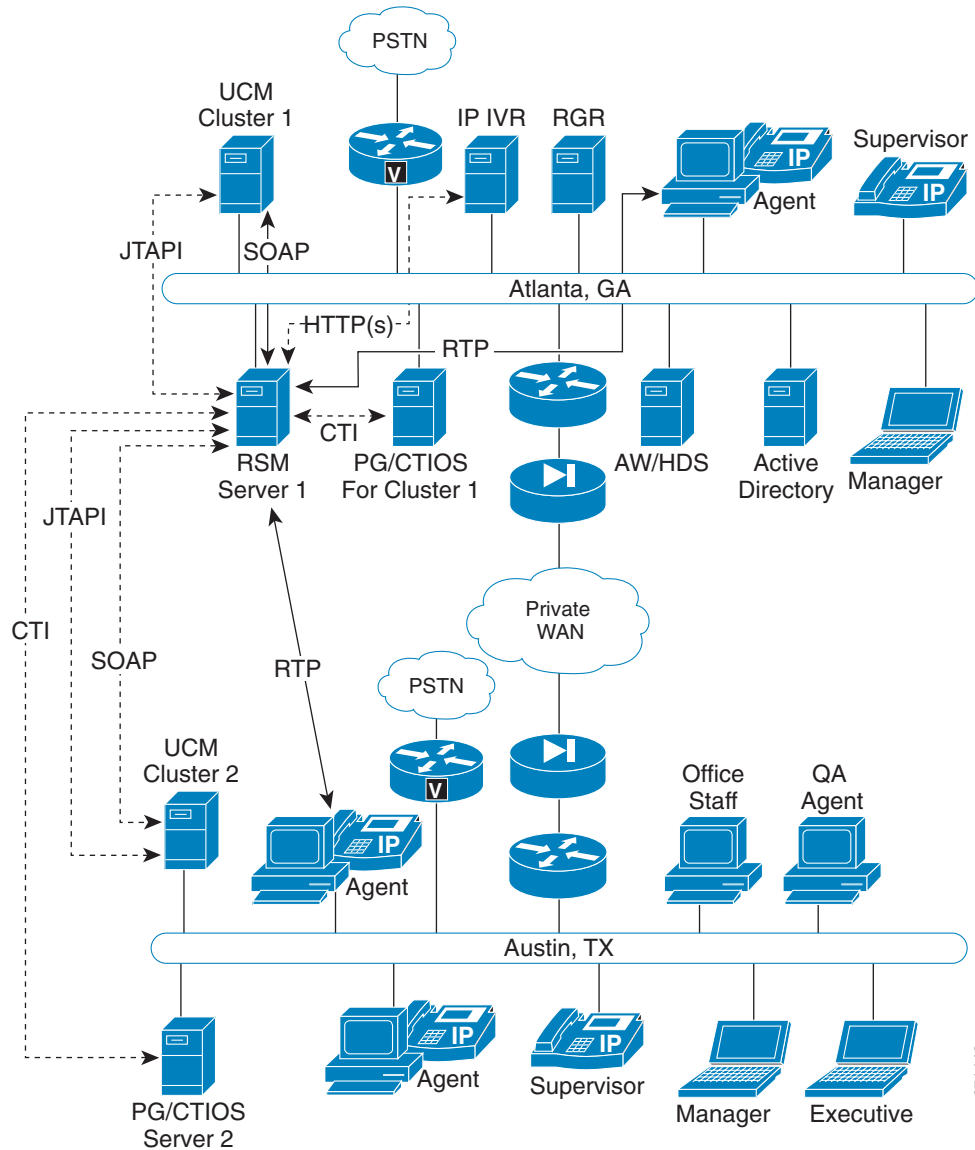
Because the Atlanta site houses the Unified CM and Unified CE environment, all RSM-related JTAPI, CTI OS, and SOAP (AXL) traffic is still confined there. However, the addition of a VXML Gateway at Austin will lead to HTTP-based traffic being streamed between the sites over the WAN. This traffic consists of relatively small requests from the gateway to the RSM server for services, and the RSM server's responses. The responses themselves can be sizeable, especially when it is the data for a monitored conversation.

Also, when an agent in Austin is monitored, the RTP data for that conversation is sent over the WAN back to the RSM server as well.

Multiple Cluster, Single VRU

Figure 4-16 depicts a multi-site deployment with multiple Unified CM clusters and a single VRU.

