



CHAPTER 1

Overview

The Cisco Unified Application Environment is a development and runtime platform designed for creating, deploying, and executing converged voice and data applications. It is integrated with Cisco Unified Communications Manager and Cisco Unified Presence.

This chapter includes these topics:

- [Understanding the Cisco Unified Application Environment, page 1-1](#)
- [Understanding the Deployment of the Cisco Unified Application Environment, page 1-4](#)

Understanding the Cisco Unified Application Environment

This section includes these topics:

- [Supported Application Development IP Telephony Functions, page 1-1](#)
- [Supported Application Development and Deployment Technologies, page 1-2](#)
- [Cisco Unified Application Environment Components, page 1-2](#)

Supported Application Development IP Telephony Functions

The Cisco Unified Application Environment can be used to create applications supporting the following IP telephony functions:

- Presence
- Mobility
- Recording
- Paging
- Conferencing
- Speech-enabled applications
- IP phone services
- Other voice and data converged applications

Supported Application Development and Deployment Technologies

It supports these application development and deployment technologies:

- Telephony call control: Session Initiation Protocol (SIP), H.323, Skinny Call Control Protocol (SCCP), and Computer Telephony Integration (CTI)
- Java Telephony Application Programming Interface (JTAPI)
- Other telephony protocols: Cisco Unified IP Phone Services, DeviceListX, AXL-SOAP, Extension Mobility, and other Cisco Unified Communications Manager APIs
- Data services and protocols: Web Services, HTTP, Lightweight Directory Access Protocol (LDAP), Structured Query Language (SQL), Simple Mail Transfer Protocol (SMTP)
- Media processing capabilities: Integrated voice response (IVR), conferencing, transcoding, text-to-speech, speech recognition, speaker verification
- Extensible plug-in framework that customers and partners can use to add support for any standards-based or proprietary protocol or interface

Cisco Unified Application Environment Components

The Cisco Unified Application Environment enables you to:

- Perform flexible deployment of Cisco Unified Application Servers and Cisco Unified Media Engines by determining the appropriate number and configuration of servers at the time of deployment.
- Avoid latency and bandwidth issues, by allowing you to distribute Cisco Unified Media Engines closer to the media endpoints used for a particular application, as they may generate considerable Real-time Transport Protocol (RTP) traffic.

The Cisco Unified Application Environment is made up of these components:

- [Cisco Unified Application Server, page 1-2](#)
- [Cisco Unified Media Engine, page 1-3](#)
- [Cisco Unified Application Environment Developer Tools, page 1-3](#)

Cisco Unified Application Server

The Cisco Unified Application server is supported on Cisco Media Convergence Servers (MCS). For a list of supported servers, see *Cisco Unified Application Environment Hardware Compatibility Matrix* listed in [“Related Documentation” section on page xii](#).

The Cisco Unified Application Server provides these functions:

- Originates and receives calls over various IP telephony protocols.
- Provides application management.
- Starts, executes, manages, and terminates application scripts that are operating in their own runtime environment.

- Hosts protocol providers that provide an interface to applications for systems outside the application environment.
- Controls Cisco Unified Media Engines to process, mix, analyze, and route digital audio data.

**Note**

To serve as an application and runtime platform, each Cisco Unified Application Environment deployment must contain at least one Cisco Unified Application Server.

Cisco Unified Media Engine

The Cisco Unified Media Engine is a software-only server which provides media processing capabilities for applications that are developed using the Cisco Unified Application Designer. It runs on the Cisco MCS. For a list of supported servers, For a list of supported servers, see *Cisco Unified Application Environment Hardware Compatibility Matrix* listed in “[Related Documentation](#)” section on page xii.

If the applications do not have any media components, a Cisco Unified Media Engine is not required.

**Note**

Each Cisco Unified Media Engine is controlled by one or more Cisco Unified Application Servers.

New Media Features

Three new media features — Seek, Pause, and Resume are added.

Seek

The SeekAndPlay API allows you to play the media file from a specified position. You must mention the position of the file (in seconds), audio sample size, and bit rate.

**Note**

The Seek feature supports only the .wav file format and can be used only with a single audio file.

Pause and Resume

The Pause feature allows you to stop playing a media file that is started using either Play or SeekAndPlay API.

The Resume feature allows you to start playing the media file from the position where it was paused.

The Pause and Resume features use the existing Cisco Unified Application Environment features and SeekAndPlay API.

