

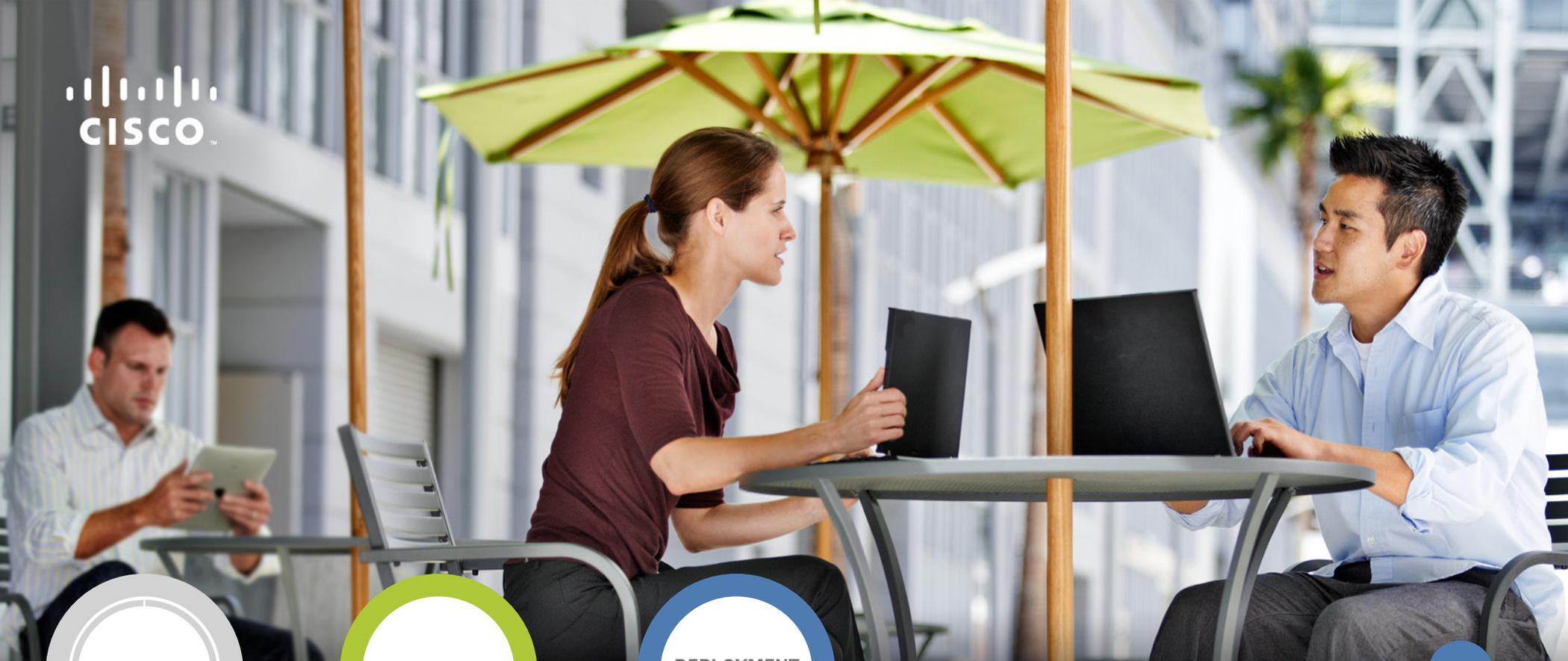


# Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to <http://www.cisco.com/go/sba>

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.





# VCS and UCM Video Integration Deployment Guide

● ● ● SMART BUSINESS ARCHITECTURE

August 2012 Series

# Preface

## Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

## Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

**month year** Series

For example, the series of guides that we released in August 2012 are the “August 2012 Series”.

You can find the most recent series of SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

## How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100  
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
ip address 10.5.204.5 255.255.255.0
```

## Comments and Questions

If you would like to comment on a guide or ask questions, please use the [SBA feedback form](#).

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

# Table of Contents

<b>What's In This SBA Guide</b> .....	1	<b>Appendix A: Product List</b> .....	43
Cisco SBA Collaboration.....	1	<b>Appendix B: Changes</b> .....	47
Route to Success .....	1		
About This Guide .....	1		
<b>Introduction</b> .....	2		
Business Overview.....	2		
Technology Overview.....	2		
<b>Deployment Details</b> .....	6		
Configuring Cisco Unified CM .....	8		
Configuring Cisco TelePresence VCS .....	23		
Configuring Cisco TelePresence Server .....	30		
Configuring Reservationless and Scheduled Conferences .....	38		

# What's In This SBA Guide

## Cisco SBA Collaboration

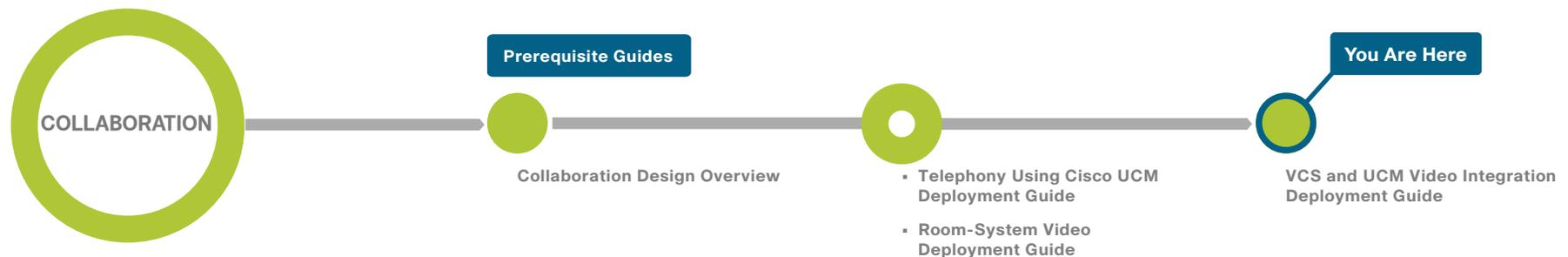
Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Collaboration is a design incorporating unified communications, video collaboration, and web conferencing. By building upon the hierarchical model of network foundation, network services, and user services, Cisco SBA Collaboration provides dependable delivery of business applications and services.

## Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.



## About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: <http://www.cisco.com/go/sba>

Partner access: <http://www.cisco.com/go/sbachannel>

# Introduction

## Business Overview

Organizations often choose between two distinct types of video solutions based on their immediate needs, without giving much thought about connecting the disparate platforms. *Multipurpose systems* are set up quickly when an organization needs to see and hear remote participants, and the quality of the experience is not that much of a concern. The units are designed to easily move from room to room. *Immersive systems* take longer to deploy because they create a virtual room experience using high-quality video and spatial audio. These high-end systems are not movable between rooms, but they offer a consistently greater level of video and audio capability to the participants.

Multipurpose video endpoints are less expensive and more versatile. They are normally purchased with rolling carts, so they are easy to relocate and use by a larger number of people in different conference rooms. They are the true workhorses of the video world, and they have been around for many years in countless organizations. On the other hand, immersive systems are deployed as an extension of the boardroom or as an executive conferencing solution. These solutions give the users the sense of being in the same room, and they are meant to make participants to feel as if they are meeting each other in person.

Just like the varied problems they are trying to solve, the underlying technologies are different between the two types of solutions. These walls of separation are acceptable when the deployments are small, but as video collaboration continues to grow, organizations need the individual siloes to communicate with each other on a regular basis. They want the multipurpose workrooms to connect with the boardroom, and they want remote workers in remote offices to communicate with executives in conference rooms at the headquarters location. The technology barriers between the two systems are not easy to overcome without proper guidance.

The biggest issues faced by organizations who want to combine their disparate video solutions are as follows:

- Endpoints require specific features to operate at their highest capabilities
- Advanced features do not interoperate between solutions
- Endpoint identification is difficult to manage
- Incorrect settings can adversely affect the network

Users of multipurpose video conferencing have grown accustomed to advanced features within their products. They do not mind configuring the system with a multi-button remote control because they need a higher level of sophistication to run effective meetings. The video conferencing endpoints handle most of the difficult functions themselves. By contrast, immersive users walk into a conference room, sit down and push a single button to virtually extend their meeting to other locations around the world. This level of simplicity hides the underlying complexity from the participants. Having two types of solutions is an operational issue for organizations when the technical intricacies are not taken into consideration.

## Technology Overview

Cisco multipurpose and Cisco TelePresence System (CTS) immersive video solutions communicate directly on point-to-point calls without a video transcoder or multipoint control unit (MCU) in the middle. This level of interoperability allows the multipurpose room systems to communicate with the immersive systems without additional video infrastructure hardware and calling complexity. Remote-site workers who use the less expensive systems can participate in video calls with the executives at the main locations when needed.

The Cisco® TelePresence Video Communication Server (VCS) manages the multipurpose systems, and Cisco Unified Communications Manager (Unified CM) manages the CTS immersive solutions and the video telephony endpoints. Certain multipurpose endpoints can also register with Unified CM, but advanced H.323 features are only supported with VCS.

Cisco VCS is deployed as a dual call-server cluster to provide resilience in the configuration. The VCS endpoints include multipurpose room systems, executive systems, and personal systems. The Unified CM configuration builds on the Cisco Smart Business Architecture (SBA) Collaboration Foundation using a multiple-server cluster. The Unified CM endpoints consist of three-screen room systems, single-screen room systems, executive systems and personal video telephones. The connection between the call agents is accomplished with the Session Initiation Protocol (SIP).

When the two call agents are connected, organizations gain the following benefits:

- Multipurpose endpoints register to VCS and maintain their advanced features, like duo-video, far end camera control (FECC), and multisite/multiway conferencing.
- CTS and video telephony endpoints register with Unified CM and maintain their centralized software updates, dynamic configuration settings, and simple, one-touch interfaces.
- Multipurpose endpoints are given a unique phone number range to simplify the routing of calls between the two call agents.
- Quality of service (QoS) is configured differently for each solution, so the traffic is properly identified in the network infrastructure.

With multipurpose video endpoints, camera angles and aspect ratios are not considered critical as long as the remote sites can see, hear, and share data with each other. The most important aspect of the multipurpose systems is the short amount of time needed to set them up and the ease with which they are deployed in various conference room environments.

Advanced video conferencing features, like duo-video for sharing presentations are only supported when using VCS. Other features that are only supported in VCS are FECC to allow remote sites to manipulate their viewing angle and multisite/multiway conferences. Multisite conferencing allows an endpoint with built-in conference capabilities to add a third device into a call. Multiway conferencing allows endpoints to initiate ad-hoc multi-point calls using a standard MCU. Bandwidth management beyond a simple hub and spoke topology is modeled with the advanced call admission control features of Pipes and Links in VCS.

On the other hand, CTS immersive systems require very particular room dimensions to accommodate specific camera angles and audio speaker placement. The conference rooms are built with strict lighting and acoustical properties to provide the highest quality experience. Heating and A/C units

are designed to run quietly, and small details like the color of the carpet and paint on the walls are taken into consideration. Matching furniture is purchased for the locations to further enhance the virtual room experience.

Multipoint control units for immersive systems have to accommodate multi-screen endpoints and have the intelligent switching capabilities to present the correct set of participants to remote sites with only a single display. The Cisco TelePresence Server has the immersive capabilities and it registers to Unified CM using a SIP trunk.

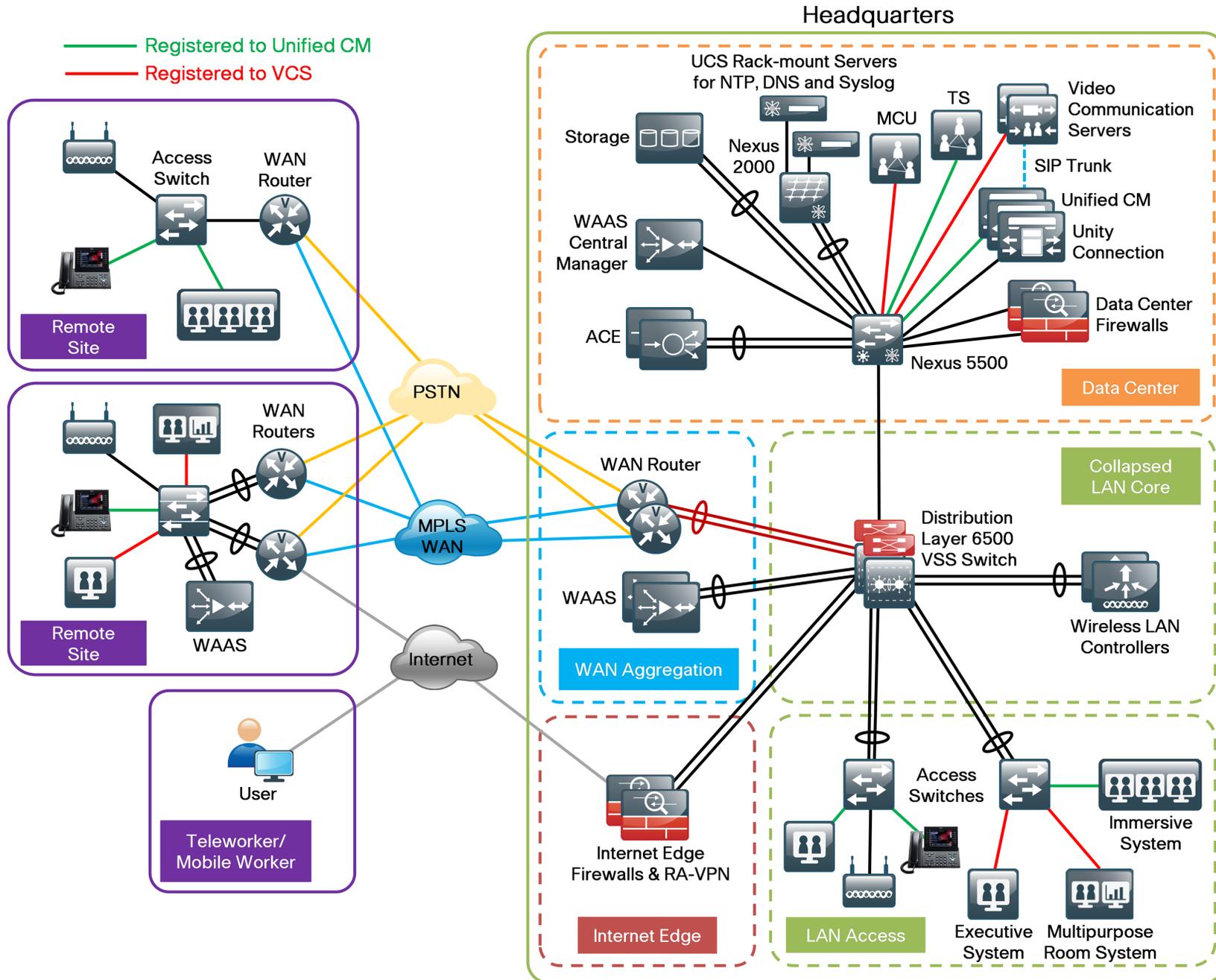
CTS endpoints register to Unified CM because it provides phone-like behavior for handling software updates and dynamic configuration settings. The user interaction on an immersive system comes from a simple telephone interface or touch screen because the intended audience is different than a multipurpose video conference deployment. The ability to connect with non-Unified CM endpoints is solved by configuring the external call signaling to use a standards-based protocol that is supported by the two call agents.

### **Solution Details**

The video integration solution includes the following components shown in the diagram below:

- VCS for multipurpose video conferencing systems
- Unified CM for CTS immersive and video telephony systems
- Personal, executive, and multipurpose room systems
- Video telephones
- Multipoint Control Unit (MCU) for immersive systems
- Network Time Protocol (NTP) server for logging consistency
- Domain Name System (DNS) for name-to-IP resolution
- Syslog server for logging events (optional)

Figure 1 - VCS and Unified CM video in SBA foundation



The video endpoints on both systems use a numeric phone number for dialing, which preserves the capability for receiving calls from devices that only support number dialing. Both call agents convert the dialed digits and domain name attributes before sending the call, so the calls are properly formatted for the respective platforms.

The solution builds upon the Cisco SBA Borderless Network, which uses the medianet QoS and bandwidth control settings recommended by Cisco. Multipurpose video conferencing traffic from VCS and video telephony traffic from Unified CM use assured forwarding 41 (AF41), and CTS traffic from Unified CM is marked as class selector 4 (CS4). The call-signaling traffic is marked as call selector 3 (CS3). The bandwidth for calls between locations is controlled by VCS for the multipurpose endpoints and by Unified CM for the CTS and video telephony endpoints. The two call agents work in parallel with each other for bandwidth control.

The priority bandwidth queues in the routers and switches are provisioned for the total amount required by both call agents. Because the call agents are working in parallel, the two types of video traffic are treated like “ships passing in the night” between the remote locations. This allows VCS and Unified CM to autonomously manage their bandwidth settings without interfering with each other at the queuing points in the network because the queues are configured to allow the combined bandwidth from both call agents. The bandwidth for calls within a location on a single call agent is handled by default call settings on each endpoint.

The Cisco SBA Borderless Network is configured to allow 23 percent of the available WAN bandwidth for video calls. In this example, the remote sites have 15 Mbps of bandwidth into the Multiprotocol Label Switching (MPLS) cloud to accommodate two 1.5 Mbps calls at each location and the headquarters site has 30 Mbps to accommodate four calls. This means that each call control agent is limited to one call in and out of the remote site. If more calls are needed, you need additional WAN bandwidth at the remote sites and the headquarters location to accommodate the higher values.

The call control agents and MCU are centralized in the data center. The access, WAN, and campus networks are medianet-enabled, using highly available designs and localized services, like medianet call monitoring and media tracing. These services are configured in the remote sites whenever possible and as close to the endpoints as practical. The video monitoring capabilities are used to troubleshoot problems when they arise and media trace allows the administrator to view the health of the network components in the path. The advantage of bringing Cisco video technologies to the Cisco SBA reference design model is that the initial foundation work remains intact because the architecture was originally designed with video communication in mind.

## Notes

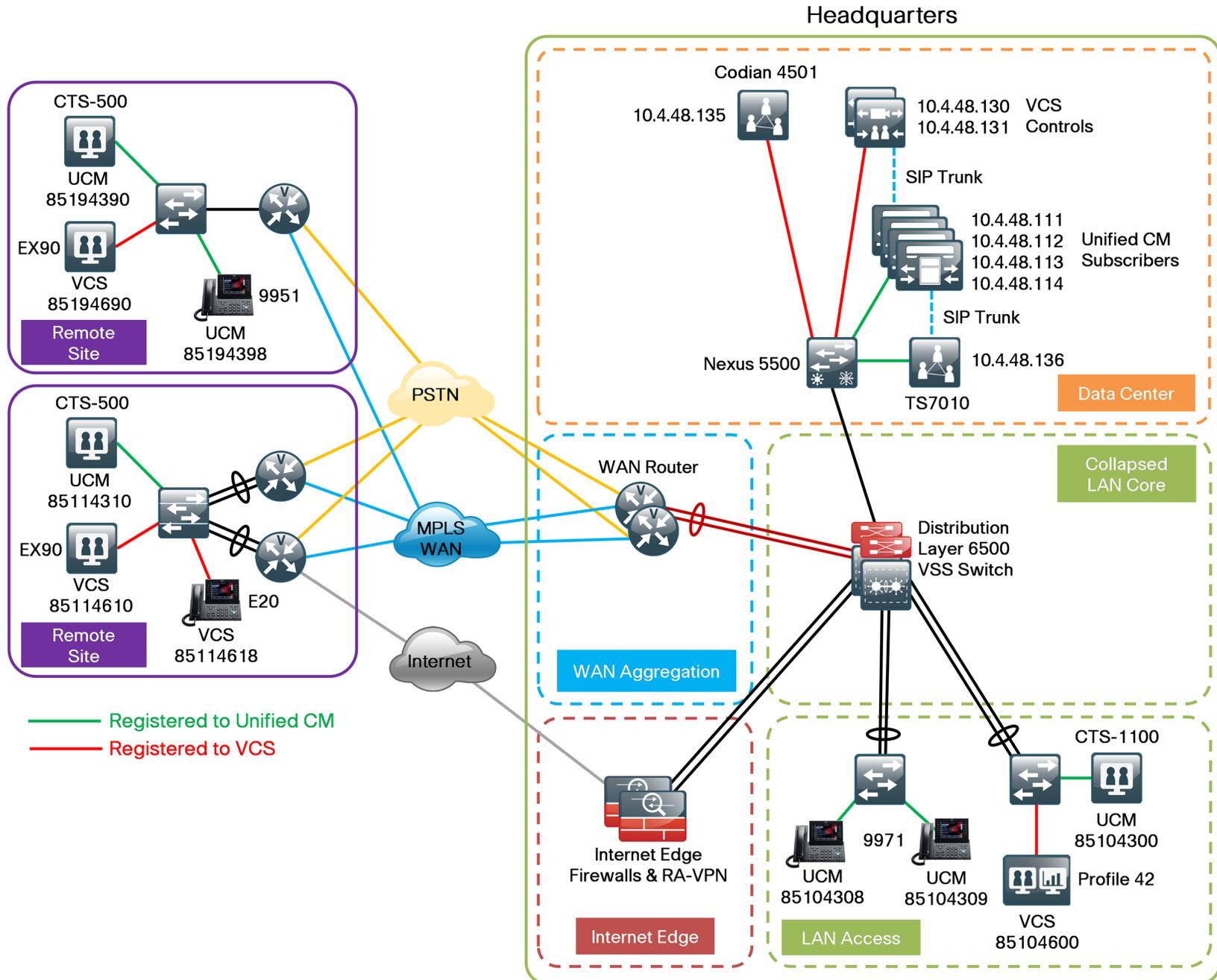
# Deployment Details

This deployment guide focuses on calls between multipurpose video conferencing systems registered to a Cisco VCS and CTS immersive video endpoints registered to a Cisco Unified CM. The procedures for configuring and registering SIP and H.323 devices to VCS is documented in the *Room-System Video Deployment Guide* and the *H.323 Video Integration Deployment Guide*, so the concepts are not covered again in this guide.

The Unified CM endpoints use their full range of extensions and a domain name of **[10.4.48.111]**. The VCS endpoints use the 8XXX46XX and 8XXX47XX range of extensions and a domain name of **cisco.local**. The distinct number range on VCS provides a non-overlapped dial plan that allows simplified call routing on each call agent.

## Notes

Figure 2 - Directory numbers for VCS and Unified CM video endpoints



## Process

### Configuring Cisco Unified CM

1. Configure CTS connectivity to the LAN
2. Configure CTS immersive endpoints
3. Configure CTS associated phones
4. Install the CTS software
5. Deploy the latest CTS software
6. Deploy the CTS phone application software
7. Configure video telephony endpoints
8. Configure UCM call admission control
9. Unified CM to Unified CM calling
10. Configure Unified CM to VCS calling

The procedures for configuring a basic Unified CM cluster are documented in the *Telephony using Cisco UCM Deployment Guide*, so the concepts are not covered again in this guide. The procedures for setting up the physical rooms and CTS endpoints are documented at <http://www.cisco.com/go/telepresenceservices/> and they are not covered in this guide.

The steps in the following four procedures must be completed for each of the CTS endpoints and their associated phones.

### Procedure 1 Configure CTS connectivity to the LAN

To ensure that video traffic is prioritized appropriately, you must configure the access switch port where the CTS endpoint is connected to trust the Differentiated Services Code Point (DSCP) markings. The easiest way to do this is to clear the interface of any previous configuration and then, apply the egress QoS macro that was defined in the access-switch platform configuration of the *Cisco SBA—Borderless Networks LAN Deployment Guide*.

**Step 1:** Login to the Catalyst switch with a username that has the ability to make configuration changes, and enter enable mode.

**Step 2:** Clear the interface's configuration on the switch port where the CTS is connected.