Figure 4-16 Multi-Site Deployment with Multiple Unified CM Clusters and a Single VRU



271442

This configuration includes a Unified CM cluster at both the Atlanta and Austin sites and a single IP IVR VRU in Atlanta. Cluster 1 handles the phone devices at the Atlanta site, while Cluster 2 handles the ones at the Austin site. The RSM server is linked to the CTI OS servers of both clusters in order to track all agents in the enterprise.

As IP IVR is in use, a supervisor call to the RSM callflow will be routed to, and media-terminated on, this IP IVR system over either the PSTN or IP WAN (as discussed previously). No VXML Gateway is involved in this configuration, and all RSM-related HTTP interaction is confined to the Atlanta site, between the RSM and IP IVR systems.

Because a Unified CM cluster now exists at the Austin site, several classes of data that RSM uses to track environment state and initiate agent monitoring requests (CTI OS, AXL/SOAP, and JTAPI traffic) are sent over the IP WAN.

Multiple Cluster, Multiple VRUs

Figure 4-17 depicts a multi-site deployment with multiple Unified CM clusters and multiple VRUs.

Figure 4-17 Multi-Site Deployment with Multiple Unified CM Clusters and Multiple VRUs

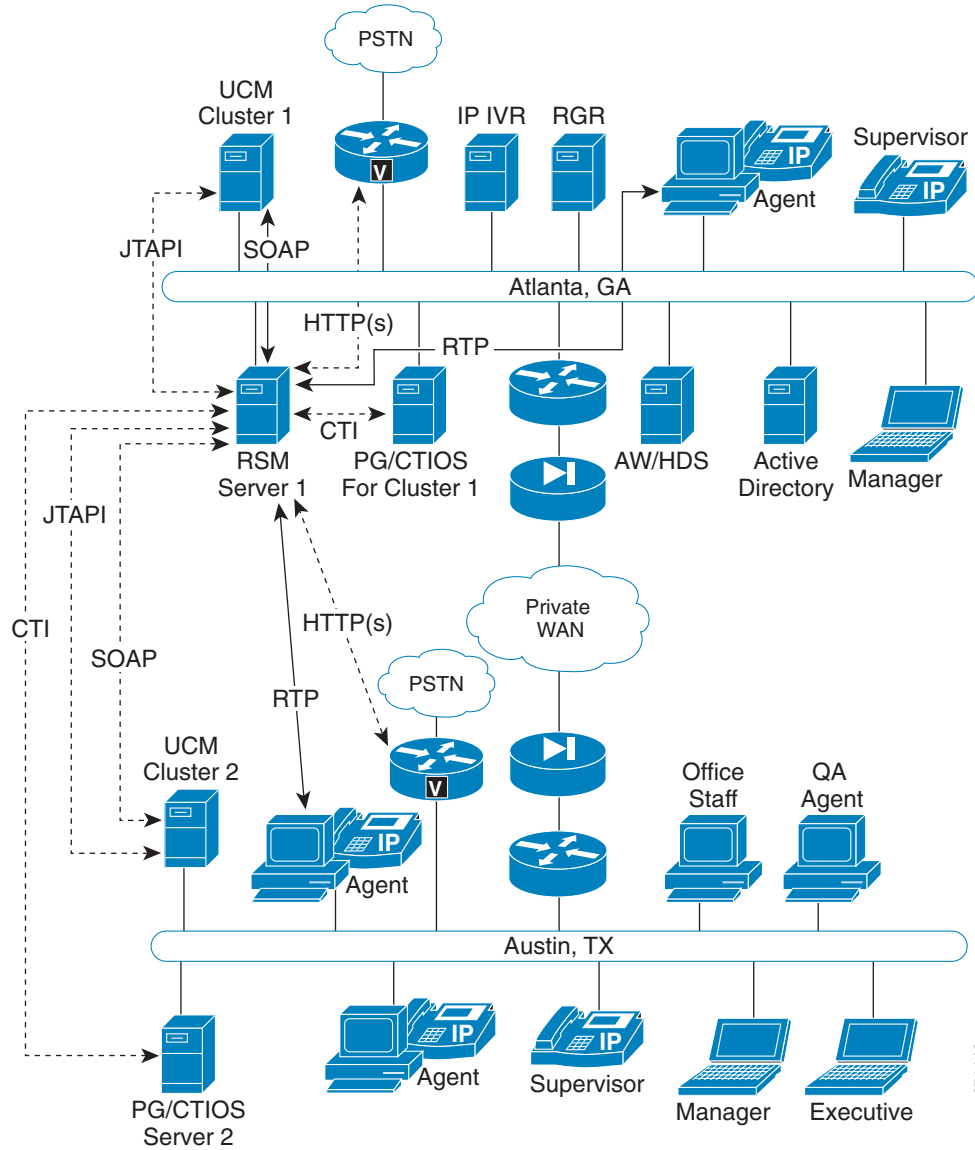


Figure 4-17 illustrates a Unified CM cluster as well as a Unified CVP VXML Gateway/voice gateway at each site. It is a combination of the previous deployment models, and it has the following characteristics:

- The Unified CVP Call Server controls the VXML Gateways at each site.
- Because there are agent phones at both sites, RTP data could be streamed either within the LAN at Atlanta (if the requested agent to monitor is in Atlanta) or across the WAN (if the requested agent is in Austin).