Cisco Unified Application Environment Developer Tools

Each one of these Cisco Unified Application Environment Developer tools enable you to create and deploy applications:

- Cisco Unified Application Designer

The Cisco Unified Application Designer is a PC-based client application which runs on Microsoft Windows XP Professional and Windows Server 2003. It is a visual Integrated Development Environment (IDE) which allows application designers to:

- Develop applications that combine voice with enterprise applications and data.
- Install applications directly from the PC or build an application package file.

- Load application package files developed with the Cisco Unified Application Designer through the Cisco Unified Application Environment Administration.
- Etch

Etch is a framework for building, exposing, and consuming network services in a language- and platform-neutral way. Using Etch and the CUAE command-line tool you can create applications and plugins using your language of choice. The CUAE command-line tool also enables you to install, package, remove, and update applications.

For more information about Etch, see the *Application Developer Getting Started Guide* at this URL: http://www.cisco.com/en/US/docs/voice_ip_comm/cuae/2_5/english/developer/getting_started/guide/CUAE_Getting-Started_Book-Wrapper.html.

Understanding the Deployment of the Cisco Unified Application Environment

This section includes these topics:

- [Deployment Topologies, page 1-4](#)
- [Understanding Network Port Usage, page 1-8](#)
- [Running 3rd-Party Platform Agents, page 1-11](#)
- [Utilizing Cisco Security Agent, page 1-13](#)

Deployment Topologies

The Cisco Unified Application Environment supports a variety of deployment topologies that incorporate Cisco Unified Application Servers and Cisco Unified Media Engines, and integrate them with one or more Cisco Unified Communications Manager clusters.

The deployment topology strategy should be based on scalability, redundancy, and networking requirements. This section describes these common topologies:

- [Single Cisco Unified Application Server with a Single Cisco Unified Communications Manager Cluster, page 1-4](#)
- [Single Application Server with Multiple Cisco Unified Communications Manager Clusters, page 1-5](#)
- [Single Cisco Unified Application Server Controlling Multiple Cisco Unified Media Engines with Multiple Cisco Unified Communications Manager Clusters, page 1-6](#)
- [Multiple Application Servers Controlling Multiple Media Engines with Multiple Cisco Unified Communications Manager Clusters, page 1-7](#)

Single Cisco Unified Application Server with a Single Cisco Unified Communications Manager Cluster

In this topology, a single physical server operates as a Cisco Unified Application Server or combined Cisco Unified Application Server and Cisco Unified Media Engine, and is integrated with a single Cisco Unified Communications Manager cluster ([Figure 1-1](#)). This configuration is appropriate when the following conditions apply:

- The Cisco Unified Application Environment must support a single Cisco Unified Communications Manager cluster.
- Fewer than 480 simultaneous media streams are required, and the projected amount of media stream traffic between IP endpoints (IP phones, H.323/MGCP gateways, Music on Hold (MOH) servers, and hardware and software conference bridges) and the media engine is not expected to add excessive network load.

**Note**

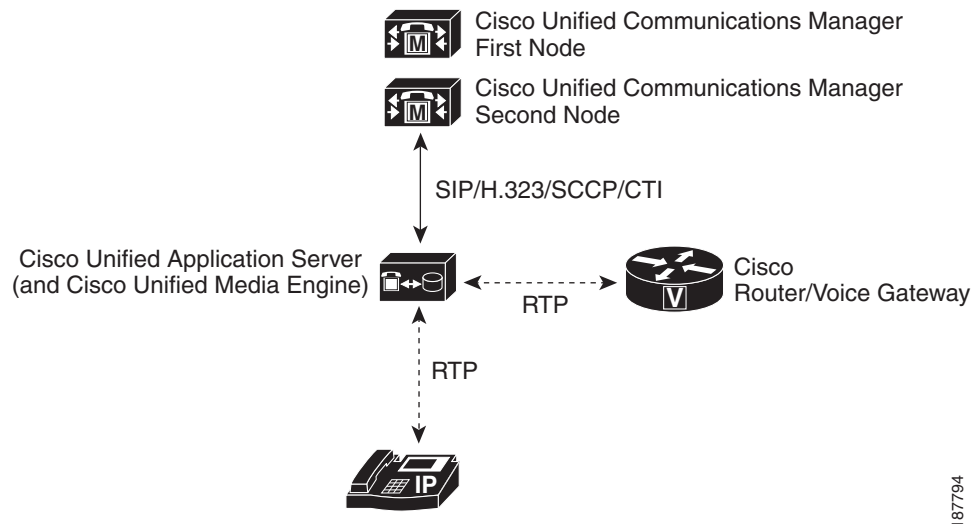
These recommendations are approximations devised from performance testing on high-capacity MCS servers. If multiple applications involve heavy conferencing, recording and playing, low bit-rate codecs, or CPU-intensive activity, fewer simultaneous media streams are supported. It is likely that using low-capacity servers also reduces the number of supported streams; however, no data for low-capacity servers is available at this time.