```
default interface GigabitEthernet 0/24
```

**Step 3:** Configure the port as an access port and apply the Egress QoS policy.

```
interface GigabitEthernet 0/24
description CTS Video Endpoint
switchport access vlan 64
switchport host
macro apply EgressQoS
logging event link-status
```

### Procedure 2 Configure CTS immersive endpoints

CTS endpoints and their associated IP phones are manually configured in Unified CM. Depending on the version of code on each device, the codec and phone might need to be upgraded to match the version in Unified CM. The upgrade process can take up to an hour to complete.

With regards to endpoint addressing, it is recommended that you use a uniform on-net dial plan containing an access code, a site code, and a four-digit extension. The use of access and site codes enables the on-net dial plan to differentiate between extensions that could otherwise overlap if a uniform abbreviated dial plan is implemented. When site codes are used, a new partition, calling search space and translation pattern per site are needed to allow four-digit dialing between endpoints at the same site which is what most users prefer.

**Step 1:** Connect the cables as specified in the endpoint installation guide, and turn on the main power switches for the codec and display. Wait several minutes for the system and associated Cisco IP phone to power up. As the system is powering up, the IP address and MAC address of the endpoint are displayed on the screen for several minutes. Make a note of this information, because you will need it in subsequent steps.

**Step 2:** Using your web browser, access the Unified CM Administration interface using the hostname or IP address.

**Step 3:** In the center of the page under **Installed Applications**, click the **Cisco Unified Communications Manager** link.

**i Tech Tip**

If you receive a warning about the website's security certificate, ignore it and continue to the website page.

**Step 4:** Enter the **Username** and **Password** you created for the application administrator, and then click **Login**.

**Step 5:** Navigate to **Device > Phone**, and then click **Add New**.

**Step 6:** In the Phone Type list, choose: **Cisco TelePresence 500-37**, and then click **Next**.

**Step 7:** On the Phone Configuration screen, under the Device Information section enter the following values.

- MAC Address—[\[MAC Address\]](#)
- Description—[RS208 CTS 500-37](#)
- Device Pool—[DP\\_RS208\\_1](#)
- Phone Button Template—[Standard\\_Cisco\\_TelePresence\\_500](#)
- Calling Search Space—[CSS\\_RS208](#)
- Location—[LOC\\_RS208](#)

Device Information	
Registration	Unknown
IP Address	Unknown
<input checked="" type="checkbox"/> Device is Active	
<input checked="" type="checkbox"/> Device is trusted	
MAC Address*	<input type="text" value="001DA2394A0C"/>
Description	<input type="text" value="RS208 CTS 500-37"/>
Device Pool*	<input type="text" value="DP_RS208_1"/> <a href="#">View Details</a>
Common Device Configuration	<input type="text" value="&lt; None &gt;"/> <a href="#">View Details</a>
Phone Button Template*	<input type="text" value="Standard_Cisco_TelePresence_500"/>
Common Phone Profile*	<input type="text" value="Standard Common Phone Profile"/>
Calling Search Space	<input type="text" value="CSS_RS208"/>
Media Resource Group List	<input type="text" value="&lt; None &gt;"/>
Location*	<input type="text" value="LOC_RS208"/>
User Locale	<input type="text" value="&lt; None &gt;"/>
Network Locale	<input type="text" value="&lt; None &gt;"/>
Device Mobility Mode*	<input type="text" value="Default"/> <a href="#">View Current Device Mobility Settings</a>
Owner User ID	<input type="text" value="&lt; None &gt;"/>
Phone Load Name	<input type="text" value=""/>
Use Trusted Relay Point*	<input type="text" value="Default"/>
Always Use Prime Line*	<input type="text" value="Default"/>
Always Use Prime Line for Voice Message*	<input type="text" value="Default"/>
Calling Party Transformation CSS	<input type="text" value="&lt; None &gt;"/>
Geolocation	<input type="text" value="&lt; None &gt;"/>
<input checked="" type="checkbox"/> Use Device Pool Calling Party Transformation CSS	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Ignore Presentation Indicators (internal calls only)	
<input checked="" type="checkbox"/> Allow Control of Device from CTI	
<input checked="" type="checkbox"/> Logged Into Hunt Group	
<input type="checkbox"/> Remote Device	



**Step 10:** On the Phone Configuration screen, under Association Information, click **Line [1] - Add a new DN**.

**Step 11:** On the Directory Number Configuration screen, enter the following values, and then click **Save**:

- Directory Number—**85194390** (Access code, site code and extension)
- Route Partition—**PAR\_Base**
- Description—**RS208 CTS 500-37**
- Alerting Name—**[Alerting name]**
- ASCII Alerting Name—**[ASCII alerting name]**

Directory Number Information	
Directory Number*	85194390
Route Partition	PAR_Base
Description	RS208 CTS 500-37
Alerting Name	Kelly Fleshner
ASCII Alerting Name	Kelly Fleshner
<input checked="" type="checkbox"/> Allow Control of Device from CTI	
Associated Devices	SEP001DA2394A0C
	<input type="button" value="Edit Device"/> <input type="button" value="Edit Line Appearance"/>
	
Dissociate Devices	

**Step 1:** Navigate to **System > Cisco Unified CM**, click **Find**, and then choose the name of the Unified CM server.

**Step 2:** Select the **Auto-registration Disabled on the Cisco Unified Communications Manager** checkbox and click **Save**.



### Tech Tip

After disabling auto-registration, the starting and ending directory number is changed to 1000. The previous values must be re-entered if auto-registration is enabled after adding the associated phones.

Server Information	
CTI ID	2
Cisco Unified Communications Manager Server*	10.4.48.111
Cisco Unified Communications Manager Name*	CM_CUCM-Sub1
Description	CUCM-Sub1

Auto-registration Information	
Starting Directory Number*	8001000
Ending Directory Number*	8004000
Partition	PAR_Base
External Phone Number Mask	
<input checked="" type="checkbox"/> Auto-registration Disabled on this Cisco Unified Communications Manager	

Cisco Unified Communications Manager TCP Port Settings for this Server	
Ethernet Phone Port*	2000
MGCP Listen Port*	2427
MGCP Keep-alive Port*	2555
SIP Phone Port*	5060
SIP Phone Secure Port*	5061

**Step 3:** Repeat Step 1 and Step 2 for all of the Unified CM servers that have auto-registration enabled.

**Step 4:** Use the touch interface of the phone to locate the MAC address under **Settings > Network Configuration > MAC Address**.

### Procedure 3

## Configure CTS associated phones

CTS endpoints use an associated IP phone to operate the day to day functions of the unit. The Unified CM design has auto-registration configured, so it is turned off temporarily to configure the associated phone as a SIP device. The directory number for the associated phone uses the 801XXXX range to distinguish it from phones that belong to individual users and phones that were auto-registered.

The easiest way to assign the directory number is to prepend 801 to the front of the four digit extension of the Cisco TelePresence System (CTS) endpoint. For example, if the CTS-500 has an extension of 4390, assign 8014390 as the directory number of the associated CP-7975 phone.

**Step 5:** On Unified CM, navigate to **Device > Phone**, click **Find**, and look for the MAC address from the previous step. Because the phone has auto-registered as a Skinny Call Control Protocol (SCCP) device, select the checkbox next to it, and then click **Delete Selected**.

**Step 6:** On the Find and List Phones screen, click **Add New**.

**Step 7:** Enter the following values and after each entry, click **Next**:

- Phone Type—**Cisco 7975**
- Select the device protocol—**SIP**

**Step 8:** On the Phone Configuration screen, enter the following values, and then click **Save**:

- MAC Address—**[MAC Address]**
- Description—**RS208 CTS 7975**
- Device Pool—**DP\_RS208\_1**
- Phone Button Template—**Standard 7975 SIP**
- Calling Search Space—**CSS\_RS208**
- Location—**LOC\_RS208**
- Device Security Profile—**Cisco 7975 - Standard SIP Non-Secure Profile**
- SIP Profile—**Standard SIP Profile**
- Web Access—**Enabled**

**Phone Type**  
**Product Type:** Cisco 7975  
**Device Protocol:** SIP

**Device Information**

Device is trusted

MAC Address\* 68BDABA5377A

Description RS208 CTS 7975

Device Pool\* DP\_RS208\_1 [View Details](#)

Common Device Configuration < None > [View Details](#)

Phone Button Template\* Standard 7975 SIP

Softkey Template < None >

Common Phone Profile\* Standard Common Phone Profile

Calling Search Space CSS\_RS208

AAR Calling Search Space < None >

Media Resource Group List < None >

User Hold MOH Audio Source < None >

Network Hold MOH Audio Source < None >

Location\* LOC\_RS208

**Protocol Specific Information**

Packet Capture Mode\* None

Packet Capture Duration 0

Presence Group\* Standard Presence group

SIP Dial Rules < None >

MTP Preferred Originating Codec\* 711ulaw

Device Security Profile\* Cisco 7975 - Standard SIP Non-Secure Profile

Rerouting Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile

Digest User < None >

Media Termination Point Required

Unattended Port

Require DTMF Reception

**Product Specific Configuration Layout**

	Param	Override Common Settings
<input type="checkbox"/>	Disable Speakerphone	
<input type="checkbox"/>	Disable Speakerphone and Headset	
Forwarding Delay*	Disabled	
PC Port *	Enabled	
Settings Access*	Enabled	<input type="checkbox"/>
Gratuitous ARP*	Disabled	
PC Voice VLAN Access*	Enabled	
Auto Line Select*	Disabled	
Web Access*	Enabled	<input checked="" type="checkbox"/>

**Step 9:** On the Phone Configuration screen, under Association Information, click **Line [1] - Add a new DN**.

**Step 10:** On the Directory Number Configuration screen, enter the following values, and then click **Save**.

- Directory Number—**8014390** (801 prepended to 4390)
- Route Partition—**PAR\_Base**
- Description—**RS208 CTS 500-37**
- Alerting Name—**[Alerting name]**
- ASCII Alerting Name—**[ASCII alerting name]**

**Directory Number Information**

Directory Number\*

Route Partition

Description

Alerting Name

ASCII Alerting Name

Active

**Step 11:** Repeat Procedure 1 through Procedure 3 for each CTS endpoint and associated phone that you want to add to Unified CM. Change the unit specific parameters to match each endpoint.

#### Procedure 4 Install the CTS software

After the CTS endpoints are registered with your Unified CM, install the latest shipping version of the endpoint software onto the TFTP servers in your cluster. You need a valid cisco.com account to download the Cisco TelePresence endpoint software. You also need Secure File Transfer Protocol (SFTP) server software to safely transfer the file to your Unified CM TFTP servers.

The installation of the CTS endpoint software is always recommended because the upgrade process automatically installs the mandatory phone application software on the TFTP servers.

**Step 1:** From your web browser, access [www.cisco.com](http://www.cisco.com), login with your User ID, and then navigate to **Support > All Downloads**.

**Step 2:** On the **Select a Product** screen, navigate to **Products > TelePresence > Telepresence Endpoints - Personal > TelePresence Office > Cisco TelePresence System Device > TelePresence Software > Latest Releases**

File Information	Release Date	Size
Cisco TelePresence Midlet Phone Application TSPM-1.8.2-P1-1S.jar	20-APR-2012	0.01 MB
Cisco TelePresence Midlet Phone Application TSPM-1.8.2-P1-1S.jar	20-APR-2012	0.39 MB
Cisco TelePresence System Software and Cisco TelePresence Touch Files for the CTS500-37, CTS1000, CTS1100, CTS1300-65, CTS3000, CTS3010, CTS3200 and CTS3210 cmterm-CTS.1-8-2-11R-K9.P1.cop.sgn	20-APR-2012	88.60 MB

**Step 3:** Choose the latest release file **cmterm-CTS.1-8-2-11R-K9.P1.cop.sgn**, and then download it to your PC.

**Step 4:** Start the SFTP server software on your PC and configure it with a username and password for accessing the downloaded software in a specified directory.

**Step 5:** From your web browser, access the Unified CM Administration interface of the TFTP server in your cluster.

**Step 6:** In the center of the page under Installed Applications, click the **Cisco Unified Communications Manager** link.

**Step 7:** In the Navigation list at the top of the page, choose **Cisco Unified OS Administration**, and then click **Go**.

**Step 8:** Enter the **Username** and **Password** for the platform administrator, and then click **Login**.

**Step 9:** Navigate to **Software Upgrades > Install/Upgrade**, enter the following information and then, click **Next**.

- Source—**Remote Filesystem**
- Directory—/
- Server—**10.4.48.152** (IP Address of PC running SFTP server software)
- User Name—**root**
- User Password—**[password]**
- Transfer Protocol—**SFTP**

**Software Location**

Source\*

Directory\*

Server\*

User Name\*

User Password\*

Transfer Protocol\*

SMTP Server

Email Destination

**Step 10:** Select the CTS endpoint file that was downloaded and click **Next**.

**Software Location**

Options/Upgrades\*

**Step 11:** After the file is downloaded and validated, verify the MD5 Hash Value on the server matches the MD5 hash on your PC.

Figure 3 - MD5 Hash Value from Unified CM

File Checksum Details	
File	cmterm-CTS.1-8-2-11R-K9.P1.cop.sgn
MD5 Hash Value	3c:26:85:80:3e:eb:08:39:3b:b4:bc:7e:c2:04:3d:05

Figure 4 - MD5 Hash Value from PC running SFTP Server

Name	Hash Value
CRC32	75114D43
MD5	3C2685803EEB08393BB4BC7EC2043D05
SHA-1	423FBC3F63342DA9A86D5B02FBE4D1C094BD86...

**Step 12:** If the MD5 Hashes do not match, transfer the file again. If they match, click **Next** and confirm the file is successfully installed.

Installation Status	
File	cmterm-CTS.1-8-2-11R-K9.P1.cop.sgn
Start Time	Tue Jun 12 15:12:54 PDT 2012
Status	Locale /common/download//cmterm-CTS.1-8-2-11R-K9.P1.cop Successfully installed