271443

- As with the previous multi-site, multi-cluster deployment, the RSM tracks the state of the entire enterprise. This means that a supervisor could dial in from either site (or anywhere in the world via PSTN) and listen to an agent in Atlanta or Austin.

Bandwidth Requirements

As part of the network planning done before deploying the RSM solution, you should verify that the network infrastructure can support the bandwidth requirements of RSM.

The RSM solution has connectivity with multiple components in the larger Cisco environment (as the diagrams in the previous section demonstrate). Table 4-4 lists these components, along with the nature of the data exchanged and the relative bandwidth requirements of that data. If RSM exchanges multiple types of data with a specific component, it is listed multiple times.

Table 4-4 Bandwidth Requirements

RSM Peer	Purpose	Protocol(s) Used	Data Format	Relative Bandwidth Requirements	Link Latency Requirements
VRU	Service Requests / Responses	TCP (HTTP)	Textual	Minimal	< 500 ms avg.
VRU	Requested Voice Data from PhoneSim to VRU	TCP (HTTP)	G711, chunked transfer mode encoding	High (about 67 to 87 kbps per session)	< 400 ms avg.
Unified CM	AXL for Phone DN to Device ID Translation	TCP (HTTP, SOAP)	Textual (XML)	Minimal	< 500 ms avg.
Unified CM	Issuance of Agent Phone Monitoring	TCP (JTAPI)	Binary (JTAPI stream)	Minimal	< 300 ms avg.
CTI OS Server (PG)	Environment Events / Supervisor Logins	TCP (CTI OS)	Binary (CTI OS stream)	Minimal (< 1000 agents) Moderate (> 1000 agents) (with 2000 agents, about 100 kbps)	< 300 ms avg.
Agent Phones	Simulated Phone Signaling	TCP or UDP (SIP)	Textual	Minimal	< 400 ms avg.
Agent Phones	Monitored Phone Voice Data	UDP (RTP)	Binary (G.711)	High (about 67 to 87 kbps per session)	< 400 ms avg.

Agent Phone Bandwidth Figures

Currently, the simulated phones on the RSM server support using only G.711 mu-law to monitor agent phones. This is primarily a limitation of the BiB (built-in-bridge) on the agent phone itself.

For bandwidth usage information, refer to the *Cisco Voice Over IP - Per Call Bandwidth Consumption* TechNote, available at

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml

Failover Redundancy and Load Balancing

Load balancing support is defined as the act of multiple RSM servers being associated together so that the incoming request load is distributed among them. The definition of failover is multiple RSM servers being associated together so that if one fails, the other(s) can act in its place. In the future, RSM will support load balancing and failover with both the Unified CVP and IP IVR VRUs. Currently, this support is not available in RSM 1.0. RSM 1.0 does, however, support the deployment of multiple standalone RSM servers within a single Unified CCE environment, and this concept is demonstrated in the advanced deployment scenarios described in this document.

Table 4-5 indicates how a failure of each of the various components affects a live supervisor call.

Table 4-5 *Impact of Failures on a Supervisor Call*

Component That Fails	Worst Possible Impact
VRU Node (IP IVR, Unified CVP)	Supervisor's call is terminated as any VRU failover occurs (depends). Supervisor may dial back in and log in again once VRU failover is complete and/or the original failed VRU is working again.
RSM Server (Hardware Failure)	Callers listening to a voice stream from the failed server will have the voice stream terminated and be returned to the main menu. Their next attempt to make a service request to the failed server (or a new callers first attempt to make such a request) will result in a configurable delay of 3 to 5 seconds or so, as the request times out and an error message is played. Furthermore, any action that attempts to contact the RSM server (for example, logging in, attempting to monitor an agent, and so forth), will fail, although the RSM callflow will still be answered because it is being hosted on the VRU node.
VLEngine or PhoneSIM software failure	Service automatically restarted via service wrapper. Supervisors with a request in-progress are given an error message and have a chance to retry their last action. During the time either service is not functioning, any action that attempts to contact the RSM server (for example, logging in, attempting to monitor an agent, and so forth), will fail, although the RSM callflow will still be answered because it is being hosted on the VRU node.