**Note**

Network traffic loads are impacted only with applications that require media.

- Redundancy is not required for the Cisco Unified Application Server or Cisco Unified Media Engine.

Figure 1-1 *Single Cisco Unified Application Server with a Single Cisco Unified Communications Manager Cluster*



187794

Single Application Server with Multiple Cisco Unified Communications Manager Clusters

In this topology, a single physical server operates as a Cisco Unified Application Server or combined Cisco Unified Application Server and Cisco Unified Media Engine and is integrated with multiple Cisco Unified Communications Manager clusters (Figure 1-2). This configuration is appropriate when these conditions apply:

- The Cisco Unified Application Environment must support multiple Cisco Unified Communications Manager clusters.

- Fewer than 480 simultaneous media streams are required and the projected amount of media stream traffic between IP endpoints (IP phones, H.323/MGCP gateways, Music on Hold (MOH) servers, and hardware and software conference bridges) and the media engine is not expected to add excessive network load.

**Note**

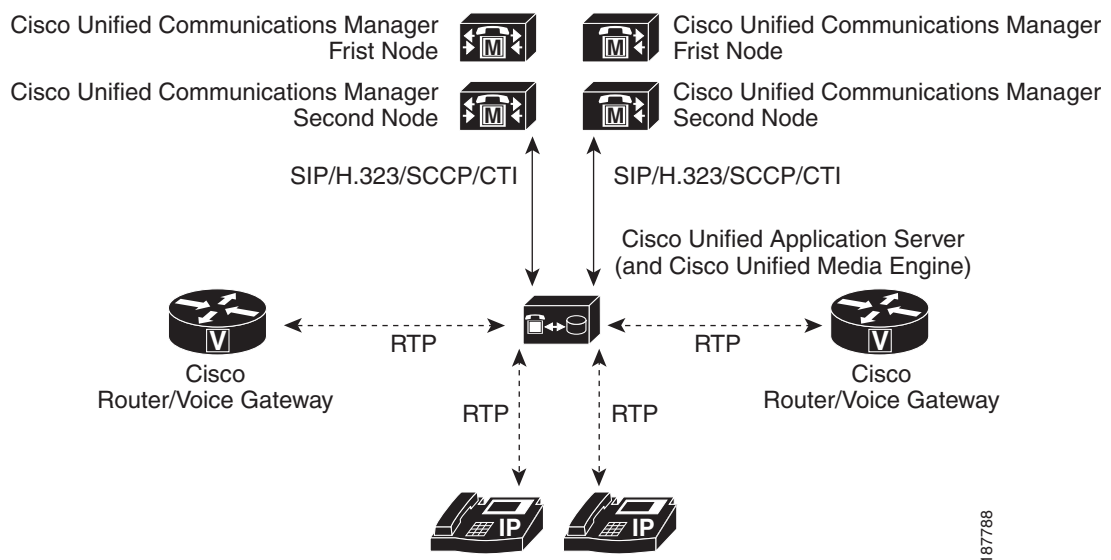
These recommendations are approximations devised from performance testing on high-capacity MCS servers. If multiple applications involve heavy conferencing, recording and playing, low bit-rate codecs, or CPU-intensive activity, fewer simultaneous media streams are supported. It is likely that using low-capacity servers also reduces the number of supported streams; however, no data for low-capacity servers is available at this time.

**Note**

Network traffic loads are impacted only with applications that require media.

- Redundancy is not required for the Cisco Unified Application Server.

Figure 1-2 Single Cisco Unified Application Server with Multiple Cisco Unified Communications Manager Clusters



Single Cisco Unified Application Server Controlling Multiple Cisco Unified Media Engines with Multiple Cisco Unified Communications Manager Clusters

In this topology, a single Cisco Unified Application Server controls multiple Cisco Unified Media Engines and is integrated with multiple Cisco Unified Communications Manager clusters (Figure 1-3).

**Note**

To avoid latency and bandwidth issues, it is recommended that you distribute Cisco Unified Media Engines close to the media endpoints used for a particular application.

