VCS and UCM Video Integration

TECHNOLOGY DESIGN GUIDE

August 2013

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. 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 at a CLI or script prompt appear as follows:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

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 feedback form.

For the most recent CVD guides, see the following site:

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

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- Multipurpose and Immersive Video System Integration—Organizations with multipurpose room systems and immersive systems want an easy way to manage their disparate video solutions, from a centralized location, without replicating costly components at their remote sites.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- Multipurpose video call agent
- Immersive video call agent
- Multipurpose room systems
- Immersive room systems
- Executive video endpoints
- Multipoint control unit
- H.323 and Session Initiation Protocol (SIP) signaling
- Quality of service (QoS) and bandwidth control

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Video**—1 to 3 years configuring voice devices and video single-screen endpoints, supporting telephony and video applications, and troubleshooting
- **CCNP Voice**—3 to 5 years designing, installing, and troubleshooting voice and unified communications applications, devices, and networks

Related CVD Guides

- Telephony Using Cisco UCM Technology Design Guide
- SIP Video Using VCS Technology Design Guide
- H.323 Video Interworking Using VCS Technology Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

Introduction

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. They give the users the sense of being in the same room, and are designed to make participants to feel as if they are meeting each other in person.

Technology Use Case

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. Organizations want the multipurpose workrooms to connect with the boardroom, and they want 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.

Use Case: Multipurpose and Immersive Video System Integration

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. Organizations need an easy way to manage their video from a central location without replicating costly components at their remote sites.

This design guide enables the following capabilities:

- Single-cluster, centralized design to simplify deployment and management while saving on infrastructure components
- Multipurpose endpoints that register to Cisco TelePresence Video Communication Server (VCS) and maintain their advanced features, like duo-video, far end camera control (FECC), and multisite/multiway conferencing
- Cisco TelePresence System (CTS) and video telephony endpoints that register with Cisco Unified CM and maintain their centralized software updates, dynamic configuration settings, and simple, one-touch interfaces
- Numeric dialing to allow legacy H.323 systems and video-enabled IP phones to participate in calls
- Calls that can be made between the call agents by using dialing rules that are familiar to each type of user
- Multipurpose endpoints with unique phone number ranges to simplify the routing of calls between the two call agents
- Quality of service (QoS) that is configured differently for each solution, so the traffic is properly identified in the network infrastructure

Design 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 is deployed as 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).

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 connects to Unified CM using a SIP trunk.