Table 4-5 *Impact of Failures on a Supervisor Call (continued)*

Component That Fails	Worst Possible Impact
Unified CCE fails (CTI OS)	RSM will lose connectivity to the CTI OS server when the PG fails or is cycled. If connectivity to both CTI servers on a cluster fails, RSM will keep retrying both, connecting to the first server that is available. (The CIL's failover code is used for all of this.) When connectivity comes back up to a CTI server, the agent and call lists will be cleared and refreshed (to avoid "stale" agents). During this time, no new call events will be received, and the system will be working from an "out-of-date" agent and call list. Therefore some monitoring requests will fail, saying the agent is not talking when he or she is, and some monitoring requests will fail because the system would think the agent is talking when he or she currently is not. This is believed to be preferable to the scenario where all cached data is deleted when the server goes down, in which case no monitoring would work.
Unified CM fails (JTAPI / AXL)	Connectivity to one or more JTAPI providers will be lost. RSM can be configured for connectivity to up to 2 JTAPI providers per-cluster. If this is the case and connectivity to either of the providers is lost, VLEngine will fail-over to the other provider if necessary, making it the active one and making its requests through it. If connectivity to both providers is lost, VLEngine will periodically retry both and re-establish the connectivity to the first that comes up. Attempts to monitor agents (for example, monitorAgent calls) made during this time will fail until the JTAPI connection is re-established.

Host-Level Security

Incoming access to the RSM server can be restricted to only the necessary components via the host-based Access Control List (ACL) functionality built into the Windows Server OS. In the most secure configuration, incoming access to the RSM system is permitted from the VRU systems. Built-in host-based access control can also be employed to allow limited access to other services if desired, such as remote administration mechanisms such as Windows Remote Desktop and VNC.

Even though this is not required, a recommended ACL Configuration for a single-server RSM configuration would be as follows:

Deny incoming access to all

Permit incoming TCP on port 8080 to each VRU node in the environment (VLEngine HTTP API Access)

Permit incoming TCP on port 29001 to each VRU node in the environment (PhoneSim HTTP API Access)

<Other rules for allowing remote administration (RDP/VNC) connectivity>

Cisco Security Agent

As part of the installation procedure, Cisco highly recommends that you install the Cisco Security Agent (CSA) software on the RSM system. This topic is covered in the Security Settings chapter of the *Cisco Remote Silent Monitoring Installation and Administration Guide*, available at <http://www.cisco.com>.

Transport or Session Level Security

Because RSM maintains multiple connections to a number of components in the larger Cisco Contact Center environment, there is no simple answer to whether transport or session level security is supported or not. The follow notes describe RSM's support for this feature by protocol type:

RSM to VRU (HTTP): Currently there is no support for encryption of the HTTP-based data exchange between RSM and the VRU node. Such support will be added in later versions for the VLEngine component only. This will allow all but one of RSM's HTTP-based API calls to be made over a HTTPS channel. The monitorAgent.jsp API request and the monitored agent voice data that is sent back as a response is implemented by the PhoneSim component, and HTTPS support is not planned for PhoneSim due to performance concerns. (The monitorAgent.jsp API call is documented in the API reference section.)

RSM to PG/CTI OS Server (CTI): Because RSM makes use of the Java CIL, all CTI OS servers used by it must be set up with security disabled. CTI OS traffic may be encrypted via the use of IPSec transport mode encryption. For more information, refer to the Security Settings chapter of the *Remote Silent Monitoring Configuration and Administration Guide*, available at <http://www.cisco.com>.

RSM to UCM (JTAPI): Like CTI OS traffic, JTAPI traffic may be encrypted via the use of IPSec transport mode encryption. For more information, refer to the Security Settings chapter of the *Remote Silent Monitoring Configuration and Administration Guide*, available at <http://www.cisco.com>.

RSM to UCM (AXL/SOAP): HTTPS is used for the connection to Unified CM's AXL service in all cases.

RSM to Agent Phone (RTP): The Unified CM 6.x and 7.0 call monitoring implementation does not currently include support for monitoring encrypted voice streams. Once it does, RSM will support it by default.