**Step 13:** In the Navigation list at the top of the page, choose **Cisco Unified Serviceability**, and then click **Go**.

**Step 14:** Enter the **Username** and **Password** for the application administrator, and then click **Login**.

**Step 15:** Navigate to **Tools > Control Center - Feature Services**, select the TFTP server, and then click **Go**.

**Step 16:** In the CM Services section, select the Cisco Tftp server radio button, and then click **Restart**.

**Step 17:** Repeat Step 5 through Step 16 for all of the TFTP servers in your cluster.

## Procedure 5 Deploy the latest CTS software

**Step 1:** After the screen refreshes on the final TFTP server, use your web browser to access the Unified CM Administration interface of the publisher server in your cluster.

**Step 2:** In the center of the page under Installed Applications, click the **Cisco Unified Communications Manager** link.

**Step 3:** Enter the **Username** and **Password** for the application administrator, and then click **Login**.

**Step 4:** Navigate to **Device > Device Settings > Device Defaults**, enter the downloaded file name without "cmterm" in the Load Information column for each CTS endpoint, and then click **Save**.

- Load Information—**CTS.1-8-2-11R-K9.P1**

 Cisco TelePresence 1000	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 1100	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 1300-47	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 1300-65	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 1310-65	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 3000	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 3200	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 500-32	SIP	CTS.1-8-2-11R-K9.P1
 Cisco TelePresence 500-37	SIP	CTS.1-8-2-11R-K9.P1

**Step 5:** Navigate to **Device > Phone**, click **Find**, and then click on the name of the CTS endpoint.

**Step 6:** From the **Phone Configuration** page, click **Reset**, and then in the **Device Reset** screen, click **Reset**. The CTS endpoint will take about an hour to upgrade the software.

**Step 7:** Repeat Step 5 and Step 6 for each CTS endpoint.

## Procedure 6 Deploy the CTS phone application software

**Step 1:** From your web browser, access the Unified CM Administration interface of the publisher in your cluster.

**Step 2:** In the Navigation list at the top of the page, choose **Cisco Unified CM Administration**, and then click **Go**.

**Step 3:** Navigate to **Device > Device Settings > Phone Services**, and then click **Add New**.

**Step 4:** On the **IP Phone Services Configuration** screen, enter the following values, and then click **Save**:

- Service Name—**TSPM-1.8.2-P1-1S**
- ASCII Service Name—**TSPM-1.8.2-P1-1S**
- Service Description—**MIDlet UI**
- Service URL—**http://10.4.48.120:6970/TSPM-1.8.2-P1-1S.jad**
- Service Category—**Java MIDlet**
- Service Type—**Standard IP Phone Service**
- Service Vendor—**Cisco**
- Enable Checkbox—**Yes**

Service Information	
Service Name*	TSPM-1.8.2-P1-1S
ASCII Service Name*	TSPM-1.8.2-P1-1S
Service Description	MIDlet UI for CTS Phones
Service URL*	http://10.4.48.120:6970/TSPM-1.8.2-P1-1S.jad
Secure-Service URL	
Service Category*	Java MIDlet
Service Type*	Standard IP Phone Service
Service Vendor	Cisco
Service Version	
<input checked="" type="checkbox"/> Enable	
<input type="checkbox"/> Enterprise Subscription	

**Step 5:** Navigate to **Device > Phone**, click **Find**, and then click the MAC address of a phone associated with a CTS endpoint.

**Step 6:** In the Related Links list, choose **Subscribe/Unsubscribe Services**, and then click **Go**.

**Step 7:** In the Select a Service list, choose the service you configured in Step 4, and then click **Next**.

**Step 8:** On the next screen, click **Subscribe**.

Service Subscription: TSPM-1.8.2-P1-1S

**Service Information**

Service Name\*

ASCII Service Name\*

After a minute or two, the application starts on the phone and it can be used to place calls.

Repeat Step 5 through Step 8 for each phone associated with a CTS endpoint.

## Procedure 7 Configure video telephony endpoints

Telephony endpoints use the auto-registration process from the Unified CM Foundation to register with the cluster. Extension mobility assigns user-specific information to the phones. Device mobility information places the phone in the correct device pool to use all of its associated settings. Video telephones can use extension mobility or they can be configured with a specific directory number.

The following steps are required to assign the correct device pool, calling search space and to prepare the phone for sending and receiving video calls.

**Step 1:** Use the touch interface of the phone to locate the MAC address under **Settings > Network Configuration > MAC Address**.

**Step 2:** On Unified CM, navigate to **Device > Phone**, click **Find**, look for the video telephone, and then click the MAC address from the previous step. In this example, the phone is configured for the RS200 location.

**Step 3:** On the **Phone Configuration** screen under the Device Information section, enter the following values.

- Device Pool—**DP\_RS200\_1**
- Calling Search Space—**CSS\_RS200**

**Device Information**

Registration Registered with Cisco Unified Communications Manager 10.4.48.111

IP Address [10.5.4.20](#)

Active Load ID sip9951.9-2-2

Inactive Load ID sip9951.9-2-1

Download Status Successful

Device is Active

Device is trusted

MAC Address\*

Description

Device Pool\*  [View Details](#)

Common Device Configuration  [View Details](#)

Phone Button Template\*

Common Phone Profile\*

Calling Search Space

**Step 4:** Under the Product Specific Configuration Layout section enter the following values, and then click **Save**.

- Cisco Camera—**Enabled**
- Video Capabilities—**Enabled**

**Product Specific Configuration Layout**

	Param	Override Common Settings
<input type="checkbox"/> Disable Speakerphone		<input type="checkbox"/>
<input type="checkbox"/> Disable Speakerphone and Headset		<input type="checkbox"/>
PC Port *	<input type="text" value="Enabled"/>	<input type="checkbox"/>
Back USB Port*	<input type="text" value="Enabled"/>	<input type="checkbox"/>
Side USB Port*	<input type="text" value="Enabled"/>	<input type="checkbox"/>
Cisco Camera*	<input type="text" value="Enabled"/>	<input checked="" type="checkbox"/>
Video Capabilities*	<input type="text" value="Enabled"/>	<input checked="" type="checkbox"/>

If the phone is not used with Extension Mobility, you must complete Step 5 and Step 6 to assign an eight-digit directory number within the proper site code and extension range of the site.

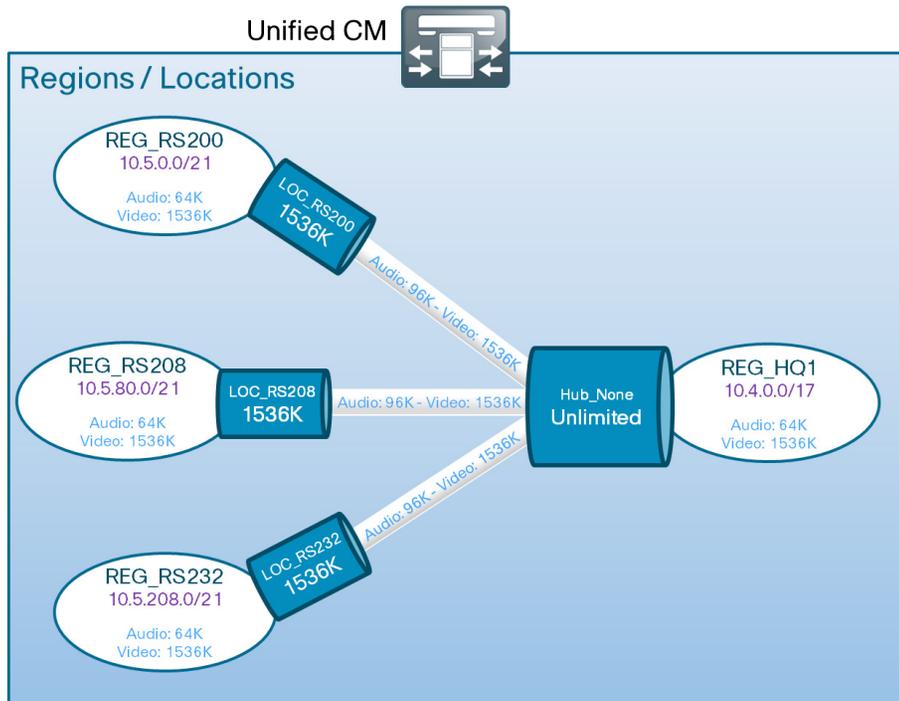
**Step 5:** On the Phone Configuration screen, under Association Information, click **Line [1]**.

**Step 6:** On the Directory Number Configuration screen, enter the following values, and then click **Save**:

- Directory Number—**85114019** (Access code, site code and extension)
- Route Partition—**PAR\_Base**

## Procedure 8 Configure UCM call admission control

Video calls between different locations are limited to 1.5 Mbps for this configuration guide, and one call is allowed per site. For this example, the remote sites require at least 15 Mbps of total WAN bandwidth and the headquarters site requires 30 Mbps into the MPLS cloud. The additional WAN bandwidth permits higher-quality video and audio between the locations. If your location needs more than one call per remote site or if you want to use a higher bandwidth per call, you must upgrade the WAN bandwidth between the sites to accommodate the higher values.



The Region configuration max audio bit rate is set to 64 kbps because the initial call signal between the two CTS endpoints is an audio-only call, which requires G.722. The Location configuration audio bandwidth is set to at least 96 kbps because video calls from multipurpose endpoints to CTS endpoints are initially audio-only calls and they will be rejected if the bandwidth is less than 96 kbps.

**Step 1:** Navigate to **System > Region**, click **Find**, and then click the name of a region.

**Step 2:** Under Modify Relationship to other Regions on the bottom of the screen, choose each region that has CTS video endpoints, change the following values, and then click **Save**:

- Max Audio Bit Rate—**64 kbps (G.722, G.711)**
- Kbps (radio button)—**Select**
- Max Video Call Bit Rate—**1536**
- Link Loss Type—**Keep Current Setting**

**Step 3:** After all of the regions in the Region list are modified, click **Apply Config**.

Region Information			
Name*	REG_HQ1		
Region Relationships			
Region	Max Audio Bit Rate	Max Video Call Bit Rate (Includes Audio)	Link Loss Type
REG_HQ1	64 kbps (G.722, G.711)	1536	Use System Default
REG_RS200	64 kbps (G.722, G.711)	1536	Use System Default
REG_RS208	64 kbps (G.722, G.711)	1536	Use System Default
REG_RS232	64 kbps (G.722, G.711)	1536	Use System Default
NOTE: Regions(s) not displayed	Use System Default	Use System Default	Use System Default

**Step 4:** Repeat Step 1 through Step 3 for each region with CTS endpoints.

**Step 5:** Navigate to **System > Location**, click **Find**, and then click the name of a remote-site location with CTS endpoints.

**Step 6:** Enter the following values, and then click **Save**:

- Audio Bandwidth radio button—**Yes**
- Audio kbps—**96** (must be at least 96)
- Video Bandwidth radio button—**Yes**
- Video kbps—**1536**

**Step 7:** Click **Resync Bandwidth**, and on the popup message that appears, click **OK**.

<b>Location Information</b>	
Name*	LOC_RS208
<b>Audio Calls Information</b>	
Audio Bandwidth*	<input type="radio"/> Unlimited <input checked="" type="radio"/> 192 kbps
If the audio quality is poor or choppy, lower the bandwidth setting. For ISDN, use multiples of 56 kbps or 64 kbps.	
<b>Video Calls Information</b>	
Video Bandwidth*	<input type="radio"/> None <input type="radio"/> Unlimited <input checked="" type="radio"/> 1536 kbps

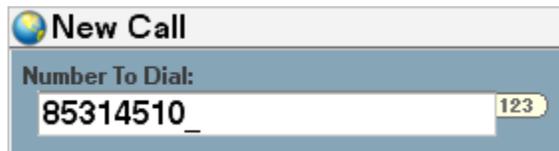
**Step 8:** Repeat Step 3 through Step 5 for each remote-site location with CTS endpoints.

## Procedure 9 Unified CM to Unified CM calling

After the endpoints have been registered and call admission control has been configured, place test calls between the locations to confirm that everything is working as expected. If calls do not work, check your work by reviewing the procedures in this process.

**Step 1:** On the associated phone, tap **New Call**.

Enter the eight digit extension of another CTS endpoint at a different location **85314510** and then tap **Dial**.



**Step 2:** From your web browser, access the CTS endpoints administrative interface <https://10.4.84.50/> and log in using the SSH admin username and password you configured in Procedure 2 of this process.

**Step 3:** On the Cisco TelePresence Systems Administration screen, enter the following values, and then click **Login**:

- Username—**admin**
- Password—**[password]**

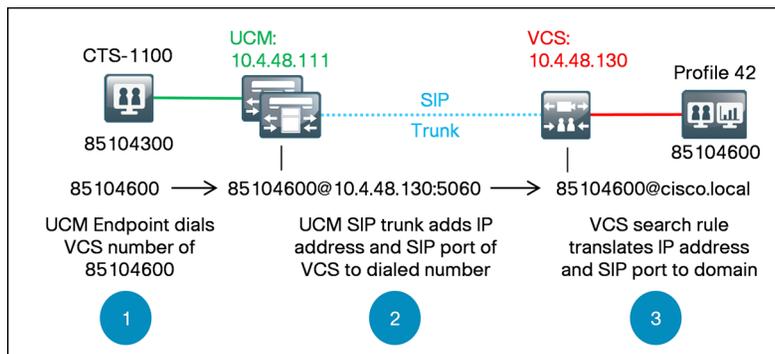
**Step 4:** Navigate to **Monitoring > Call Statistics** and verify the bandwidth is what you expect. If the bandwidth is too high or too low, confirm the values you entered in Procedure 8 match the available bandwidth for the link.

Real Time Call Statistics	
Call Connected	Yes
Registered to Cisco Unified Communications Manager	Yes
Local Number	85194390
Audio/Video Call	
Call Start Time	Wed Jun 13 11:44:02 2012
Call Duration	225 seconds
Call Type	Outgoing
Remote Number	85314510
Call State	Answered
Security Level	Non-Secure
Actual Bit Rate	972000 bps, 1280x720
Negotiated Bit Rate	1472000 bps
Historical Call Statistics (Not including current call, if any)	
Call Statistics Clear Time	Sun Jan 15 06:57:26 2006
Last Call Start Time	Wed Jun 13 11:41:50 2012
Last Call Duration	13 seconds
Number of Calls Since System Setup	232
Time in Calls Since System Setup (seconds)	304930
Number of Calls Since Last Reboot	5
Time in Calls Since Last Reboot (seconds)	529
Registered to Cisco Unified Communications Manager	Yes
Configured Bit Rate	Highest Detail, Best Motion: 1080p

**Step 5:** To hang up the call from the phone, tap **End Call**.

## Procedure 10 Configure Unified CM to VCS calling

Calls from Unified CM to VCS are routed using a SIP trunk. Sending calls for the 8XXX46XX and 8XXX47XX range of numbers requires a single route pattern in Unified CM. The diagram below shows the call flow for simple numeric dialing from a Unified CM endpoint to a VCS endpoint.



A SIP trunk, route group, route list and route pattern send the calls to the IP address of the VCS. Before adding the SIP trunk, you will also create a standard SIP profile and a non-secure SIP trunk security profile. After you finalize the Unified CM dial plan, you perform additional steps in the subsequent process to translate the called number format in the VCS.

**Step 1:** From your web browser, access the Unified CM Administration interface of the publisher in your cluster.

**Step 2:** In the center of the page under Installed Applications, click the **Cisco Unified Communications Manager** link.

**Step 3:** Enter the **Username** and **Password** you created for the application administrator, and then click **Login**.

**Step 4:** Navigate to **Device > Device Settings > SIP Profile** and click **Copy** to create a new SIP profile based on the default.

**Step 5:** From the SIP Profile Configuration screen enter the following information, and then click **Save**:

- Name—**Standard SIP Profile for VCS**
- Description—**SIP Profile for VCS**
- Redirect by Application—**Yes**
- Allow Presentation Sharing using BFCP—**Yes**
- Leave the rest of the fields at their defaults

SIP Profile Information	
Name*	Standard SIP Profile for VCS
Description	SIP Profile for VCS
Default MTP Telephony Event Payload Type*	101
Resource Priority Namespace List	< None >
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Ager
<input checked="" type="checkbox"/> Redirect by Application	
<input type="checkbox"/> Disable Early Media on 180	
<input type="checkbox"/> Outgoing T.38 INVITE include audio mline	
<input type="checkbox"/> Enable ANAT	
<input type="checkbox"/> Require SDP Inactive Exchange for Mid-Call Media Change	