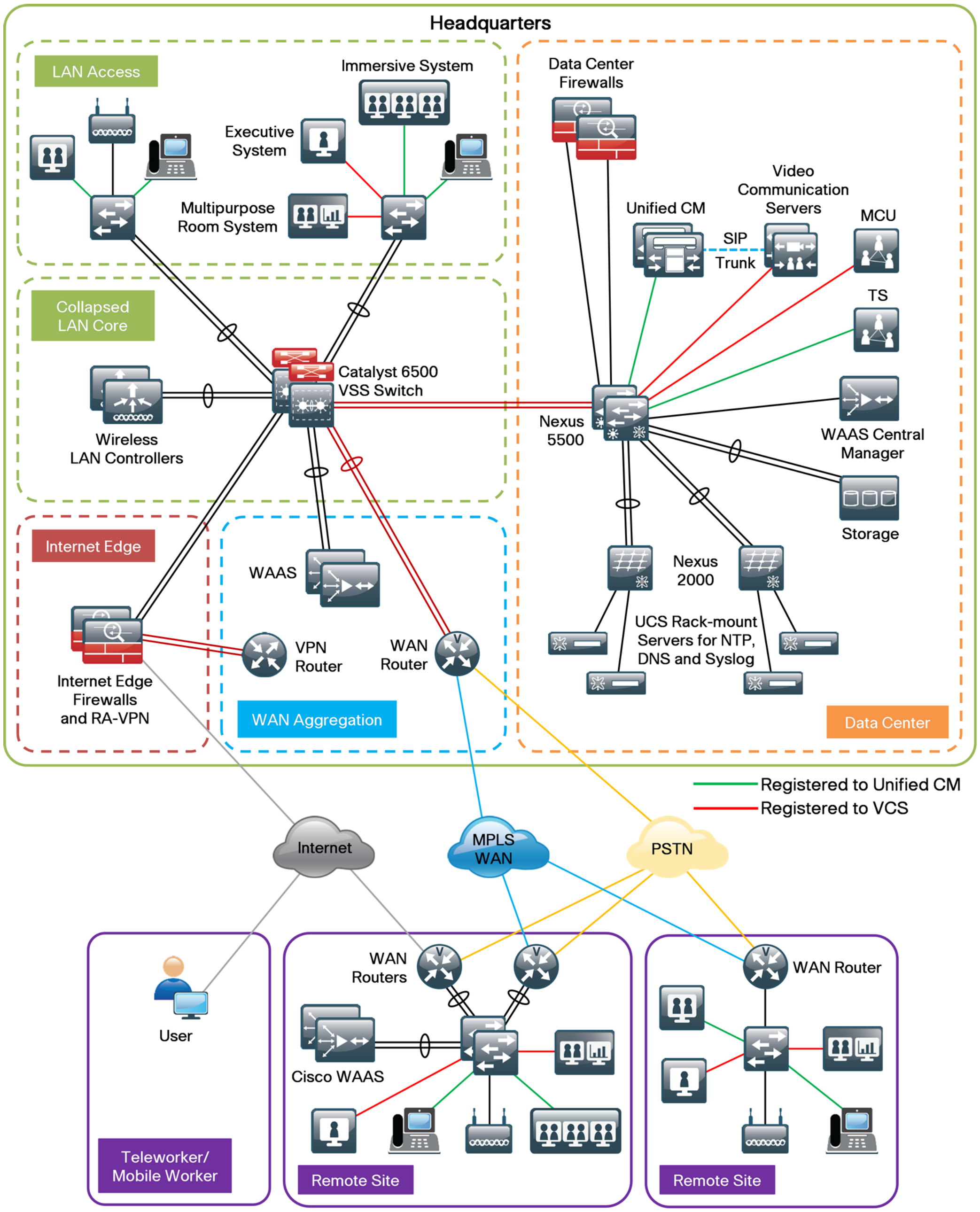
CTS endpoints register to Unified CM because it provides phone-like behavior for handling software updates and dynamic configuration settings. The user interaction on an immersive system comes from a simple telephone interface or touch screen because the intended audience is different than a multipurpose 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 Figure 1):

- 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 multipurpose systems
- Telepresence Server (TS) 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 integration



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.

QoS and Bandwidth Control

The solution 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 class 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 WAN is configured to allow 23 percent of the available 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.