Support for Mobile Agent, IP Communicator, and Other Endpoints

Currently, the underlying Unified CM 6.x and 7.0 monitoring functionality does not provide monitoring support for endpoints using any one of the following:

- Cisco Mobile Agent
- Cisco IP Communicator
- Second generation or older phones, such as the Cisco Unified IP Phone 7940 or 7960
- A media-terminated CTI OS Agent Desktop
- Monitoring of encrypted phone calls

Therefore, support for these products is also not available through RSM. For further information on this restriction, see [Silent Monitoring, page 4-18](#).

Cisco Agent Desktop Presence Integration

Cisco Agent Desktop (CAD) agents and supervisors have long been able to communicate with each other via the chat services built into the desktop applications. Now, for customers who have deployed Cisco Unified Presence in their environments, agents and supervisors can use these same desktop applications to see the presence status of subject matter experts (SMEs) as well as other critical members of the enterprise and to initiate chat sessions with them. The subject matter experts use the familiar Cisco Unified Personal Communicator or IP Phone Messenger (IPPM) to initiate chat sessions with agents who

are configured as Unified Presence users and to respond to chat requests from them. Subject matter experts can also use Microsoft Office Communicator if Cisco Unified Presence is configured to support federated users.

For example, suppose that a customer calls a Cisco Unified Contact Center that has integrated Cisco Unified Presence with CAD. The customer's call is routed to an available agent. If the agent requires assistance in addressing the caller's needs, the agent can launch the contact selection window from the Agent Desktop toolbar. The contact selection window will display the presence status of other agents, supervisors, and subject matter experts who are assigned to the agent's work flow group. The agent can then select a contact who is available and can initiate a chat session with the contact. If appropriate, the agent can also use the contact selection window to conference a contact into the call, or even transfer the customer's call to the contact.

Figure 4-18 and the description that follows describe how various components of CAD and Cisco Unified Presence interface with each other.