<input type="checkbox"/> Use Fully Qualified Domain Name in SIP Requests	
Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on*	Never
RSVP Over SIP*	Local RSVP
<input checked="" type="checkbox"/> Fall back to local RSVP	
SIP Rel1XX Options*	Disabled
<input type="checkbox"/> Deliver Conference Bridge Identifier	
<input type="checkbox"/> Early Offer support for voice and video calls (insert MTP if needed)	
<input type="checkbox"/> Send send-receive SDP in mid-call INVITE	
<input checked="" type="checkbox"/> Allow Presentation Sharing using BFCP	

**Step 6:** Navigate to **System > Security > SIP Trunk Security Profile**, click **Find**, and then click **Copy** to create a new security profile from the default.

**Step 7:** From the SIP Trunk Security Profile Configuration screen, enter the following values, and then click **Save**:

- Name—**Non Secure SIP Trunk Profile for VCS**
- Accept unsolicited notification—**Yes**
- Accept replaces header—**Yes**

**SIP Trunk Security Profile Information**

Name*	Non Secure SIP Trunk Profile for VCS
Description	Non Secure SIP Trunk Profile authenticated by null Stri
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

**Step 8:** Navigate to **Device > Trunk**, and then click **Add New**.

**Step 9:** On the Trunk Configuration screen, enter the following values, and then click **Next**.

- Trunk Type—**SIP Trunk**
- Device Protocol—**SIP**
- Trunk Service Type—**None (Default)**

**Trunk Information**

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

**Step 10:** On the next screen in the Device Information section, enter the following values.

- Device Name—**SIP\_VCS\_Trunk**
- Description—**CUCM to VCS SIP Trunk for Video**
- Device Pool—**DP\_HQ1\_1**
- Call Classification—**OnNet**
- Location—**Hub\_None**
- Retry Video Call as Audio—**Yes**
- Run On All Active Unified CM Nodes—**Yes**

**Device Information**

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SIP_VCS_Trunk
Description	CUCM to VCS SIP Trunk for Video
Device Pool*	DP_HQ1_1
Common Device Configuration	< None >
Call Classification*	OnNet
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0
<input type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Path Replacement Support	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> Transmit UTF-8 Names in QSIG APDU	
<input type="checkbox"/> Unattended Port	
<input type="checkbox"/> SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.	
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default
<input checked="" type="checkbox"/> PSTN Access	
<input checked="" type="checkbox"/> Run On All Active Unified CM Nodes	

**Step 11:** In the Inbound Calls section, enter the following values.

- Significant Digits—**All**
- Calling Search Space—**CSS\_Base**
- Redirecting Diversion Header Delivery Inbound—**Yes**

<b>Inbound Calls</b>	
Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	CSS_Base
AAR Calling Search Space	< None >
Prefix DN	
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Inbound	

**Step 12:** In the SIP Information section, enter the following values, and then click **Save**.

- Destination Address 1—**10.4.48.130**
- Destination Port 1—**5060**
- Destination Address 2—**10.4.48.131** (click + sign to add new row)
- Destination Port 2—**5060**
- SIP Trunk Security Profile—**Non Secure SIP Trunk Profile for VCS**
- SIP Profile—**Standard SIP Profile for VCS**
- DTMF Signaling Method—**RFC 2833**
- Normalization Script—**vcs-interop**

<b>SIP Information</b>										
<b>Destination</b>										
<input type="checkbox"/> Destination Address is an SRV										
	<table border="1"> <thead> <tr> <th>Destination Address</th> <th>Destination Address IPv6</th> <th>Destination Port</th> </tr> </thead> <tbody> <tr> <td>1* 10.4.48.130</td> <td></td> <td>5060</td> </tr> <tr> <td>2 10.4.48.131</td> <td></td> <td>5060</td> </tr> </tbody> </table>	Destination Address	Destination Address IPv6	Destination Port	1* 10.4.48.130		5060	2 10.4.48.131		5060
Destination Address	Destination Address IPv6	Destination Port								
1* 10.4.48.130		5060								
2 10.4.48.131		5060								
MTP Preferred Originating Codec*	711ulaw									
Presence Group*	Standard Presence group									
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile for VCS									
Rerouting Calling Search Space	< None >									
Out-Of-Dialog Refer Calling Search Space	< None >									
SUBSCRIBE Calling Search Space	< None >									
SIP Profile*	Standard SIP Profile for VCS									
DTMF Signaling Method*	RFC 2833									
<b>Normalization Script</b>										
Normalization Script	vcs-interop									
<input type="checkbox"/> Enable Trace										
	<table border="1"> <thead> <tr> <th>Parameter Name</th> <th>Parameter Value</th> </tr> </thead> <tbody> <tr> <td>1</td> <td></td> </tr> </tbody> </table>	Parameter Name	Parameter Value	1						
Parameter Name	Parameter Value									
1										

**Step 13:** On the Message popup, click **OK**.

**Step 14:** On the Trunk Configuration screen, click **Reset**.

**Step 15:** From the Device Reset screen, click **Reset**, and then click **Close**.

<b>Reset Information</b>
<b>Selected Device: SIP_VCS_Trunk (CUCM to VCS SIP Trunk for Video; SIP Trunk)</b>
If a device is not registered with Cisco Unified Communications Manager, you cannot reset or restart it. If a device is registered, to restart a device without shutting it down, click the <b>Restart</b> button. To shut down a device and bring it back up, click the <b>Reset</b> button. To return to the previous window without resetting/restarting the device, click <b>Close</b> .
<b>Note:</b> Resetting a gateway/trunk/media devices <b>drops</b> any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.
<input type="button" value="Reset"/> <input type="button" value="Restart"/> <input type="button" value="Close"/>

**Step 16:** Navigate to **Call Routing > Route / Hunt > Route Group**, and then click **Add New**.

**Step 17:** On the Route Group Configuration screen, enter the Route Group Name **RG\_VCS\_SIP\_Trunk**.

**Step 18:** From the Available Devices, choose **SIP\_VCS\_Trunk (All Ports)**, click **Add to Route Group**, and then click **Save**.

<b>Route Group Information</b>
Route Group Name* RG_VCS_SIP_Trunk
Distribution Algorithm* Circular
<b>Route Group Member Information</b>
<b>Find Devices to Add to Route Group</b>
Device Name contains <input type="text"/> <input type="button" value="Find"/>
Available Devices**
SIP_RS211_GWY
SIP_RS221_GWY
SIP_RS222_GWY
SIP_TS7010
<b>SIP_VCS_Trunk</b>
Port(s) None Available
<input type="button" value="Add to Route Group"/>
<b>Current Route Group Members</b>
Selected Devices (ordered by priority)*
SIP_VCS_Trunk (All Ports)
<input type="button" value="Reverse Order of Selected Devices"/>
Removed Devices***

**Step 19:** Navigate to **Call Routing > Route / Hunt > Route List**, and then click **Add New**.

**Step 20:** On the Route Group Configuration screen, enter the following values, and then click **Save**.

- Name—**RL\_VCS**
- Description—**Route List for VCS Video Calls**
- Cisco Unified Communications Manager Group—**Sub1\_Sub2** (Default)

**Route List Information**

Device is trusted

Name\*

Description

Cisco Unified Communications Manager Group\*

**Step 21:** On the Route List Configuration screen, click **Add Route Group**.

**Step 22:** On the Route List Detail Configuration screen, enter the following value, and then click **Save**.

- Route Group—**RG\_VCS\_SIP\_Trunk [NON-QSIG]**

**Route List Member Information**

Route Group\*

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask\*

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Party Number Type\*

Calling Party Numbering Plan\*

**Called Party Transformations**

Discard Digits

Called Party Transform Mask

Prefix Digits (Outgoing Calls)

Called Party Number Type\*

Called Party Numbering Plan\*

**Step 23:** Navigate to **Call Routing > Route/Hunt > Route Pattern**, and then click **Add New**.

**Step 24:** On the Route Pattern Configuration screen, enter the following values, and then click **Save**.

- Route Pattern—**8XXX4[6-7]XX**
- Route Partition—**PAR\_Base**
- Description—**Route Pattern for Video Calls to VCS**
- Gateway/Route List—**RL\_VCS**
- Call Classification—**OnNet**

**Pattern Definition**

Route Pattern\*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence\*

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain

Route Class\*

Gateway/Route List\*  [\(Edit\)](#)

Route Option

Route this pattern

Block this pattern

Call Classification\*

Allow Device Override  Provide Outside Dial Tone  Allow Overlap Sending  Urgent Priority

Require Forced Authorization Code

Authorization Level\*

Require Client Matter Code

## Process

### Configuring Cisco TelePresence VCS

1. Configure VCS inbound calls
2. Configure VCS outbound calls
3. Configure VCS call admission control
4. VCS to Unified CM dialing
5. Unified CM to VCS dialing

After registering the CTS endpoints with Unified CM, modifying call admission control, and creating the dial plan, you configure Cisco VCS to allow inbound and outbound calls to and from the neighboring call agent.

## Procedure 1

### Configure VCS inbound calls

When a call is received from Unified CM, the called number is in the format of [called number]@[VCS IP address]:5060. Cisco VCS uses a search rule to translate the called number to the format [called number]@[domain name]. You will create one search rule for each VCS in the cluster.

For example, a call to a VCS endpoint at extension 85104600 arrives as 85104600@10.4.48.130:5060. The VCS translates the called number to 85104600@cisco.local before searching for the device in the local zone.

When a call is received from Unified CM, the callback number is in the format of [calling number]@[IP address of Unified CM]. For the VCS to route the call back to Unified CM, VCS uses a transform to translate the calling number to the format [calling number]@[domain name]. You will create one transform for each Unified CM subscriber.

For example, a Unified CM endpoint call from 85104300 arrives as 85104300@10.4.48.111. The VCS translates the calling number to 85104300@cisco.local before it is sent to the endpoint so the recent calls list has the properly formatted callback number.

**Step 1:** Using your web browser, access the administration interface of the master VCS in your cluster, and then click **Administrator login**.

**Step 2:** Enter the following values and click **Login**.

- Username—**admin**
- Password—**[password]**

**Step 3:** Navigate to **VCS configuration > Dial Plans > Search rules** and click **New**.

**Step 4:** Enter the following values and click **Create search rule**.

- Rule name—**CUCM Calls to VCSc1**
- Description—**8XXX4[6-7]XX to registered VCS endpoints**
- Priority—**40**
- Source—**Any**
- Request must be Authenticated—**No**
- Mode—**Alias Pattern Match**
- Pattern Type—**Regex**
- Pattern String—**(8\d{3}4[6-7]\d{2})@10.4.48.130:5060**
- Pattern behavior—**Replace**
- Replace String—**\1@cisco.local**
- On successful match—**Stop**
- Target—**LocalZone**
- State—**Enabled**

**Configuration**

Rule name: **CUCM Calls to VCSc1**

Description: **8XXX4[6-7]XX to registered VCS endpoints**

Priority: **40**

Source: **Any**

Request must be authenticated: **No**

Mode: **Alias pattern match**

Pattern type: **Regex**

Pattern string: **(8\d{3}4[6-7]\d{2})@10.4.48.130:5060**

Pattern behavior: **Replace**

Replace string: **\1@cisco.local**

On successful match: **Stop**

Target: **LocalZone**

State: **Enabled**

**Step 5:** Repeat Step 3 and Step 4 for every VCS IP address in your VCS cluster. Change the Rule name, the Pattern string's IP address and increase the Priority by 1 for each search rule.

40	✓ Enabled	CUCM Calls to VCSc1	Any	No	Alias pattern match	Regex	(8\d{3}4[6-7]\d{2})@10.4.48.130:5060	Replace	Stop	LocalZone
41	✓ Enabled	CUCM Calls to VCSc2	Any	No	Alias pattern match	Regex	(8\d{3}4[6-7]\d{2})@10.4.48.131:5060	Replace	Stop	LocalZone

**Step 6:** Navigate to **VCS configuration > Dial Plans > Transforms**, and then click **New**.

**Step 7:** Enter the following values, and then click **Create transform**.

- Priority—**3**
- Description—**CUCM\_Sub1 IP Address to Domain Name**
- Pattern type—**Regex**
- Pattern string—**(.\*)@10.4.48.111((:|:).\*)?**
- Pattern behavior—**Replace**
- Pattern string—**\1@cisco.local\2**
- State—**Enabled**

**Configuration**

Priority: **3**

Description: **CUCM\_Sub1 IP Address to Domain Name**

Pattern type: **Regex**

Pattern string: **(.\*)@10.4.48.111((:|:).\*)?**

Pattern behavior: **Replace**

Replace string: **\1@cisco.local\2**

State: **Enabled**

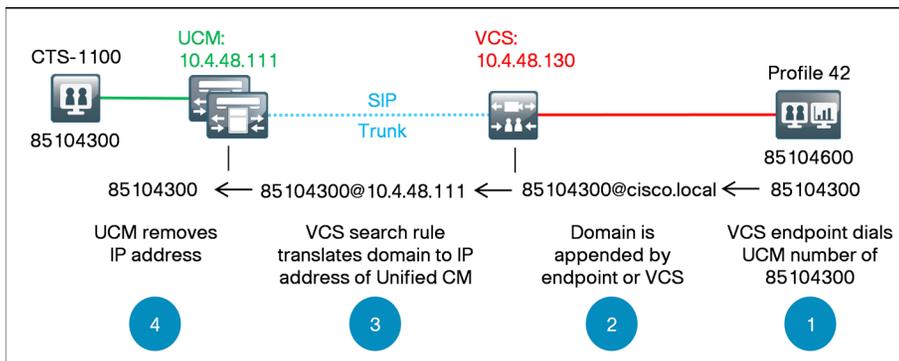
**Step 8:** Repeat Step 6 and Step 7 for every subscriber IP address in your Unified CM cluster. Change the Description, Pattern string's IP address and increase the Priority by 1 each time.

3	✓ Enabled	CUCM_Sub1 IP Address to Domain Name	(.*)@10.4.48.111((: :).*)?	Regex	Replace	\1@cisco.local\2
4	✓ Enabled	CUCM_Sub2 IP Address to Domain Name	(.*)@10.4.48.112((: :).*)?	Regex	Replace	\1@cisco.local\2
5	✓ Enabled	CUCM_Sub3 IP Address to Domain Name	(.*)@10.4.48.113((: :).*)?	Regex	Replace	\1@cisco.local\2
6	✓ Enabled	CUCM_Sub4 IP Address to Domain Name	(.*)@10.4.48.114((: :).*)?	Regex	Replace	\1@cisco.local\2

## Procedure 2

## Configure VCS outbound calls

Calls from multipurpose endpoints are routed from VCS to Unified CM using SIP trunks. You create a neighbor zone and two search rules for every Unified CM subscriber to allow resilient dialing between the two systems. The diagram below shows the call flow for numeric dialing from a VCS endpoint to a Unified CM endpoint.



You configure a different neighbor zone for each subscriber to provide signaling redundancy. You create search rules with the same priority to send calls to the neighbor zones defined for the Unified CM cluster. The local domain name is replaced with the IP address of the specified Unified CM subscriber.