This configuration is appropriate when these conditions apply:

- The Cisco Unified Application Environment must support multiple Cisco Unified Communications Manager clusters.
- More than 480 simultaneous media streams are required and the projected amount of media stream traffic between IP endpoints (IP phones, H.323/MGCP gateways, Music on Hold (MOH) servers, and hardware and software conference bridges) and the media engine could potentially add excessive network load across WAN links.



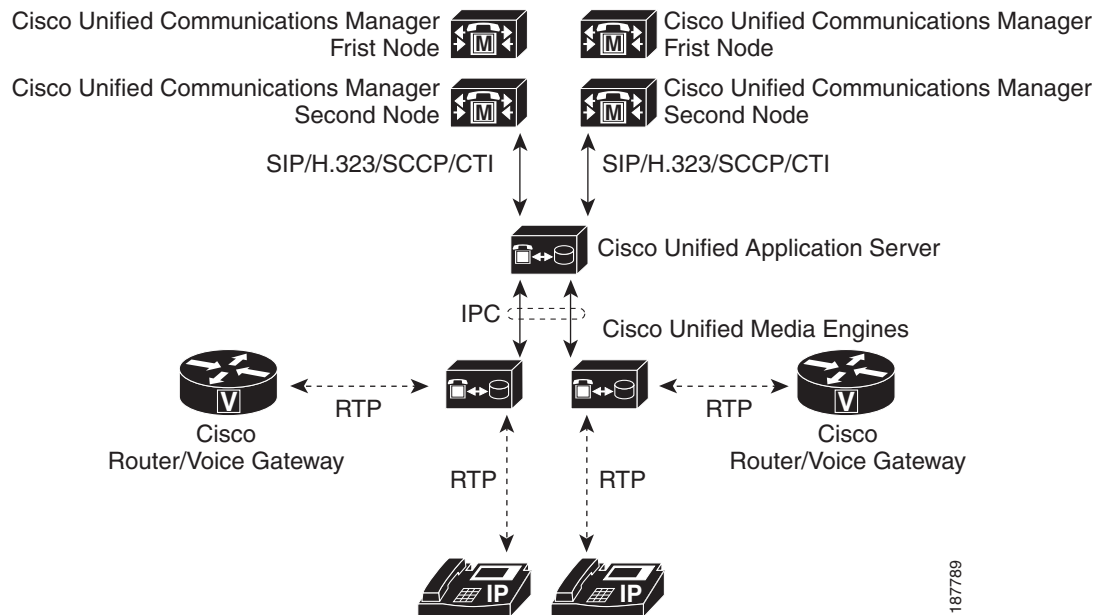
Note This is applicable only on high-capacity MCS servers, and is an approximation. If multiple applications involve heavy conferencing, recording and playing, low bit-rate codecs, or CPU-intensive activity, fewer simultaneous media streams are supported.



Note Network traffic loads are impacted only with applications that require media.

- When there is no redundant Cisco Unified Application Server, then application processing beyond the capabilities of one Cisco Unified Application Server is needed.
- Either redundancy or over 480 streams of media is required for the Cisco Unified Media Engine.

Figure 1-3 *Single Cisco Unified Application Server with Multiple Cisco Unified Media Engines, and Multiple Cisco Unified Communications Manager Clusters*



Multiple Application Servers Controlling Multiple Media Engines with Multiple Cisco Unified Communications Manager Clusters

In this topology, multiple application servers control multiple media engines and are integrated with multiple Cisco Unified Communications Manager clusters (Figure 1-4). This configuration is appropriate when these conditions apply:

- The Cisco Unified Application Environment must support multiple Cisco Unified Communications Manager clusters.
- More than 480 simultaneous media streams are required, or the projected amount of media stream traffic between IP endpoints is expected to add significant network load.