Figure 4-18 Interface Between CAD and Cisco Unified Presence

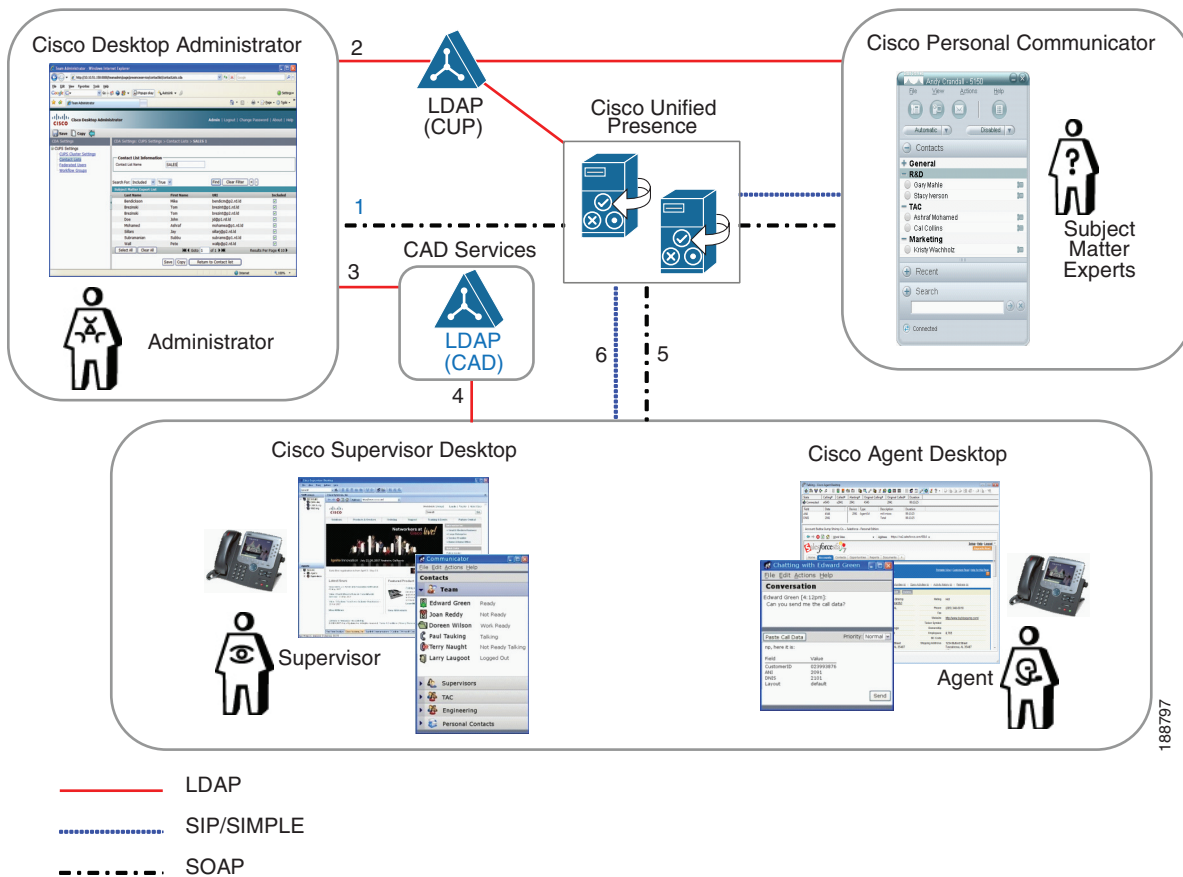


Figure 4-18 depicts the following sequence of events:

1. Cisco Desktop Administrator retrieves an LDAP configuration profile through the SOAP Interface.
2. Cisco Desktop Administrator binds to the LDAP server for SME searches and information (name, telephone number, and so forth).

3. The Administrator places SMEs in logical groups called contact lists and then assigns them to specific work flow groups. In this way, administrators can segment contact lists and ensure that only those agents assigned to a specific work flow group have visibility to the appropriate contact list. This configuration is saved in the CAD LDAP directory so that each agent/supervisor does not have to access the Cisco Unified Presence LDAP server, which might have limitations on the number of connections and other parameters. Administrators can also control whether SMEs can see the agent's presence state.
4. CAD retrieves the contact list associated with the agent's workflow group.
5. CAD retrieves various configuration profiles via the SOAP interface (for example, Cisco Unified Presence server information).
6. CAD sends a SIP REGISTER message to register with Cisco Unified Presence, followed by individual SIP SUBSCRIBE messages for each user in its contact list. CAD also sends a SIP SUBSCRIBE message for "user-contacts" for contacts configured on Cisco Unified Presence. A SIP NOTIFY message is received whenever a contact in the contact list changes state. CAD does not allow agents to change their presence states; it only sends a single SIP PUBLISH message to Cisco Unified Presence when the agent logs in.

Call control is done via the existing CAD main window call controls using CTI.

All SIP traffic and presence information sent between CAD and Cisco Unified Presence is not encrypted and is done via TCP or UDP.

Cisco Unified Presence 7.x can evenly assign the users registered with it across all nodes within the Cisco Unified Presence cluster. If a user attempts to connect to a node that is not assigned to him, CAD will connect to the SOAP and Cisco Unified Presence servers specified in redirect messages from the publisher.

Design Considerations

All communication between CAD agents and SMEs is via the Cisco Unified Presence server and is not routed through any CAD servers. For deployment guidelines, refer to the information on Cisco Unified Presence in the *Cisco Unified Communications SRND*, available at

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

NAT and Firewalls

This section discusses deploying Cisco Agent Desktop (CAD) and CTI Toolkit Desktop in an environment where two or more disjointed networks are interconnected using Network Address Translation (NAT).

For more information regarding NAT and firewalls, see the chapter on [Securing Unified CCE, page 8-1](#).

Cisco Agent Desktop and NAT

When the CAD desktop is deployed in a network environment where two or more disjointed networks are interconnected using NAT, the CAD Base Services must all be located on the same network. Network Address Translation (NAT) and Port Address Translation (PAT) are not supported between CAD Base Services servers. The CAD, CAD-BE, and Cisco Supervisor Desktop (CSD) applications support NAT and PAT but only over a VPN connection. Cisco Desktop Administrator (CDA) and Services Management Console (SMC) do not support NAT or PAT and must be installed on the same network as the CAD Base Services.

Firewalls are supported between the CAD services and desktop applications and between the desktop applications as long as the firewall allows the required type of traffic through and the appropriate ports are opened. Figure 4-19 shows the traffic types used between the CAD components.

For detailed port information, refer to the *Port Utilization Guide for Cisco ICM/IPCC Enterprise and Hosted Editions*, available at