The calls will round robin between search rules with the same priority which in turn will round robin between the Unified CM subscribers. If a subscriber is unreachable, the zone will become inactive and the search rule for the unreachable subscriber will be ignored until it comes back online.

**Step 1:** Navigate to **VCS Configuration > Zones**, and then click **New**.

**Step 2:** On the **Create Zone** screen, under the Configuration, H.323 and SIP sections enter the following values.

- Name—**CUCM\_Sub1 Neighbor**
- Type—**Neighbor**
- H.323 Mode—**Off**
- SIP Mode—**On**
- SIP Port—**5060**
- SIP Transport—**TCP**
- Accept proxied registrations—**Deny**

The screenshot shows the configuration for a new VCS zone. The Configuration section is expanded, showing the following settings:

- Name: CUCM\_Sub1 Neighbor
- Type: Neighbor
- Hop count: 15

The H.323 section is also expanded, showing the following settings:

- Mode: Off
- Port: 1719

The SIP section is expanded, showing the following settings:

- Mode: On
- Port: 5060
- Transport: TCP
- Accept proxied registrations: Deny

**Step 3:** Under the Location and Advanced sections enter the following values, and then click **Create Zone**.

- Peer 1 Address—**10.4.48.111** (first subscriber)
- Zone Profile—**Cisco Unified Communications Manager**

**Location**

Peer 1 address	<input type="text" value="10.4.48.111"/>	
Peer 2 address	<input type="text"/>	
Peer 3 address	<input type="text"/>	
Peer 4 address	<input type="text"/>	
Peer 5 address	<input type="text"/>	
Peer 6 address	<input type="text"/>	

**Advanced**

Zone profile	<input type="text" value="Cisco Unified Communications Manager"/>
--------------	---

**Step 4:** Repeat Step 1 through Step 3 for each subscriber in the Unified CM cluster. Change the Name and Peer 1 Address for each zone.

DefaultZone	Default Zone	0	0 kbps	On	On	
<a href="#">CUCM_Sub1 Neighbor</a>	Neighbor	0	0 kbps	Off	Active	No <a href="#">search rules</a> configured
<a href="#">CUCM_Sub2 Neighbor</a>	Neighbor	0	0 kbps	Off	Active	No <a href="#">search rules</a> configured
<a href="#">CUCM_Sub3 Neighbor</a>	Neighbor	0	0 kbps	Off	Active	No <a href="#">search rules</a> configured
<a href="#">CUCM_Sub4 Neighbor</a>	Neighbor	0	0 kbps	Off	Active	No <a href="#">search rules</a> configured

**Step 5:** Navigate to VCS configuration > Dial Plans > Search rules, and then click **New**.

**Step 6:** Enter the following values, and then click **Create search rule**.

- Rule name—**Route1 to CUCM\_Sub1**
- Description—**Send all 8XXX4XXX except 8XXX4[6-7]XX calls to CUCM**
- Priority—**100** (same priority for all subscribers)
- Source—**Any**
- Request must be Authenticated—**No**
- Mode—**Alias Pattern Match**
- Pattern Type—**Regex**
- Pattern String—**(8\d{3}4[^6-7]\d{2})@cisco.local(.\*)**
- Pattern behavior—**Replace**
- Replace String—**\1@10.4.48.111**
- On successful match—**Stop**
- Target—**CUCM\_Sub1 Neighbor**
- State—**Enabled**

**Configuration**

Rule name	* <input type="text" value="Route1 to CUCM_Sub1"/>	
Description	<input type="text" value="Send all 8XXX4XXX except 8XXX4[6-7]XX calls to CUCM"/>	
Priority	* <input type="text" value="100"/>	
Source	<input type="text" value="Any"/>	
Request must be authenticated	<input type="text" value="No"/>	
Mode	<input type="text" value="Alias pattern match"/>	
Pattern type	<input type="text" value="Regex"/>	
Pattern string	* <input type="text" value="(8\d{3}4[^6-7]\d{2})@cisco.local(.*)"/>	
Pattern behavior	<input type="text" value="Replace"/>	
Replace string	<input type="text" value="\1@10.4.48.111"/>	
On successful match	<input type="text" value="Stop"/>	
Target	* <input type="text" value="CUCM_Sub1 Neighbor"/>	
State	<input type="text" value="Enabled"/>	

**Step 7:** Navigate to **VCS configuration > Dial Plans > Search rules**, and then click **New**.

**Step 8:** Enter the following values, and then click **Create search rule**:

- Rule name—**Route2 to CUCM\_Sub1**
- Description—**Send all calls except 8XXX4XXX@cisco.local to CUCM**
- Priority—**102** (same priority for all subscribers)
- Source—**Any**
- Request must be Authenticated—**No**
- Mode—**Alias Pattern Match**
- Pattern Type—**Regex**
- Pattern String—**(8\d{3}[^4]\d{3})@cisco.local(.\*)**
- Pattern behavior—**Replace**
- Replace String—**\1@10.4.48.111**
- On successful match—**Stop**
- Target—**CUCM\_Sub1 Neighbor**
- State—**Enabled**

**Step 9:** Repeat Step 5 through Step 8 for each subscriber in the Unified CM cluster. Change the Rule name, Replace string's IP address and Target for each set of search rules.

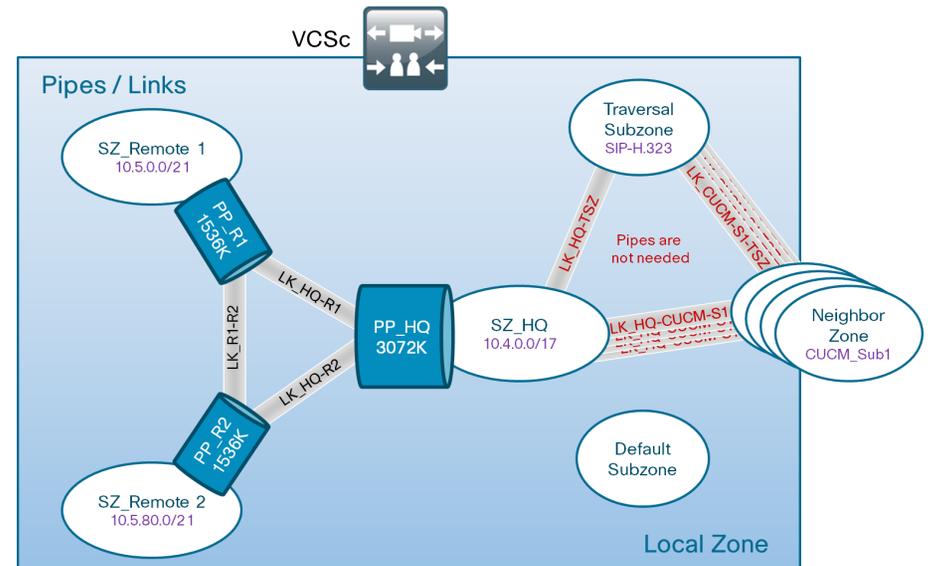
100	Enabled	Route1 to CUCM_Sub1	Any	No	Alias pattern match	Regex	(8\d{3}4[^6-7]\d{2})@cisco.local(.*)	Replace	Stop	CUCM_Sub1 Neighbor
100	Enabled	Route1 to CUCM_Sub2	Any	No	Alias pattern match	Regex	(8\d{3}4[^6-7]\d{2})@cisco.local(.*)	Replace	Stop	CUCM_Sub2 Neighbor
100	Enabled	Route1 to CUCM_Sub3	Any	No	Alias pattern match	Regex	(8\d{3}4[^6-7]\d{2})@cisco.local(.*)	Replace	Stop	CUCM_Sub3 Neighbor
100	Enabled	Route1 to CUCM_Sub4	Any	No	Alias pattern match	Regex	(8\d{3}4[^6-7]\d{2})@cisco.local(.*)	Replace	Stop	CUCM_Sub4 Neighbor
102	Enabled	Route2 to CUCM_Sub1	Any	No	Alias pattern match	Regex	(8\d{3}[^4]\d{3})@cisco.local(.*)	Replace	Stop	CUCM_Sub1 Neighbor
102	Enabled	Route2 to CUCM_Sub2	Any	No	Alias pattern match	Regex	(8\d{3}[^4]\d{3})@cisco.local(.*)	Replace	Stop	CUCM_Sub2 Neighbor
102	Enabled	Route2 to CUCM_Sub3	Any	No	Alias pattern match	Regex	(8\d{3}[^4]\d{3})@cisco.local(.*)	Replace	Stop	CUCM_Sub3 Neighbor
102	Enabled	Route2 to CUCM_Sub4	Any	No	Alias pattern match	Regex	(8\d{3}[^4]\d{3})@cisco.local(.*)	Replace	Stop	CUCM_Sub4 Neighbor

### Procedure 3

### Configure VCS call admission control

You modify call admission control from the VCS base configuration to accommodate the higher bandwidth requirements of the CTS endpoints. The remote-site locations allow a single call at 1536 kbps and the head-quarters site allows two calls at 1536 kbps. The additional WAN bandwidth permits higher quality video and audio between the locations.

A link is automatically created between the traversal subzone and the Unified CM neighbor zone, which permits H.323 calls to CTS endpoints. However, a link is needed between the neighbor zone and the headquarters subzone to allow SIP calls between the two systems. The bandwidth is controlled by the remote-site settings in each call agent, so pipes are not needed on the links to the neighbor zone.



**Step 1:** Navigate to **VCS Configuration > Bandwidth > Pipes**, and then click the name of the main site location—**PP\_HQ**.

**Step 2:** On the Edit pipe configuration screen, enter the following values, and then click **Save**:

- Total bandwidth limit (kbps)—**3072** (two 1.5 Mbps calls)
- Per call bandwidth limit (kbps)—**1536**

**Step 3:** On the Pipes screen, click the name of the remote site pipe—**PP\_R1**

**Step 4:** On the Edit pipe configuration screen, enter the following values, and then click **Save**:

- Total bandwidth limit (kbps)—**1536** (one 1.5 Mbps call)
- Per call bandwidth limit (kbps)—**1536**

**Step 5:** Repeat Step 3 and Step 4 for all remote-site locations. Change the Name for each Pipe.

**Step 6:** Navigate to **VCS Configuration > Bandwidth > Links**, and then click **New**.

**Step 7:** On the Create link screen, enter the following values, and then click **Create link**:

- Name—**LK\_HQ\_CUCM\_S1**
- Node 1—**SZ\_HQ**
- Node 2—**CUCM\_Sub1 Neighbor**

**Step 8:** Repeat Step 6 and Step 7 for each subscriber neighbor zone in the VCS cluster. Change the Name and Node 2 for each Link.

<a href="#">LK_HQ_CUCM_S1</a>	<a href="#">SZ_HQ</a>	<a href="#">CUCM_Sub1 Neighbor</a>	0 0 kbps
<a href="#">LK_HQ_CUCM_S2</a>	<a href="#">SZ_HQ</a>	<a href="#">CUCM_Sub2 Neighbor</a>	0 0 kbps
<a href="#">LK_HQ_CUCM_S3</a>	<a href="#">SZ_HQ</a>	<a href="#">CUCM_Sub3 Neighbor</a>	0 0 kbps
<a href="#">LK_HQ_CUCM_S4</a>	<a href="#">SZ_HQ</a>	<a href="#">CUCM_Sub4 Neighbor</a>	0 0 kbps

VCS creates default links to the CUCM Neighbor Zone. Step 9 and Step 10 modify the name of the Traversal Subzone link to make it more readable. Step 12 deletes the link to the Default Zone because it is not needed.

**Step 9:** From the Links screen, click **Zone001toTraversalSZ**.

**Step 10:** From the Edit link screen, change the name of the link to LK\_CUCM\_S1\_TSZ, and then click **Save**.

**Configuration**

Name: \* LK\_CUCM\_S1\_TSZ

Node 1: CUCM\_Sub1 Neighbor

Node 2: TraversalSubZone

Pipe 1:

Pipe 2:

**Step 11:** Repeat Step 9 and Step 10 for each Unified CM subscriber neighbor zone in the VCS cluster. Change the Name and Node 1 for each Link.

<a href="#">LK_CUCM_S1_TSZ</a>	<a href="#">CUCM_Sub1_Neighbor</a>	<a href="#">TraversalSubZone</a>	0	0 kbps
<a href="#">LK_CUCM_S2_TSZ</a>	<a href="#">CUCM_Sub2_Neighbor</a>	<a href="#">TraversalSubZone</a>	0	0 kbps
<a href="#">LK_CUCM_S3_TSZ</a>	<a href="#">CUCM_Sub3_Neighbor</a>	<a href="#">TraversalSubZone</a>	0	0 kbps
<a href="#">LK_CUCM_S4_TSZ</a>	<a href="#">CUCM_Sub4_Neighbor</a>	<a href="#">TraversalSubZone</a>	0	0 kbps

**Step 12:** From the Links screen, select **Zone001toDefaultSZ**, **Zone002toDefaultSZ**, **Zone003toDefaultSZ**, **Zone004toDefaultSZ**, click **Delete**, and then in the Confirm popup window click **Yes**.

<input checked="" type="checkbox"/>	<a href="#">Zone001ToDefaultSZ</a>	<a href="#">CUCM_Sub1_Neighbor</a>	<a href="#">DefaultSubZone</a>	0	0 kbps
<input checked="" type="checkbox"/>	<a href="#">Zone002ToDefaultSZ</a>	<a href="#">CUCM_Sub2_Neighbor</a>	<a href="#">DefaultSubZone</a>	0	0 kbps
<input checked="" type="checkbox"/>	<a href="#">Zone003ToDefaultSZ</a>	<a href="#">CUCM_Sub3_Neighbor</a>	<a href="#">DefaultSubZone</a>	0	0 kbps
<input checked="" type="checkbox"/>	<a href="#">Zone004ToDefaultSZ</a>	<a href="#">CUCM_Sub4_Neighbor</a>	<a href="#">DefaultSubZone</a>	0	0 kbps

#### Procedure 4 VCS to Unified CM dialing

After the configurations in both call agents are complete, place a numeric call from the VCS endpoint to the Unified CM endpoint to verify that everything is working as expected.

**Step 1:** If there is no menu on the screen, press the **Home** button on the remote.

**Step 2:** Enter the extension of a CTS endpoint **85194390** and press the green **Call** button.

**CALL**

85194390

Call

**Step 3:** Use the remote to navigate to **Home > Settings > System Information**, and on the Systems Information screen, verify the following settings:

- Video: Transmit: Channel Rate—**1472 kbps** (variable based on movement)
- Video: Receive: Channel Rate—**1472 kbps** (variable based on movement)
- Audio: Transmit: Channel Rate—**64 kbps**
- Audio: Receive: Channel Rate—**64 kbps**

**Step 4:** Press the red **End call** button to hang up the call.

#### Procedure 5 Unified CM to VCS dialing

Place a numeric call from a Unified CM endpoint to a VCS endpoint to verify everything is working as expected.

**Step 1:** On the associated phone, select **New Call**.

**Step 2:** Dial the four-digit extension of a multipurpose endpoint **85104600**, and then select **Dial**.

**New Call**

Number To Dial:

85104600

123

**Step 3:** Use your web browser to access the endpoints administrative interface <https://10.5.84.50/>, and then log in using the SSH admin username and password.

**Step 4:** On the Cisco TelePresence Systems Administration screen, enter the following values, and then click **Login**:

- Username—**admin**
- Password—**[password]**

**Step 5:** Navigate to **Monitoring > Call Statistics** to verify the bandwidth being used.

<b>Real Time Call Statistics</b>	
Call Connected	Yes
Registered to Cisco Unified Communications Manager	Yes
Local Number	85194390
<b>Audio/Video Call</b>	
Call Start Time	Wed Jun 13 17:59:38 2012
Call Duration	208 seconds
Call Type	Outgoing
Remote Number	85104600
Call State	Answered
Security Level	Non-Secure
Actual Bit Rate	1472000 bps, 1280x720
Negotiated Bit Rate	1472000 bps
<b>Historical Call Statistics (Not including current call, if any)</b>	
Call Statistics Clear Time	Sun Jan 15 06:57:26 2006
Last Call Start Time	Wed Jun 13 17:57:44 2012
Last Call Duration	59 seconds
Number of Calls Since System Setup	239
Time in Calls Since System Setup (seconds)	324739
Number of Calls Since Last Reboot	12
Time in Calls Since Last Reboot (seconds)	20338
Registered to Cisco Unified Communications Manager	Yes
Configured Bit Rate	Highest Detail, Best Motion: 1080p

**Step 6:** To hang up the call from the phone, select **End Call**.

## Process

Configuring Cisco TelePresence Server

1. Configure MCU connectivity to the LAN
2. Prepare the Cisco MCU platform
3. Configure the Cisco MCU
4. Configure SIP Trunk from Unified CM
5. Configure search rule from VCS to MCU

**Step 1:** The Cisco TelePresence Server, also known as a Multipoint Control Unit (MCU), is used for reservationless and scheduled conferences between the video endpoints. Cisco has several MCUs with different capacities. Depending on how many endpoints you need in concurrent calls, you can choose the MCU that scales to your needs.

If your organization plans to make extensive use of reservationless conferences, Cisco recommends separating the two conference types onto two MCUs. Separating the two conference types prevents reservationless conferences from using all of the resources on the MCU that supports scheduled conferences.

**Step 2:** Scheduled conference calls are created on the Cisco MCU for call-in and call-out types of meetings. Before getting started, you need to collect certain information specific to your site. You can fill in the following table.

Table 1 - Information you need before configuring Cisco TelePresence Server

Item	Cisco SBA configuration	Site-specific details
IPV4 address	10.4.48.136	
IPV4 subnet	255.255.255.0	
IPV4 default gateway	10.4.48.1	
Host name	TS7010	
DNS server address	10.4.48.10	
DNS local host name	TS7010	
DNS domain name	cisco.local	
NTP server address	10.4.48.17	
Time zone	Pacific -8	
SNMP read-only community	cisco	
SNMP read/write community	cisco123	
SNMP trap community	cisco	
Remote syslog server	10.4.48.35	

**Step 3:** Configure the port as an access port and apply the QoS policy.