**Note**

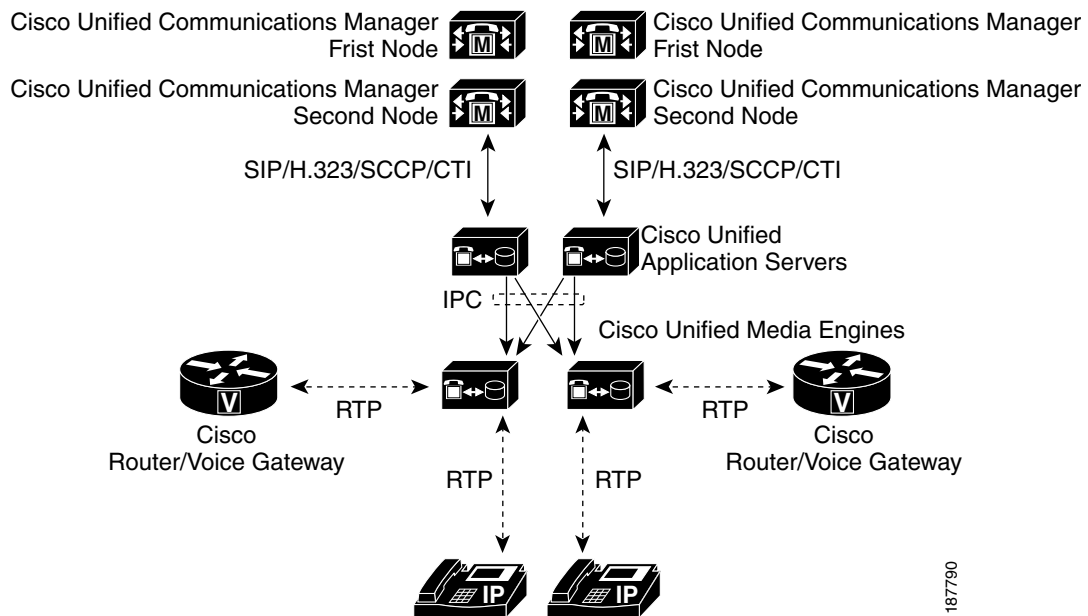
This is applicable only on high-capacity MCS servers, and is an approximation. If multiple applications involve heavy conferencing, recording and playing, low bit-rate codecs, or CPU-intensive activity, fewer simultaneous media streams are supported.

**Note**

Network traffic loads are impacted only with applications that require media.

- Redundancy is required for the Cisco Unified Application Server and Cisco Unified Media Engine.

Figure 1-4 Multiple Application Servers, Multiple Media Engines, Multiple Cisco Unified Communications Manager Clusters



Understanding Network Port Usage

This section lists the network ports used by the Cisco Unified Application Environment and provides detailed information about ports that accept only local connections and also ports that must accept remote connections.

Cisco Unified Application Environment default installations require certain ports to be opened in surrounding firewalls that restrict network connectivity to the Cisco Unified Application Server or Cisco Unified Media Engine.

Port Usage

This section specifies the ports used by components of the Cisco Unified Application Environment. [Table 1-1](#) lists the ports used by the Cisco Unified Application Server. [Table 1-2](#) lists the ports used by the Cisco Unified Media Engine.

Depending on how you configure your environment, some of the ports listed in [Table 1-1](#) and [Table 1-2](#) do not need to be opened. For example, if the Cisco Unified Application Server and Cisco Unified Media Engine are co-located, you do not need to open ports required for communication between those components. Also, if the port number is listed as Local in [Table 1-1](#) and [Table 1-2](#), the port does not need to be opened in a firewall; Local ports are used for local communication only between services on the Cisco Unified Application Server.



Note

This section does not list any ports used for remote OS administration, such as VNC/Terminal Services or for additional IP telephony applications deployed on the Cisco Unified Application Server.

Table 1-1 **Application Server Port Usage**

Port Number	Protocol	Usage	Configurable?
Remote:22	TCP	SFTP for Application and Media Deployment Required for application media deployment from Application Server to Media Engine. Also used for Application Designer to deploy applications directly to the Application Server.	No
Remote: 25	TCP	SMTP Required for sending e-mail alarms over SMTP. If you do not use SMTP alarm management, this port does not need to be opened for external communication.	Yes
Remote:80 (or 443)	TCP	HTTP for Web Management (port 443 if HTTPS) Required for communication with the Application Server. Used to administer the system. Port 80 is used by default, but if SSL is configured, then port 443 will be used.	No
Remote:161	UDP	SNMP Required for remote monitoring of Cisco Unified Application Environment resource usage and general server statistics. Cisco Unified Application Environment also uses this port to retrieve information from Cisco Unified Communications Manager via Cisco DeviceListX.	No
Remote:1720	TCP	H.225 Signaling for H.323 Required for communication via H.323. More specifically, this port is used for H.225 signaling for H.323. If H.323 is not being used for inbound calls, then remote access to this port is not required.	No
Remote:5060	UDP/ TCP	SIP Required for communication via SIP. If SIP is not being used, then remote access to this port is not required.	No