http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html

Figure 4-19 Communication Between CAD Components

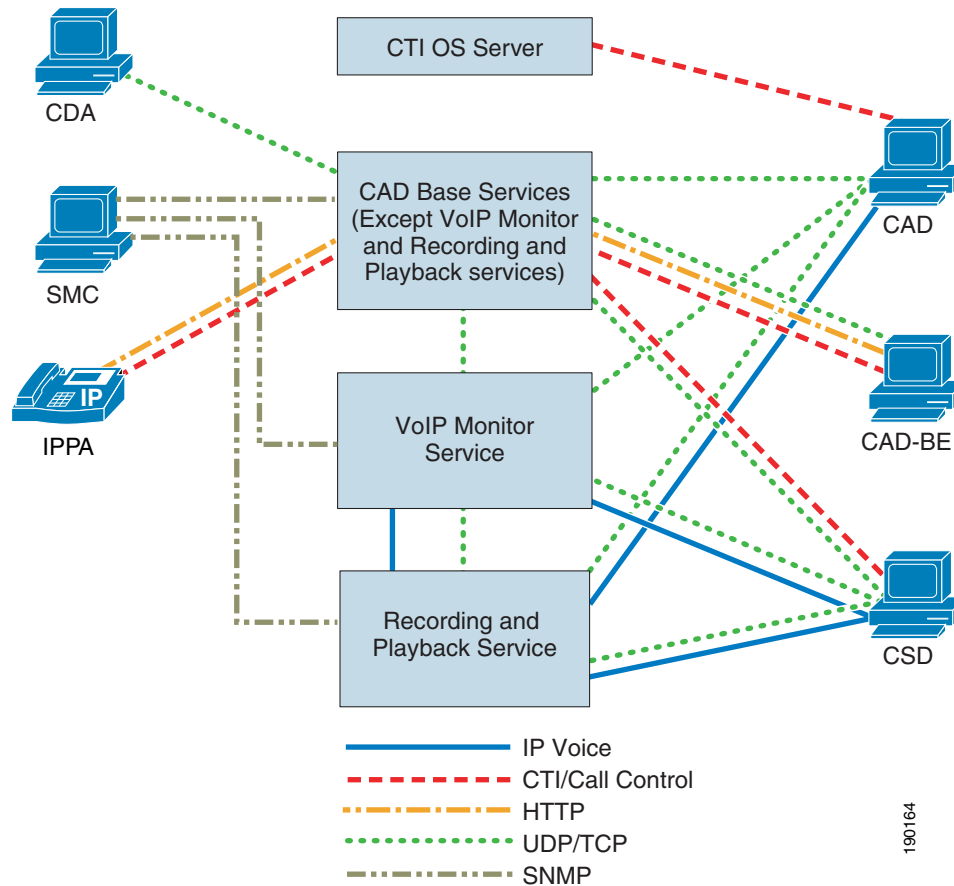


Figure 4-19 shows that IP voice streams are exchanged between the VoIP providers (CAD, the VoIP Monitor service, and the Recording & Playback service) and the VoIP requestors (CSD and the Recording & Playback service).

CTI and call control data (agent state, skill information, and call events) flow either from the CTI OS service (in the case of CAD) or from one or more of the CAD Base Services communicating directly with the CTI server (in the case of CAD-BE, CSD, and IPPA agents).

Note that, in the case of the IP Phone Agent XML service, the CTI information exchanged applies only for agent state changes requested by the agent using the IPPA application and for skill information displayed on the phone. Call control messages are still exchanged between the phone and Unified CM.

HTTP communication is performed between the SMC applet and the SMC servlet running on the CAD Base Services machine. HTTP is also the protocol used by the IPPA service and CAD-BE applet to communicate with the Browser and IP Phone Agent service.

The UDP/TCP traffic shown in the figure represent the socket connections used to exchange messages between servers and clients, which includes the CORBA connections used by most of the clients to request services and information from the servers.

The SMC servlet that runs on the CAD Base Services machine uses SNMP to gather status information on all the CAD services that are part of an installation.

CTI Toolkit Desktop and NAT

When the Cisco CTI Toolkit Desktop is deployed in a network environment where two or more disjointed networks are interconnected using NAT, then Unified CM, the physical IP Phone, the Cisco CTI OS Server, the Cisco CTI Toolkit Desktop, and the Cisco CTI OS IPCC Supervisor Desktop must be on the same network.

Co-Residency of CTI OS and CAD Services on the PG

Beginning with Cisco Unified CCE Release 7.0(0), Cisco recommends that you install CTI OS and CAD Services (including VoIP Monitor and Recording) on the PG. This does reduce the supported maximum agent capacity on the PG. If the supported PG capacity numbers provided in the chapter on [Sizing Unified CCE Components and Servers, page 10-1](#), are not sufficient and you want to run these software components on separate servers to increase agent capacity on the PG, then prior approval from the Unified CCE product management team is required.

Legacy deployments where CTI OS or CAD Services were previously installed on separate servers are still supported. However, customers are encouraged to migrate CTI OS and CAD Services onto the PG. For more information regarding deployment configurations, see the chapter on [Deployment Models, page 2-1](#).