```
interface Ethernet107/1/4
description TS7010
switchport access vlan 148
spanning-tree port type edge
service-policy type qos input DC-FCOE+1P4Q_INTERFACE-DSCP-QOS
```

i **Tech Tip**

When deploying a dual-homed Nexus 2248, this configuration is applied to both Nexus 5548s.

## Procedure 1

### Configure MCU connectivity to the LAN

The TelePresence Server can be connected to a Nexus switch in the Data Center or a Catalyst switch in the Server Room. In both cases, QoS policies are added to the ports to maintain video quality during conferences. Please choose the option that is appropriate for your environment.

#### Option 1. Connect the TS7010 to a Nexus 2248UP

**Step 1:** Login to the Nexus switch with a username that has the ability to make configuration changes.

**Step 2:** If there is a previous configuration on the switch port where the TS7010 is connected, remove the individual commands by issuing a **no** in front of each one to bring the port back to its default state.

#### Option 2. Connect the TS7010 to a Catalyst 3750-X

To ensure that video traffic is prioritized appropriately, you must configure the Catalyst access switch port where the TS7010 is connected to trust the Differentiated Services Code Point (DSCP) markings. The easiest way to do this is to clear the interface of any previous configuration and then, apply the egress QoS macro that was defined in the access-switch platform configuration of the Cisco SBA—*Borderless Networks LAN Deployment Guide*.

**Step 1:** Login to the Catalyst switch with a username that has the ability to make configuration changes, and enter enable mode.

**Step 2:** Clear the interface's configuration on the switch port where the TS7010 is connected.