Table 1-1 Application Server Port Usage (continued)

Port Number	Protocol	Usage	Configurable?
Remote:8000	TCP	HTTP for Applications Required for Application Server communication if any applications use HTTP to expose events. Do not change this port number.	Yes, however, this port number should not be changed.
Remote:8120	TCP	Application Server: Management Required for Application Server for remote access only if applications are being deployed directly from the Cisco Unified Application Designer.	No
Remote:8130	TCP	Application Server: Application Debugging Required for Application Server if developers using the Cisco Unified Application Designer wish to use the Remote Debugging feature.	Yes
Remote:8140	TCP	Application Server: Remote Log View Required for Application Server if developers using the Cisco Unified Application Designer wish to use the remote log feature, or if administrators and/or developers wish to use the rconsole remote console tool.	Yes
Remote:9000	TCP/ TLS	This port is required to be open for the Etch Bridge to communicate with applications and plugins.	Yes
Remote:9001	TCP/ TLS	This port is required to be open for the Management Service to communicate with the Cisco Unified Application Environment Administration interface and the CUAЕ command-line tool.	Yes
Remote:9090	TCP	Application Server: Cluster Interface Required for Application Servers within a cluster to communicate. This port number is not configurable. Remote access is required if redundancy is configured.	No
Remote: 9530	TCP	Required for Application Server to communicate with a remote Media Engine.	No
Remote:10000-11000	TCP	H.245 Signaling for H.323 Required for communication via H.323. More specifically, this port is used for H.245 signaling for H.323. If H.323 is not being used for inbound calls, then this range of ports does not require remote access.	Yes
Local:3306	TCP	MySQL If there are multiple Application Server nodes in one cluster, this port must be opened for communication between Application Servers. Not required for a co-located Application Server and Media Engine deployment. This port number should not be changed.	Yes, however this number should not be changed.
Local:9434	TCP	Application Server: Apache Interface	No
Local:8400	TCP	Log Server	No
Local:9200	TCP	StatsService: Management	No
Local:9201	TCP	StatsService: Publishing	No

Table 1-1 **Application Server Port Usage (continued)**

Port Number	Protocol	Usage	Configurable?
Local:9202	TCP	StatsService: Queries	No
Local:8500	TCP	H.323 Service	No
Local:9500	TCP	SIP Service	No
Local:9100	TCP	JTAPI 4.0 Service	No
Local:9110	TCP	JTAPI 4.1 Service	No
Local:9120	TCP	JTAPI 3.3 Service	No
Local:9130	TCP	JTAPI 4.2 Service	No
Local:9140	TCP	JTAPI 5.0 Service	No
Local:9150	TCP	JTAPI 5.1 Service	No
Local:9160	TCP	JTAPI 6.0 Service	No
Local:9170	TCP	JTAPI 6.1 Service	No
Local:9180	TCP	JTAPI 7.0 Service	No

Table 1-2 **Media Engine Port Usage**

Port Number	Protocol	Usage	Configurable?
Remote:22	TCP	SFTP for Application and Media Deployment. Required for application media deployment from Application Server to Media Engine. Also used for Application Designer to deploy applications directly to the Application Server.	No
Remote:80 (or 443)	TCP	HTTP for Web Management (port 443 if HTTPS). Required for communication with the Media Engine. Used to administer the system. Port 80 is used by default, but if SSL is configured, then port 443 will be used.	No
Remote: 4904	TCP	Speech recognition server	Yes
Remote:9530	TCP	Application Server control channel. Required for remote Application Server and Media Engine communication.	No
Remote:20480-32768	UDP	This is the range of ports used for RTP Media.	Yes
Remote: 27000	TCP	Speech Recognition server licensing	Yes
Local:1070-1073	TCP	Dialogic HMP	No
Local:2812-2818	TCP	Dialogic HMP	No
Local:7000-7001	TCP	VT Server Text-to-Speech	No

Running 3rd-Party Platform Agents

This section describes the Cisco Unified Application Environment policy on the use of 3rd-party platform agents.

Overview

Cisco engineers test the Cisco Unified Application Environment on specific hardware, operating system, and software configurations to maximize predictability and stability in customer deployments. Platform agents, also called onboard agents, on-box agents, or co-resident agents, are third-party applications that reside on the same hardware and operating system as Cisco Unified Application Environment products and interact with it to provide a desired function. Examples include virus protection and system management applications.