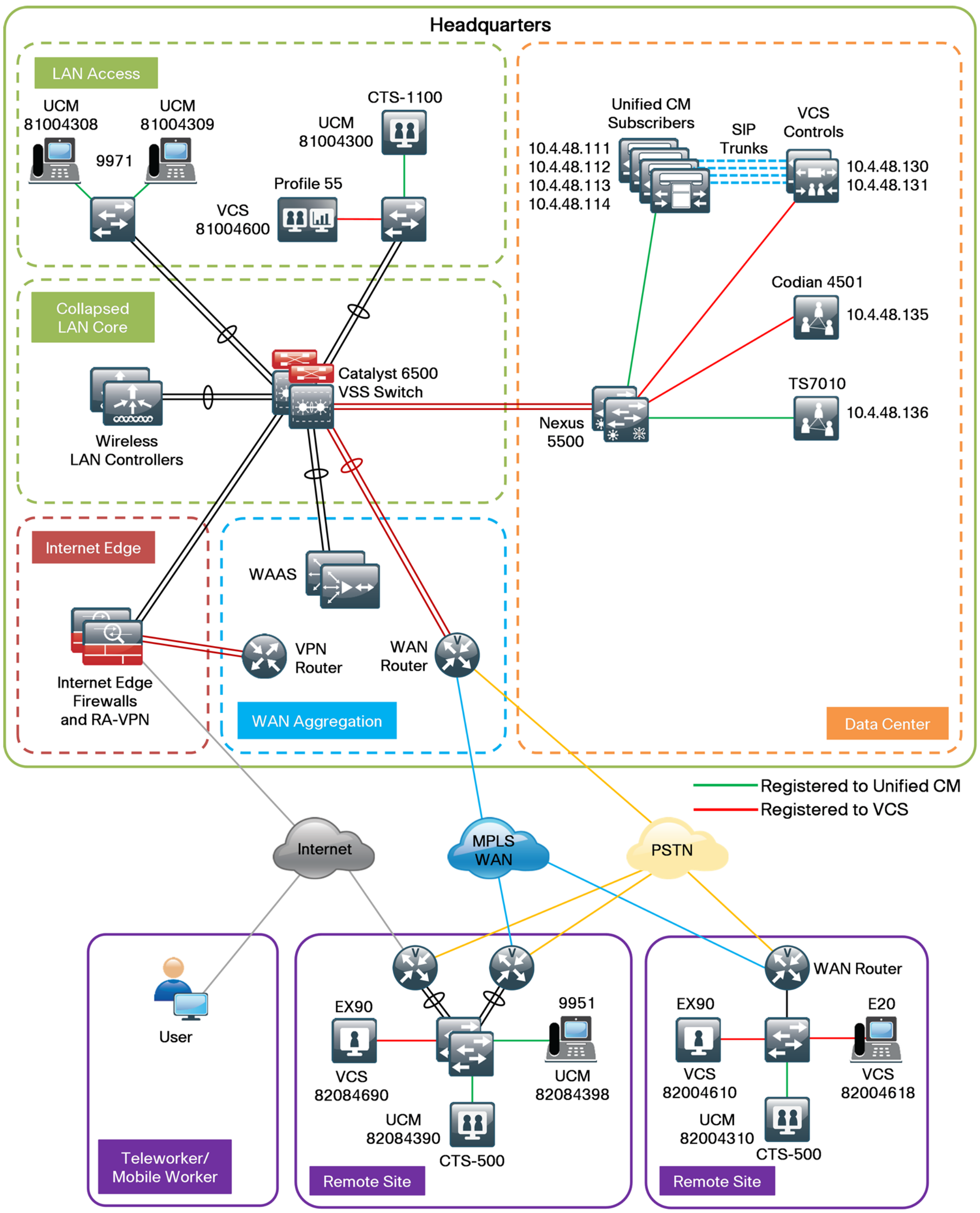
The call control agents and MCU are centralized in the data center. The access, WAN, and campus networks are medianet-enabled, using highly available designs and localized services, like medianet performance monitor. These services are configured in the remote sites whenever possible and as close to the endpoints as practical. The media 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.

Deployment Details

This design 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 SIP Video Using VCS Design Guide and the H.323 Video Interworking Using VCS Design 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.

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



PROCESS

Configuring Cisco Unified CM

1. Install TelePresence Room licenses
2. Configure CTS connectivity to the LAN
3. Configure CTS immersive endpoints
4. Configure CTS associated phones
5. Install the CTS software
6. Deploy the latest CTS software
7. Deploy the CTS phone application software
8. Configure video telephony endpoints
9. Configure Unified CM regions
10. Configure Unified CM locations
11. Unified CM to Unified CM calling
12. Configure Unified CM to VCS calling

The procedures for configuring a basic Unified CM cluster are documented in the Telephony using Cisco UCM Design 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. You must obtain licenses for the CTS endpoints prior to installing them on your cluster.

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

Procedure 1 Install TelePresence Room licenses

Prior to installing your first TelePresence endpoint on Unified CM, you need to add your licenses in the Enterprise Licensing Manager.

Step 1: Use your web browser to access the IP address or hostname of the publisher, and in the center of the page under Installed Applications, select **Cisco Enterprise License Manager**.

Step 2: On the login page, enter the publisher's application username and password, and then click **Login**:

- User Name—**CUCMAdmin** (case-sensitive)
- Password—**[password]**

Step 3: Navigate to **License Management > Licenses**, click **Other Fulfillment Options,** and then select **Fulfill Licenses from File**.

> **Tech Tip**
>
> Extract the .bin file from the .zip before installing the license in the next step. The installation process will return an error if you try to install the .zip file.