```
default interface GigabitEthernet1/0/12
```

**Step 3:** Configure the port as an access port and apply the Egress QoS policy.

```
interface GigabitEthernet1/0/12
description TS7010
switchport access vlan 148
switchport host
macro apply EgressQoS
```

## Procedure 2 Prepare the Cisco MCU platform

In the following steps, you set the initial configuration by using a PC connected to the console port with a serial cable.

**Step 1:** Ensure power is connected to Cisco MCU and the Status LED is green.

**Step 2:** Connect the Ethernet LAN cable from the Ethernet A port on the front of the unit to your network.

**Step 3:** Connect the console port of Cisco MCU to the serial port of your PC using the blue RJ45 to DB9 cable supplied.

**Step 4:** Use terminal emulation software such as PuTTY and configure the serial port on the PC as follows:

- Baud rate—**38400**
- Data bits—**8**
- Parity—**none**
- Stop bits—**1**
- Flow control—**none**

**Step 5:** Press **Enter**. The MCU command prompt appears on the terminal.

**Step 6:** Configure Ethernet Port A for auto-sensing.

```
ethertype auto
```

**Step 7:** Assign a static IP address, subnet mask, default gateway and DNS server.

```
static A 10.4.48.136 255.255.255.0 10.4.48.1 10.4.48.10
```

**Step 8:** Disconnect the serial cable and store it in a safe place.

## Procedure 3 Configure the Cisco MCU

The rest of the configuration of the Cisco MCU is done using a standard web browser. Use the information collected in Table 1 at the beginning of this configuration process to fill in the fields.

**Step 1:** Using your web browser, access the administration interface of the Cisco MCU.

**Step 2:** Enter the following values and click **Log in**:

- Username—**admin**
- Password—(leave the **password** field blank)

**Step 3:** Using the drop down menu navigate to **Configuration > Change password**.

**Step 4:** On the Change password screen, enter the following values, and then click **Change password**.

- New password—**[password]**
- Re-enter password—**[password]**

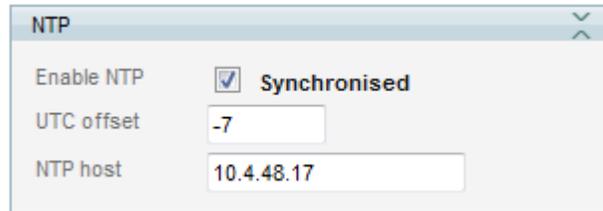
**Step 5:** Navigate to **Network > DNS**, enter the following values, and then click **Update DNS configuration**:

- DNS configuration—**Manual**
- Host name—**TS7010**
- Name server—**10.4.48.10**
- Domain name (DNS suffix)—**cisco.local**

DNS configuration	
DNS configuration	Manual
Host name	TS7010
Name server	10.4.48.10
Secondary name server	
Domain name (DNS suffix)	cisco.local
<input type="button" value="Update DNS configuration"/>	

**Step 6:** Navigate to **Configuration > Time**, select **Enable NTP**, enter the following values, and then click **Update NTP settings**:

- UTC offset— **-7**
- NTP host IP address— **10.4.48.17**



NTP	
Enable NTP	<input checked="" type="checkbox"/> Synchronised
UTC offset	<input type="text" value="-7"/>
NTP host	<input type="text" value="10.4.48.17"/>

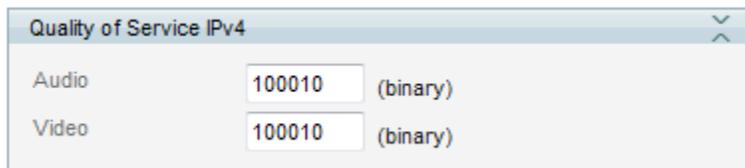
### Tech Tip

QoS is needed to put the media and signaling traffic into the low-latency queues defined in the *LAN Deployment Guide*. The QoS setting gives the video packets a higher priority over non-real-time traffic in the data queues.

The Differentiated Service markings match the medianet-recommended settings for interactive video traffic in Cisco SBA.

**Step 7:** Navigate to **Network > QoS**, enter the following values under Quality of Service IPv4, and then click **Update QoS settings**:

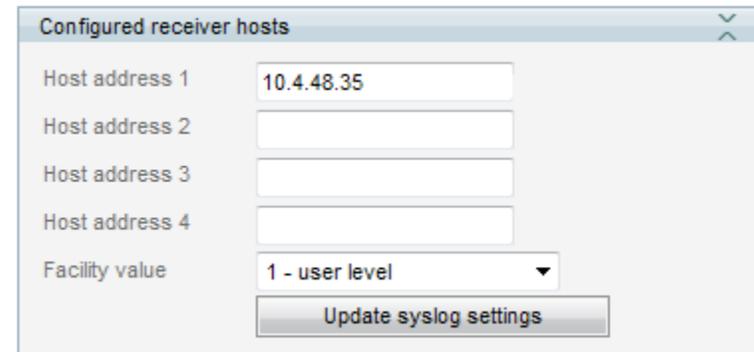
- Audio— **100010** (AF41)
- Video— **100010** (AF41)



Quality of Service IPv4	
Audio	<input type="text" value="100010"/> (binary)
Video	<input type="text" value="100010"/> (binary)

By default, the system log level is set to level 1. This setting configures Cisco MCU to output high-level (easily readable) events in system log and syslog messages. The system logs are stored on a Solarwinds server at the IP address listed below. Administrators can use the information when troubleshooting problems with the device.

**Step 8:** Navigate to **Logs > Syslog**, in the **Host address 1** box, enter **10.4.48.35**, and then click **Update syslog settings**.



Configured receiver hosts	
Host address 1	<input type="text" value="10.4.48.35"/>
Host address 2	<input type="text"/>
Host address 3	<input type="text"/>
Host address 4	<input type="text"/>
Facility value	<input type="text" value="1 - user level"/>
<input type="button" value="Update syslog settings"/>	

The platform configuration of the Cisco MCU is complete.

### **Procedure 4** Configure SIP Trunk from Unified CM

Configure a Cisco TelePresence Server with a SIP Trunk from Unified CM to allow the MCU to accept reservationless calls that are made using a service prefix. This is a simple method for allowing endpoints to dial a common phone number and be connected directly into the conference bridge without pausing at the Auto Attendant. It also allows for a common voice signaling integration strategy with Unified CM.

The SIP trunk between the two systems will also allow the MCU to call video endpoints registered to Unified CM or VCS at the start of scheduled conferences.

**Step 1:** From the main menu of the TelePresence Server, navigate to **Configuration > System settings**, enter the following values in the **SIP configuration section**, and then click **Apply changes**:

- Outbound call configuration—**Use Trunk**
- Outbound address—**10.4.48.111**
- Outbound domain—**10.4.48.111** (domain for Unified CM subscriber)

**Step 2:** At the top of the page on the right side, click **Log out**.

**Step 3:** Using your web browser, access the Unified CM Administration interface of the publisher in your cluster.

**Step 4:** In the center of the page under Installed Applications, click the **Cisco Unified Communications Manager** link.

**Step 5:** Enter the **Username** and **Password** you created for the application administrator, and then click **Login**.

**Step 6:** Navigate to **Device > Trunk** and click **Add New**.

**Step 7:** Under **Trunk Type** select **SIP Trunk** and click **Next**.

**Step 8:** Enter the following values in the **Device Information** configuration section.

- Device Name—**SIP\_TS7010**
- Description—**SIP Trunk to TelePresence Server 7010**
- Device Pool—**DP\_HQ1\_1**
- Call Classification—**OnNet**
- Location—**Hub\_None**
- Retry Video Call as Audio—**Yes**

In the **Inbound Calls** section under the **Call Routing Information** section, use the drop down labeled **Calling Search Space** to select **CSS\_Base**.

**Step 9:** Enter the following values in the **SIP Information** section, and then click **Save**.

- Destination Address—**10.4.48.136**
- Destination Port—**5060**
- SIP Trunk Security Profile—**Non Secure SIP Trunk Profile**
- SIP Profile—**Standard SIP Profile**

**Destination**

Destination Address is an SRV

1\*

MTP Preferred Originating Codec\*

Presence Group\*

SIP Trunk Security Profile\*

Relouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile\*

DTMF Signaling Method\*

**Step 10:** On the Message popup, click **OK**.

**Step 11:** On the Trunk Configuration screen, click **Reset**.

**Step 12:** From the Device Reset screen, click **Reset**, and then click **Close**.

**Reset Information**

**Selected Device: SIP\_TS7010 (SIP Trunk to TelePresence Server 7010; SIP Trunk)**

If a device is not registered with Cisco Unified Communications Manager, you cannot reset or restart it. If a device is registered, to restart a device without shutting it down, click the **Restart** button. To shut down a device and bring it back up, click the **Reset** button. To return to the previous window without resetting/restarting the device, click **Close**.

**Note:**  
Resetting a gateway/trunk/media devices **drops** any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.

**Step 13:** Navigate to **Call Routing > Route/Hunt > Route Group** and click **Add New**.

**Step 14:** On the Route Group Configuration screen, enter the Route Group Name: **RG\_TS7010\_SIP**.

**Step 15:** From the Available Devices, choose **SIP\_TS7010 (All Ports)**, click **Add to Route Group**, and then click **Save**.

**Route Group Information**

Route Group Name\*

Distribution Algorithm\*

**Route Group Member Information**

**Find Devices to Add to Route Group**

Device Name contains

Available Devices\*\*

- SIP\_RS211\_GWY
- SIP\_RS221\_GWY
- SIP\_RS222\_GWY
- SIP\_TS7010**
- SIP\_VCS\_Trunk

Port(s)

**Current Route Group Members**

Selected Devices (ordered by priority)\*

- SIP\_TS7010 (All Ports)

Removed Devices\*\*

**Step 16:** Navigate to **Call Routing > Route/Hunt > Route List** and click **Add New**.

**Step 17:** On the Route Group Configuration screen, enter the following values, and then click **Save**:

- Name—**RL\_TS7010**
- Description—**Route List for TelePresence Server 7010**
- Cisco Unified Communications Manager Group—**Sub1\_Sub2**

**Route List Information**

Device is trusted

Name\*

Description

Cisco Unified Communications Manager Group\*

**Step 18:** On the Route List Configuration screen, click **Add Route Group**.

**Step 19:** On the Route List Detail Configuration screen, enter the following value, and then click **Save**:

- Route Group—**RG\_TS7010\_SIP-[NON-QSIG]**

**Route List Member Information**

Route Group\*

---

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask\*

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Party Number Type\*

Calling Party Numbering Plan\*

---

**Called Party Transformations**

Discard Digits

Called Party Transform Mask

Prefix Digits (Outgoing Calls)

Called Party Number Type\*

Called Party Numbering Plan\*

This design uses a 3 digit prefix to differentiate between meeting types and a 4 digit meeting identifier for a total of 7 digits. The 885 prefix is for adhoc and the 886 prefix is for scheduled conferences.

**Step 20:** Navigate to **Call Routing > Route/Hunt > Route Pattern** and click **Add New**.

**Step 21:** On the Route Pattern Configuration screen, enter the following values, and then click **Save**:

- Route Pattern—**88[5-6]XXXX**
- Route Partition—**PAR\_Base**
- Description—**Route Pattern for TelePresence Server 7010**
- Gateway/Route List—**RL\_TS7010**
- Call Classification—**OnNet**
- Provide Outside Dial Tone—**No** (Unchecked)

**Pattern Definition**

Route Pattern\*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence\*

Apply Call Blocking Percentage

Resource Priority Namespace

Network Domain

Route Class\*

Gateway/Route List\*  [\(Edit\)](#)

Route Option

Route this pattern

Block this pattern

Call Classification\*

Allow Device Override  Provide Outside Dial Tone  Allow Overlap Sending  Urgent Priority

Require Forced Authorization Code

Authorization Level\*

Require Client Matter Code

### Procedure 5

### Configure search rule from VCS to MCU

An additional set of search rules are required on the VCS cluster to allow the multipurpose endpoints to call the conferences on the Cisco TelePresence server which is registered to Unified CM. You create search rules with the

same priority to send calls to the neighbor zones defined for the Unified CM cluster. The local domain name is replaced with the IP address of the specified Unified CM subscriber.

The calls will round robin between search rules with the same priority which in turn will round robin between the Unified CM subscribers. If a subscriber is unreachable, the zone will become inactive and the search rule for the unreachable subscriber will be ignored until it comes back online.

This design uses a 3 digit prefix to differentiate between meeting types and a 4 digit meeting identifier for a total of 7 digits. The 885 prefix is for adhoc and the 886 prefix is for scheduled conferences.

**Step 1:** Using your web browser, access the administration interface of the master VCS in your cluster, and then click **Administrator login**.

**Step 2:** Enter the following values, and then click **Login**:

- Username—**admin**
- Password—**[password]**

**Step 3:** Navigate to **VCS configuration > Dial Plans > Search rules**, and then click **New**.

**Step 4:** Enter the following values, and then click **Create search rule**:

- Rule name—**Route to MCU on CUCM\_Sub1**
- Description—**Send 88[5-6]XXXX calls to CUCM for MCU**
- Priority—**110**
- Source—**Any**
- Request must be Authenticated—**No**
- Mode—**Alias Pattern Match**
- Pattern Type—**Regex**
- Pattern String—**(88[5-6]\d{4})@cisco.local(.\*)**
- Pattern behavior—**Replace**
- Replace String—**\1@10.4.48.111**
- On successful match—**Stop**
- Target—**CUCM\_Sub1 Neighbor**
- State—**Enabled**

The screenshot shows the configuration interface for a search rule. The fields are as follows:

Field	Value
Rule name	Route to MCU on CUCM_Sub1
Description	Send 88[5-6]XXXX calls to CUCM for MCU
Priority	110
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	(88[5-6]\d{4})@cisco.local(.*)
Pattern behavior	Replace
Replace string	\1@10.4.48.111
On successful match	Stop
Target	CUCM_Sub1 Neighbor
State	Enabled

**Step 5:** Repeat Step 3 and Step 4 for the subscribers in the Unified CM cluster. Change the Rule name, Replace string's IP address and Target for each Search rule.

110	✓ Enabled	<a href="#">Route to MCU on CUCM_Sub1</a>	Any	No	Alias pattern match	Regex	(88[5-6]d{4})@cisco.local(.*)	Replace	Stop	<a href="#">CUCM_Sub1 Neighbor</a>
110	✓ Enabled	<a href="#">Route to MCU on CUCM_Sub2</a>	Any	No	Alias pattern match	Regex	(88[5-6]d{4})@cisco.local(.*)	Replace	Stop	<a href="#">CUCM_Sub2 Neighbor</a>
110	✓ Enabled	<a href="#">Route to MCU on CUCM_Sub3</a>	Any	No	Alias pattern match	Regex	(88[5-6]d{4})@cisco.local(.*)	Replace	Stop	<a href="#">CUCM_Sub3 Neighbor</a>
110	✓ Enabled	<a href="#">Route to MCU on CUCM_Sub4</a>	Any	No	Alias pattern match	Regex	(88[5-6]d{4})@cisco.local(.*)	Replace	Stop	<a href="#">CUCM_Sub4 Neighbor</a>

## Process

Configuring Reservationless and Scheduled Conferences

1. Configure reservationless conferences
2. Configure scheduled conferences

Configure reservationless conferences first and then move to scheduled conferences. The scheduled conference configuration includes one conference where participants call in and another where the Cisco MCU calls each participant at the appointed time.