Cisco understands that certain customers want to use platform agents with Cisco Unified Application Environment as part of their operations strategy. Please note the following:

- The Cisco Technology Developer Program offers third-party technology integration (including agents) support with Cisco Unified Communications products. You should encourage your agents' vendors to join this program for deployment success. More information is available at: <http://www.cisco.com/web/partners/pr46/tdp/index.html>.
- Cisco performs "best effort or passive" testing of select agents from vendors that are not in the Cisco Technology Developer Program. For these agents, no agent-specific "test to fail" or "test to verify" tests are performed, but if standard Cisco testing succeeds with the agents loaded on select representative releases, support is claimed. In other words, not all combinations of agent versions with Cisco versions are explicitly tested (including regression), and application notes are updated less frequently. Agents are supported only on specific versions of Cisco Unified Application Environment running on the IP telephony (Windows) OS that Cisco provides.
- Installing agents with Cisco Unified Application Environment may affect functions and performance. Cisco or third-party labs have verified interoperability for the agents and versions listed for a single-agent scenario only. Multiple agents deployed together are not tested, so these deployments may experience additional effects on function and performance.
- If you are running Cisco Security Agent, you must disable Cisco Security Agent before installing any of the Cisco Unified Application Environment components or other 3rd party platform agents.
- The Cisco Technical Assistance Center (TAC) provides coordinated support for customers who install supported third-party platform agents with Cisco Unified Application Environment. If the root cause of a problem is with the third-party agent, Cisco TAC might ask you to remove a supported platform agent or to consult the third party.

Support Policies for 3rd-Party Software

Cisco support policy is that customers can deploy third-party software on the Cisco Unified Application Environment for the following purposes:

- Virus-scanning software
- Backup and restore
- Monitoring
- Security

However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with Cisco Unified Application Environment before the products are deployed, to mitigate the risk of problems being discovered within the production environment between Cisco Unified Application Environment and the third-party products loaded on the Cisco Unified Application Environment server.

If a customer calls Cisco TAC with a problem, a Cisco TAC engineer may require that such third-party software be turned off or even removed from the Cisco Unified Application Environment server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and Cisco Unified Application Environment was the root cause of the problem, then the third-party software will be required to be disabled or removed from the Cisco Unified Application Environment server until such time that the interoperability issue is addressed, so that the customer can continue to have a functional Cisco Unified Application Environment system.

Before installing any qualified Microsoft service pack on the Cisco Unified Application Environment server, confirm that the manufacturer of any optional third-party software or hardware that you are using also supports the service pack for use with its product.

**Note**

In general, you should not apply Microsoft updates unless instructed by TAC. You can apply the Cisco-provided SRs, which contain Microsoft updates, but have been tested by the Cisco OS team.

Utilizing Cisco Security Agent

This section describes how the Cisco Unified Application Environment utilizes the Cisco Security Agent for intrusion detection and prevention and how you can request the Cisco Unified Application Environment CSA Policy.

Overview

The Cisco Security Agent provides Windows platform security that is based on a tested security rules set—called a “policy”—which has rigorous levels of host intrusion detection and prevention. It controls system operations by adhering to the rules set to allow or deny specific system actions before system resources are accessed.

In Cisco Security Agent, security rules are grouped into containers called rule modules. Rule modules are then attached to a policy. A policy is attached to a group. The host systems are associated with one or more groups.

For more information about the Cisco Security Agent, such as Release Notes and other documentation, see the Cisco Security Agents support information page on Cisco.com:

<http://www.cisco.com/en/US/partner/products/sw/secursw/ps5057/index.html>

Management Center for Cisco Security Agents

The CSA profile for the Cisco Unified Application Environment uses a static security policy. As such, additional 3rd party applications deployed to the application server may not function properly with the base Cisco Unified Application Environment CSA profile. Contact the application developer for additional rule modules and policies required to make that application function with CSA.

To add, change, delete, or view policies you must purchase and install the fully-managed console product, Management Center for Cisco Security Agent.

If you have the Management Center for Cisco Security Agent and want access to the Cisco Unified Application Environment security policy, contact Cisco TAC.