Support for Mix of CAD and CTI OS Agents on the Same PG

Unified CCE deployments can support a mix of CAD and CTI OS agents on the same PG. If a mix is deployed, the sizing limitations of CAD apply. Note that Cisco Supervisor Desktop (CSD) can monitor only CAD agents, and the CTI OS supervisor application can monitor only CTI OS agents.

Support for IP Phones and IP Communicator

CAD, CAD-BE, and the CTI Toolkit Desktop support the use of Cisco IP hardware phones and/or the Cisco IP Communicator software phone.

Some CAD agent application features (CAD, CAD-BE, and IPPA) require particular phone models, and some installations support either hardware phones or software phones but not both. For information on the exact phone models and IP Communicator versions supported, refer to the CAD documentation available at <http://www.cisco.com>.

IP Phones and Silent Monitoring

Silent Monitoring of agents is supported using either IP hardware phones or the Cisco IP Communicator.

IP Phones and Mobile Agent

The Mobile Agent feature does not require any specific type of phone. Even analog phones can be used for this feature.

IP Phones and Citrix or MTS

Both the Cisco IP hardware phones and the Cisco IP Communicator are supported when using Citrix or MTS with either CAD or the CTI Toolkit desktops. In these environments, the Cisco IP Communicator must be installed on the Agent desktop PC and cannot be deployed on the Citrix or MTS server.

IP Phone Agent

The IP Phone XML service agent application supports only hardware IP phones because there is no desktop.

Miscellaneous Deployment Considerations

This section briefly describes the following additional deployment considerations:

Layer-3 Devices

Layer-3 network devices (routers and gateways) cannot exist between an agent's telephone device (hardware or software phone) and the switch port used by the VoIP Monitor service that is configured to capture voice packets for silent monitoring and recording. This restriction applies only if a VoIP Monitor is configured as the primary or backup service for capturing voice streams. If desktop monitoring is configured as the primary method (with no secondary method), this information does not apply.

Network Hubs

A network hub (including a "smart" hub) is not allowed between an agent's hardware phone and PC when Desktop Monitoring is configured for the agent.

Multiple Daisy-Chained Hardware Phones

There may be only a single hardware phone connected in series between the agent's PC and the switch when Desktop Monitoring is configured for the agent.

NDIS Compliance of NICs

The network interface cards (NICs) used by the VoIP Monitor services and on the agent's PC (when Desktop Monitoring is configured) must support promiscuous mode packet sniffing as stated. If the NIC card or driver does not support this functionality through the NDIS interface, the monitoring and recording feature will not work.

Encrypted Voice Streams

If the voice streams are encrypted using SRTP, silent the monitoring and recording feature will not work correctly. Although the voice streams can still be captured, they will not be decoded correctly. The end result is that the speech will be unintelligible.

High Availability and Failover Recovery

For detailed information about CAD and CTI Toolkit Desktop high availability, see the chapter on [Design Considerations for High Availability, page 3-1](#).

Bandwidth and Quality of Service

For detailed information about CAD and CTI Toolkit Desktop bandwidth usage and QoS, see the chapter on [Bandwidth Provisioning and QoS Considerations](#), page 12-1.

References to Additional Desktop Information

The following additional information related to Cisco Agent Desktop and Cisco Supervisor Desktop is available at the listed URLs:

- *CTI Compatibility Matrix*

Provides tables outlining Unified ICM Peripheral Gateway (PG) and Object Server (OS) support for versions of Cisco Agent Desktop, CTI OS Server, CTI OS Client, Data Collaboration Server (DCS), Siebel 6, and Siebel 7.

http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_technical_reference_list.html

- *Voice-Over IP Monitoring Best Practices Deployment Guide for CAD*

This document provides information about the abilities and requirements of Voice over IP (VoIP) monitoring for Cisco Agent Desktop (CAD). This information is intended to help you deploy VoIP monitoring effectively.

http://www.cisco.com/en/US/products/sw/custcosw/ps427/prod_technical_reference_list.html

- *Integrating CAD Into a Citrix MetaFrame Presentation Server or Microsoft Terminal Services Environment*

This document helps guide a Citrix administrator through the installation of Cisco Agent Desktop applications in a Citrix thin-client environment.

http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/cad_enterprise/cad_enterprise7_2/installation/guide/CADCitrixMTS.pdf

- *Cisco CAD Service Information*

This document provides release-specific information such as product limitations, service connection types and port numbers, configuration files, registry entries, event/error logs, error messages, and troubleshooting.

http://www.cisco.com/en/US/products/sw/custcosw/ps427/prod_technical_reference_list.html