### Procedure 1 **Configure reservationless conferences**

On the TelePresence Server, reservationless conferences are created via web console. This type of conference is not scheduled ahead of time, so the resources are not reserved on the Cisco MCU.

Individual users or groups are assigned logins that have privileges to create reservationless meetings. Participants are added to the conference by dialing out from the web interface or by users dialing into the meeting with a predefined meeting number. Video endpoints can be added mid-conference if needed.

This example shows this adhoc meeting from the perspective of the administrator acting as the meeting originator. The administrator has to create the endpoints, the meeting room and the users before creating a conference for the first time.

To start the conference, the meeting originator logs into the web based user interface, initiates a meeting with two participants, and adds another

endpoint midway through the call via the web console. Another user joins by dialing the meeting number, and finally the meeting originator ends the conference.

**Step 1:** Using your web browser, access the administration interface of the Cisco MCU.

**Step 2:** Enter the following values and click **Log in**:

- Username—**admin**
- Password—**[password]**

**Step 3:** Navigate to **Endpoints > Endpoints** and click **Add new endpoint**.



### Tech Tip

In this design, all call control traffic from the Cisco MCU traverses a SIP trunk to Unified CM for call routing. The Call Protocol is always SIP and the Address is always the number without a domain regardless of the endpoints signaling protocol or IP address.

**Step 4:** Enter the following values in the **Endpoint** configuration section and click **Add new endpoint**.

- Name—**RS208 TX1300**
- Address—**85194390**
- Call Protocol—**SIP**

<b>Endpoint</b>	
Name	RS208 TX1300
Type	Standard
Display name override	
Minimum screen layout	Auto detect
Received audio gain	0 dB
Transmitted audio gain	0 dB
<b>Call-out parameters</b>	
Address	85194390
Call protocol	SIP

**Step 5:** Repeat Step 3 and Step 4 for additional endpoints. Change the Name and Address for each Endpoint.

### Tech Tip

The Third party interop feature is required on the Cisco TelePresence Server to create a room. Navigate to **Configuration > Upgrade** and scroll down to the Feature Management section to confirm. Please contact your Cisco representative if the feature is not present on your system.

**Step 6:** Navigate to **Rooms > Rooms** and click **Add new room**.

**Step 7:** Enter the following values in the **Room** configuration section and click **Add new room**.

- Name—**Reservationless Meeting Room**
- User ID—**reservationless\_user**
- Password—**[password]**
- Endpoint—**RS208 TX1300**
- Numeric ID—**8851000**

<b>Room</b>	
Name	Reservationless Meeting Room
User ID	reservationless_user
Password	••••••••
Endpoint	RS208 TX1300
Allow call-out to user-supplied address	<input checked="" type="checkbox"/>
Add all endpoints to conference	<input type="checkbox"/>
<b>Conferences</b>	
Numeric ID	8851000
Register numeric ID with H.323 gatekeeper	<input type="checkbox"/>
Register numeric ID with SIP registrar	<input type="checkbox"/>
Conference locked	<input type="checkbox"/>
Encryption	Optional
Use OneTable mode when appropriate	4 person mode
Content channel	Enabled
<input type="button" value="Add new room"/> <input type="button" value="Change password"/>	

**Step 8:** Repeat Step 6 and Step 7 for additional rooms. Change the Name, User ID, Password, Endpoint and Numeric ID for each room.

Preconfigured endpoints can be added to a Room so that users can quickly dial out to other endpoints.

**Step 9:** In the Pre-configured participants section, click **Add pre-configured participants**.

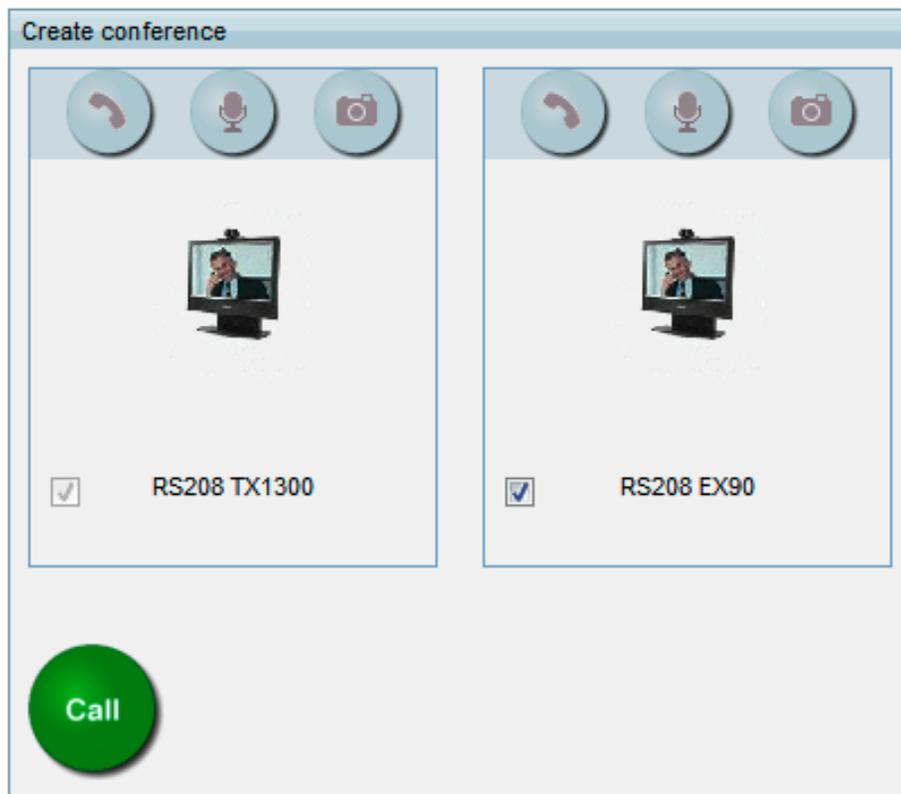
**Step 10:** Select the desired endpoints to be added and click **Update conference**. In the example **RS208 EX90** and **RS232 TX1300** are selected.

**Step 11:** To test the configuration, logout of the administrator account by clicking the **key icon** near the top right of the page.

**Step 12:** On the Log in screen, enter the following values from Step 7 and click **Log in**:

- Username—**reservationless\_user**
- Password—**[password]**

**Step 13:** Start a meeting with two participants by selecting an additional pre-configured participant. In this example **RS208 EX90** is selected. To initiate the meeting, click the green circle labeled **Call**.



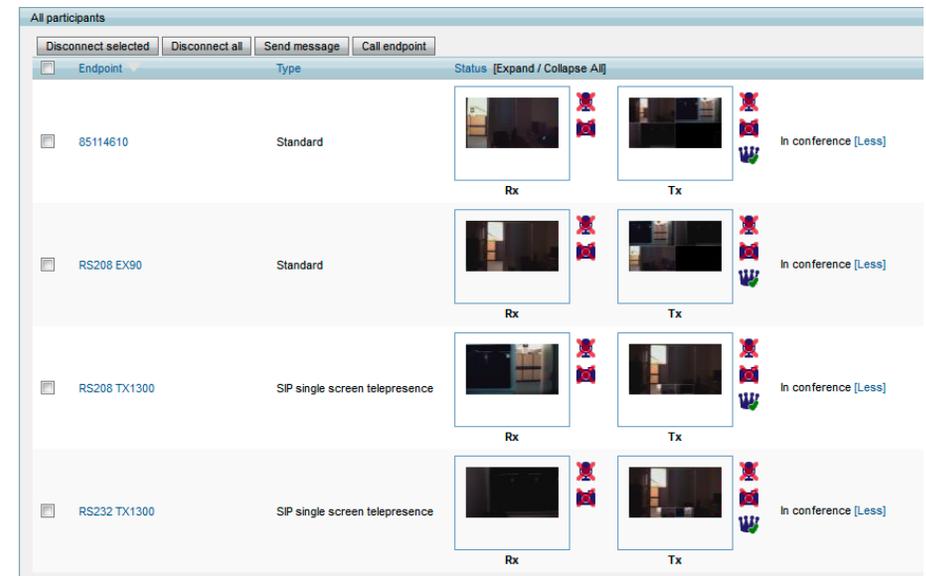
**Step 14:** Add an additional pre-configured participant midway through the call by selecting the participant and click the green circle labeled **Call**.

**Step 15:** Another video endpoint can dial in using the **Numeric ID** configured in Step 7.

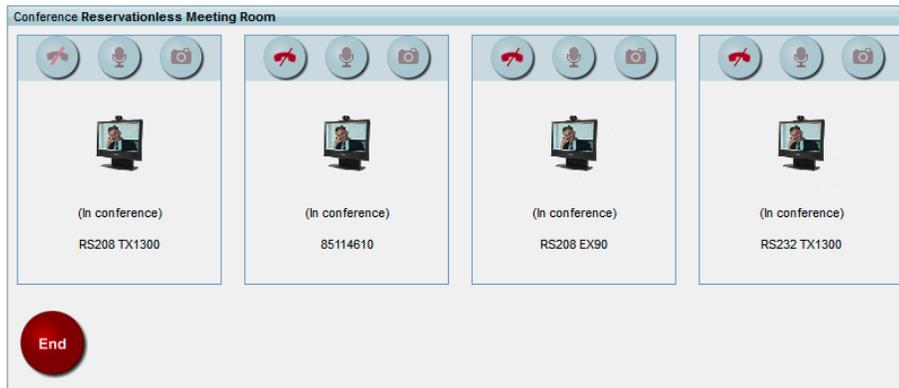
**Step 16:** The conference can be monitored by the administrator if necessary. Using the methods outlined in Step 1 and Step 2, log into the administrator console.

**Step 17:** As the administrator, navigate to **Conferences > Conferences** and click the room name: **Reservationless Meeting Room (room)**

**Step 18:** Click **[more]** next to the endpoints to see **Rx** and **Tx** video for each endpoint as well as control video mute, audio mute, and to assign importance.



**Step 19:** Reservationless meetings are ended by the meeting originator leaving the conference or by clicking red circle labeled **End**.



**Step 3:** Use Step 2 and Step 3 from Procedure 1 "Configure reservationless conferences" to create additional endpoints, if needed.

The next set of steps will create a onetime call-out conference.

**Step 4:** Navigate to **Conferences > Conferences** and click **Add new conference**.

**Step 5:** Enter the following values in the **Conference** configuration section and click **Add new conference**.

- Name—**Onetime Call-Out**
- Numeric ID—**8861234**
- Schedule—**Yes**
- Start time—**[start of meeting]**
- End time—**[end of meeting]**

## Procedure 2 Configure scheduled conferences

Scheduled conferences are created on Cisco MCU by the administrator. The endpoints can call into the conference, or the MCU can dial out to the endpoints at the start of the meeting. A permanent meeting can also be created that reserves the resources of a particular meeting and can be used at any time by the participants.

Scheduled conferences have a prefix of 886. This allows them to be differentiated from the reservationless conferences, which start with 885. In this example, a onetime call-out conference will use the ID of 8861234 and a permanent call-in conference will use 8866789.

If you want Cisco MCU to call the participants at the beginning of the meeting, the endpoint information is entered into the MCU ahead of time. SIP or H323 endpoints are added to the MCU before creating the conferences.

**Step 1:** Using your web browser, access the administration interface of the Cisco MCU.

**Step 2:** Enter the following values and click **Log in**:

- Username—**admin**
- Password—**[password]**

**Step 6:** Click **Add pre-configured participants**, select **RS200 E20** and **RS200 EX90**, and then click **Update**.

**Conference**

Name: Onetime Call-Out  
 Numeric ID: 8851234  
 Register numeric ID with H.323 gatekeeper:   
 Register numeric ID with SIP registrar:   
 Conference locked:   
 Encryption: Optional  
 Use OneTable mode when appropriate: 4 person mode  
 Content channel: Enabled  
 Port limits: Video: 0, Audio only: 0  
 Show lobby screen: <use default>  
 Lobby message:   
 Scheduling: Schedule:   
 Start time: 17 : 00 Date: 19 June 2012  
 Permanent:   
 End time: 18 : 00 Date: 19 June 2012  
 Conference ending notification: <use default>  
 Update conference Start now

**Pre-configured participants**

Delete selected Add pre-configured participants

Endpoint	Type	Status
<input checked="" type="checkbox"/> RS200 E20	Standard	Available
<input checked="" type="checkbox"/> RS200 EX90	Standard	Available

The next set of steps will create a permanent call-in conference.

**Step 7:** Navigate to **Conferences > Conferences** and click **Add new conference**.

**Step 8:** Enter the following values in the **Conference** configuration section and click **Add new conference**.

- Name—**Permanent Call-In**
- Numeric ID—**8866789**
- Schedule—**Yes**
- Start time—**[current time and date]**
- Permanent—**Yes**

**Conference**

Name: Permanent Call-in  
 Numeric ID: 8866789  
 Register numeric ID with H.323 gatekeeper:   
 Register numeric ID with SIP registrar:   
 Conference locked:   
 Encryption: Optional  
 Use OneTable mode when appropriate: 4 person mode  
 Content channel: Enabled  
 Port limits: Video: 0, Audio only: 0  
 Show lobby screen: <use default>  
 Lobby message:   
 Scheduling: Schedule:   
 Start time: 15 : 00 Date: 21 June 2012  
 Permanent:   
 End time: 16 : 00 Date: 21 June 2012  
 Conference ending notification: <use default>  
 Add new conference

**Pre-configured participants**

Delete selected Add pre-configured participants

Endpoint	Type	Status
<input checked="" type="checkbox"/> Permanent Call-In	Standard	Available
<input checked="" type="checkbox"/> Permanent Call-Out	Standard	Available

The conference scheduling section is complete.

# Appendix A: Product List

## Data Center or Server Room

Functional Area	Product Description	Part Numbers	Software
Call Control for Multipurpose Endpoints	Cisco TelePresence Video Communication Server Control	CTI-VCS-BASE-K9	X7.1.0
	License Key - VCS K9 Software Image	LIC-VCS-BASE-K9	
	Enable Device Provisioning, Free, VCS Control ONLY	LIC-VCS-DEVPROV	
	Enable GW Feature (H323-SIP)	LIC-VCS-GW	
	100 Traversal Calls for VCS Control only	LIC-VCSE-100	
Call Control for Immersive Endpoints	Cisco Media Convergence Server 7845-I3 for Unified Communications Manager up to 10,000 users	MCS7845I3-K9-CMD3A	8.6(2a)SU1
	Cisco Media Convergence Server 7835-I3 for Unified Communications Manager up to 2500 users	MCS7835I3-K9-CMD3A	
Call Control Virtual Servers for Immersive Endpoints	Cisco UCS C210 M2 General-Purpose Rack-Mount Server for unified communications applications	UCS-C210M2-VCD2	8.6(2a)SU1 ESXi4.1
	Cisco UCS C200 M2 High-Density Rack-Mount Server for unified communications applications	UCS-C200M2-VCD2	
	Unified CMBE6K UCS C200M2 for Unified Communications Manager up to 500 users	UCS-C200M2-BE6K	
Multipoint Control Unit	Cisco TelePresence Server 7010	CTI-7010-TPSRV-K9	2.2(1.54)
	TS-7000 9 Screen Default License	LIC-7000-TPSRV9	
	AES and HTTPS Enable Upgrade	LIC-AESCDN6-K9	
	License Key For 7010 TelePresence Server software Image	LIC-7010-TPSRV9	
	Software image for 7000 Telepresence Server, Latest Version	SW-7000-TPSRV9	

## Video Endpoints

Functional Area	Product Description	Part Numbers	Software
Executive Room System	Cisco TelePresence System EX90 w NPP, Touch UI	CTS-EX90-K9	TC5.1.0
	Cisco TelePresence Touch 8-inch for EX Series	CTS-CTRL-DV8	
	Software 5.x Encryption	SW-S52000-TC5.XK9	
	Cisco TelePresence Executive 90 Product License Key	LIC-EX90	
	Cisco TelePresence EX Series NPP Option	LIC-ECXX-NPP	
	Cisco TelePresence System License Key Software Encrypted	LIC-S52000-TC5.XK9	
Multipurpose Room System	Cisco TelePresence Profile 42 w PHD 1080p 12x Cam, NPP, Touch, 2 Mics	CTS-P42C40-K9	TC5.1.0
	Cisco TelePresence Monitor Assembly 42	CTS-P42MONITOR	
	Cisco TelePresence Profile 42, 52 and 55 in single screen Wheel Base Mount Kit	CTS-P4252S-WBK	
	Cisco TelePresence Profile 42 C40 Product ID	LIC-P42SC40	
	Codec C40	CTS-C40CODEC-K9-	
	Cisco TelePresence Touch 8-inch for C Series, Profile Series, Quick Set C20	CTS-CTRL-DVC8	
	Cisco TelePresence System DNAM III	CTS-DNAM-III-	
	Cisco TelePresence Precision HD 1080p 12X Unit - Silver, + indicates auto expand	CTS-PHD-1080P12XS+	
	Cisco TelePresence Remote Control TRC 5	CTS-RMT-TRC5	
	Cisco TelePresence Profile Series NPP option	LIC-PCXX-NPP	
	Software 5.x Encryption	SW-S52000-TC5.XK9	
	Video Telephones	Unified IP Phone with six lines, video, color, Wi-Fi, Bluetooth, USB	
Unified IP Phone with four lines, video, color		CP-8945	9-1-2-SR-1
CTS Immersive Endpoints	Cisco TelePresence System 1100 for 1 or 2 users	CTS-1100	1.8.2(11)
	Cisco TelePresence System 500 for 1 or 2 users	CTS-500-32	
	Cisco TelePresence System 500 Table Stand	CTS500-STRUC-TABL	
CTS Phone	Unified IP Phone with eight lines, color for CTS control	CP-7975G-CTS	9-2-1S SIP

## Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.1(3)N1(1a) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

## Server Room

Functional Area	Product Description	Part Numbers	Software
Stackable Ethernet Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 ports	WS-C3750X-48T-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Ethernet Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 ports	WS-C3560X-48T-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 ports	WS-C3560X-24T-S	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

## LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

# Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We added a Cisco TelePresence Server conferencing section to describe how to configure the MCU with a SIP trunk to Unified CM. We also discuss how to create and manage reservationless and scheduled conferences with the MCU.
- We created a VCS-specific standard SIP profile and a non-secure SIP trunk security profile in Unified CM to align with the recommended configuration of the VCS SIP trunk.
- We added resiliency to the zones, search rules and transforms in VCS to take into account the redundant VCS and Unified CM cluster configurations.
- We added the steps for updating the CTS endpoint software and the associated phone application software to the Unified CM TFTP servers.
- We changed the dial plan information, to align it with new video integration guides. This change ensures the video guides use a common set of extension numbers and dialing rules.
- We updated the software on the video infrastructure equipment and the endpoints to the latest shipping versions.

## Notes

## Feedback

Click [here](#) to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)