Backward Compatibility

Cisco Unified Application Environment 8.5 supports the following core APIs by integrating with Unified CM, Cisco Unified Presence, and Cisco Unified Messaging:

- Call control
- Presence
- Messaging

Before you implement Cisco Unified Application Environment 8.5, you must ensure that it can interoperate with the following applications:

- Cisco Unified Communications Manager
- Cisco Unified IP Phones
- Cisco Unified Presence
- Cisco Unified Messaging (Unity & Unity Connection)

Cisco Unified Communications Manager

Cisco Unified Application Environment 8.5 is backward compatible with the following Unified CM versions:

- Unified CM 4.x
- Unified CM 5.x
- Unified CM 6.x
- Unified CM 7.x
- Unified CM 8.0(1)
- Unified CM 8.5(1)

Cisco Unified IP Phones

To support Cisco Unified IP Phone 6900 Series, Cisco Unified IP Phone 8900 Series and Cisco Unified IP Phone 9900 Series, the JTAPI Service component of the Cisco Unified Application Environment system has been modified. To support the new APIs, changes have been made to Cisco Unified Application Designer, Etch, Telephony Manager, JTAPI Provider and JTAPI Service.

Cisco Unified IP Phones 8900 and 9900 Series Device Family

Cisco Unified Application Designer and Etch support the new Cisco Unified IP Phone 8900 Series and Cisco Unified IP Phone 9900 Series phone features. This allows the Cisco Unified Application Designer and Etch Developers to develop applications using JTAPI APIs. Cisco Unified Application Environment supports CTI call control on Cisco Unified IP Phone 6900, 8900, and 9900 series phones. This includes support for new JTAPI APIs for Join and Direct Transfer. The following APIs are supported:

Join/Join Across Lines

Enables calls on different phone lines to be joined and can also be used to create a conference. You can use the JTAPI Conference API to support this feature. Cisco Unified IP Phone 8900 and 9900 series phones do not have a Common Transfer Controller, but Cisco Unified IP Phones 6900 Series phones do have a Common Transfer Controller.

Direct Transfer/ Direct Transfer across Lines

Enables two calls on different addresses of the same terminal to be transferred by using the Transfer soft key on the phone or the Transfer API that is provided by JTAPI. This feature uses the JTAPI Transfer API which accepts Call Object as input.

Explicit Cancel

Explicit Cancel feature allows users to cancel a pending consultation transfer or conference. The held and active call remains, but the transfer/conference operation gets cancelled.

- Explicit Cancel results in a new event to be sent to applications
- Explicit Cancel is applicable only to Cisco Unified IP Phone 8900 and 9900 Series
- CiscoCallFeatureCancelledEv is delivered when CANCEL operation is invoked.
- Cisco Unified Application Environment does not need to handle this particular event.

Cisco Unified Presence

Applications developed using Cisco Unified Application Environment Presence APIs use the Cisco Unified Application Environment Presence plug-ins and reciprocate SIP stack to communicate with the Cisco Unified Presence Server. The communication between Cisco Unified Application Environment Presence and Cisco Unified Presence is based on the SIP SIMPLE interface and the SUBSCRIBE NOTIFY framework. Cisco Unified Application Environment Presence subscribes to Cisco Unified Presence for status changes. Whenever the status of the presentities changes, Cisco Unified Application Environment triggers the application and provides the details of the change. Using the Presence APIs, a Cisco Unified Application Environment application monitors the real time status changes of different presence entities.

Cisco Unified Application Environment 8.5 supports the following presence APIs:

- **TriggeringSubscribe**—Subscribes to Cisco Unified Presence Server to receive the presence status changes of presentities. Once, the application subscribes to this API, it receives a Notify event that initiates a new script whenever the presence status of the watched entities changes.
- **NonTriggeringSubscribe**—Subscribes to Cisco Unified Presence Server to receive the presence status changes of presentities. After the application subscribes to this API, it receives a 'Notify' event whenever the presence status of the watched entities changes. The event will be received only by the script that initiated the 'NonTriggeringSubscribe' and when the script is running.
- **Unsubscribe**—Removes the subscription from Cisco Unified Presence Server to receive the presence status changes of presentities.
- **SubscriptionTerminated**—Indicates the application that the subscription is terminated. This event occurs when the 'Unsubscribe' API is called or when the subscription is terminated by the Cisco Unified Presence server.
- **Notify**—Indicates the application that the presence status of at least one presentity has changed. This event contains a string which stores the data about status changes. The data is stored in XML format. The application can read the data using the 'PresenceNotification' native types.
- **PresenceNotification**—A complex data type that parses the XML data in a format that is usable by the C# processing.

Cisco Unified Messaging (Unity and Unity Connection 8.0)

Cisco Unified Application Environment interoperates with the following Unity/Unity Connection versions:

- Unity 7.x and 8.0(1)
- Unity Connection 7.x and 8.0(1)