Step 4: On the Install License File popup page, click Browse to locate the directory that contains the TelePresence Room license files you obtained prior to installation. Select the .bin file, click **Open**, and then click **Install**. A message will indicate the license was successfully installed.

Step 5: Repeat Step 4 for each additional license file for your installation. After all files have been installed, click **Close**.

Step 6: To verify the licenses have been properly installed, navigate to **Monitoring > License Usage** and confirm the TelePresence Room has licenses installed and the status is In Compliance. If there is a problem, please notify your Cisco representative to obtain new license files.

License Usage

Type	Product Scope	Required	Installed	Unused	Status
Enhanced (9.0)	Unified CM	19	10000	9946	In Compliance
Basic (9.0)	Unified CM	2	0	0	In Compliance
Essential (9.0)	Unified CM	33	0	0	In Compliance
TelePresence Room (9.0)	Unified CM	0	100	100	In Compliance
Basic Messaging (9.0)	Unity Connection	33	10000	9967	In Compliance

After updating your licenses, you begin the process of installing the endpoints.

Procedure 2 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 Campus Wired LAN Design Guide.

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

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 3 Configure CTS immersive endpoints

CTS endpoints and their associated IP phones are configured in Unified CM. Depending on the version of code on each device, the codec and phone might need to be upgraded. 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 of the publisher by using the hostname or IP address.

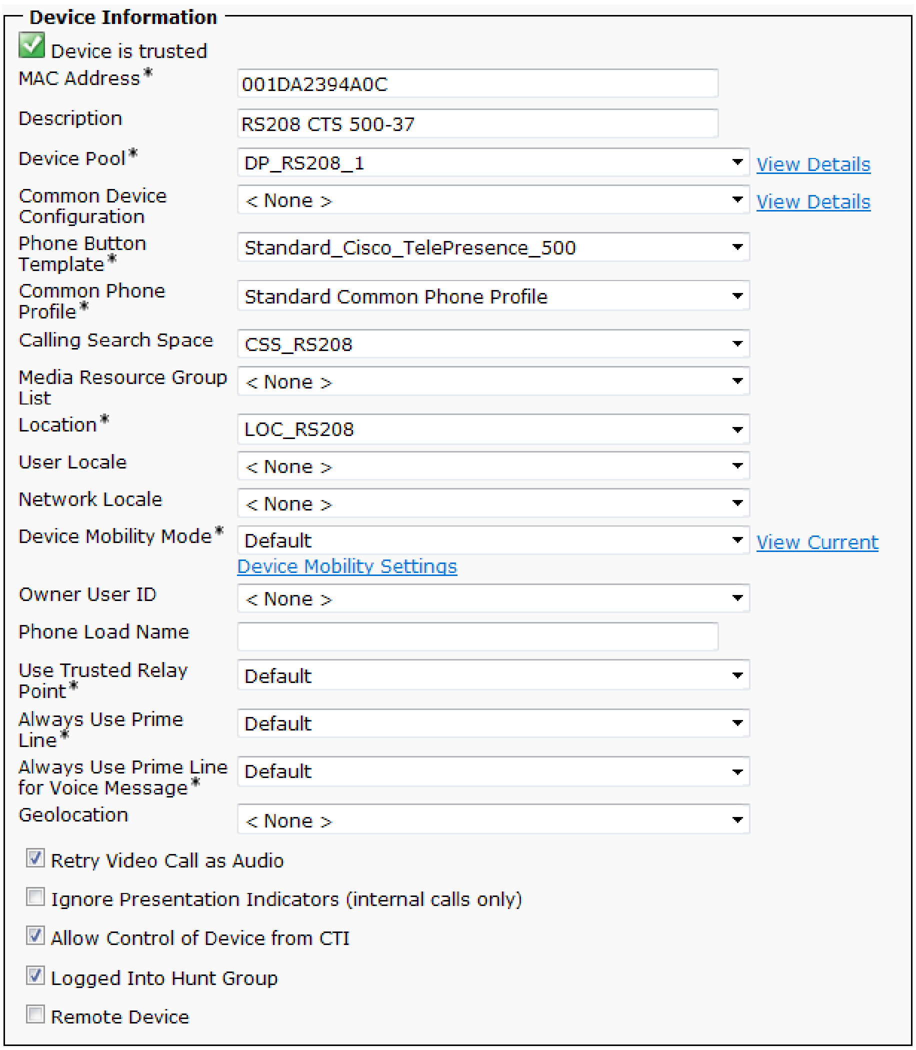
Step 3: In the center of the page under **Installed Applications**, click the **Cisco Unified Communications Manager** link.

> **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**.

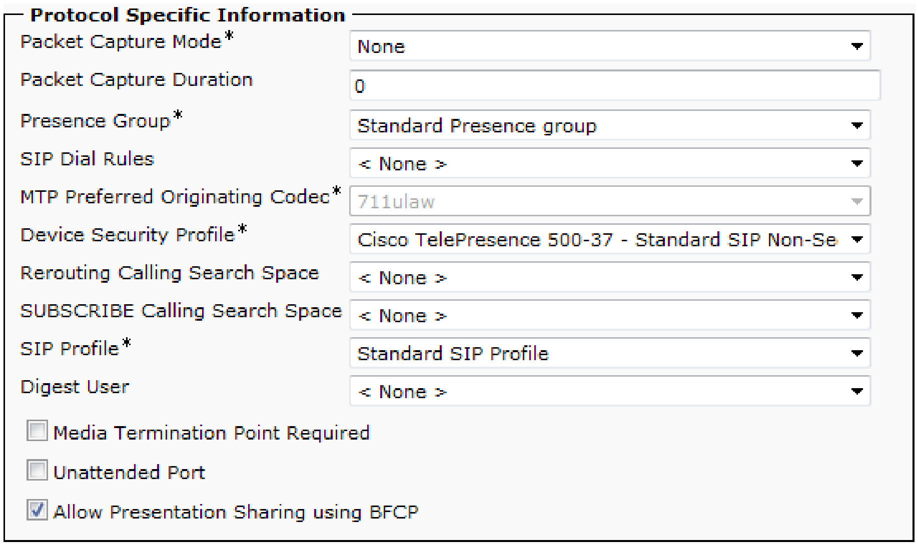
Step 5: Navigate to **Device > Phone**, click **Find**, look for the CTS MAC address in the Device Name column that you wrote down from Step 1, and then click on the name. On the Phone Configuration page under the Device Information section, enter the following values:

- 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
Device is trusted
MAC Address* 001DA2394A0C
Description RS208 CTS 500-37
Device Pool* DP_RS208_1 View Details
Common Device Configuration < None > View Details
Phone Button Template* Standard_Cisco_TelePresence_500
Common Phone Profile* Standard Common Phone Profile
Calling Search Space CSS_RS208
Media Resource Group List < None >
Location* LOC_RS208
User Locale < None >
Network Locale < None >
Device Mobility Mode* Default View Current Device Mobility Settings
Owner User ID < None >
Phone Load Name
Use Trusted Relay Point* Default
Always Use Prime Line* Default
Always Use Prime Line for Voice Message* Default
Geolocation < None >
Retry Video Call as Audio
Ignore Presentation Indicators (internal calls only)
Allow Control of Device from CTI
Logged Into Hunt Group
Remote Device

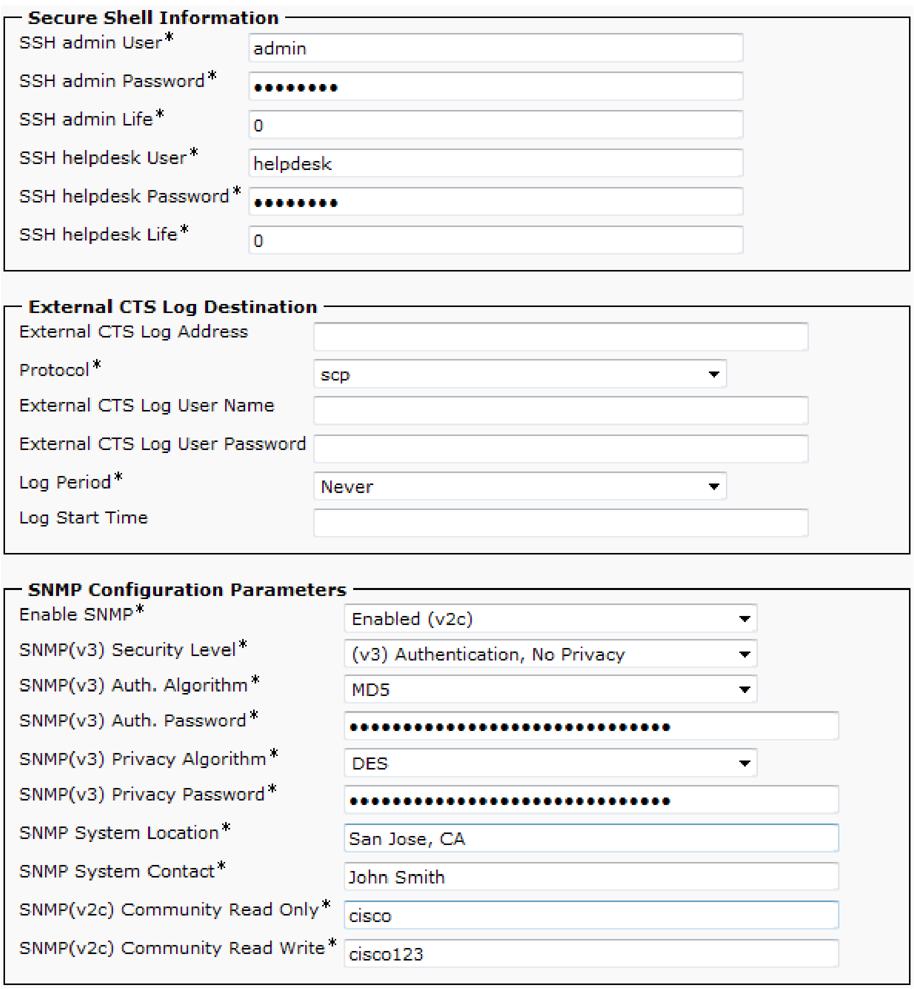
Step 6: Under the Protocol Specific Information section enter the following values.

- Device Security Profile—**Cisco TelePresence 500-37 - Standard SIP Non-Secure Profile**
- SIP Profile—**Standard SIP Profile**
- Allow Presentation Sharing using BFCP—**Select**



Step 7: Under the Secure Shell Information and SNMP Configuration Parameters sections enter the following values, and then click **Save.** On the message page, click **OK**.

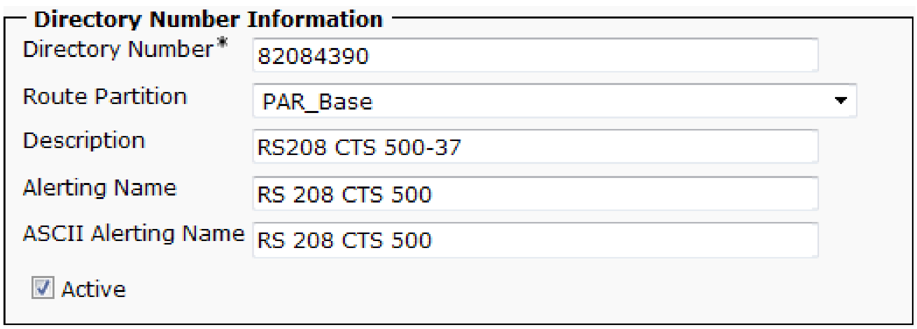
- SSH admin Password—**[password]**
- SSH admin Life—**0** (does not expire)
- SSH helpdesk Password—**[password]**
- SSH helpdesk Life—**0** (does not expire)
- Enable SNMP—**Enabled (v2c)**
- SNMP System Location—**San Jose, CA** (optional)
- SNMP System Contact—**John Smith** (optional)
- SNMP (v2c) Community Read Only—**cisco**
- SNMP (v2c) Community Read Write—**cisco123**



Step 8: On the Phone Configuration page, under Association Information, click **Line [1] - Add a new DN.**

Step 9: On the Directory Number Configuration page, enter the following values, and then click **Save:**

- Directory Number—**82084390** (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]**
- Active—**Select**



Procedure 4 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.

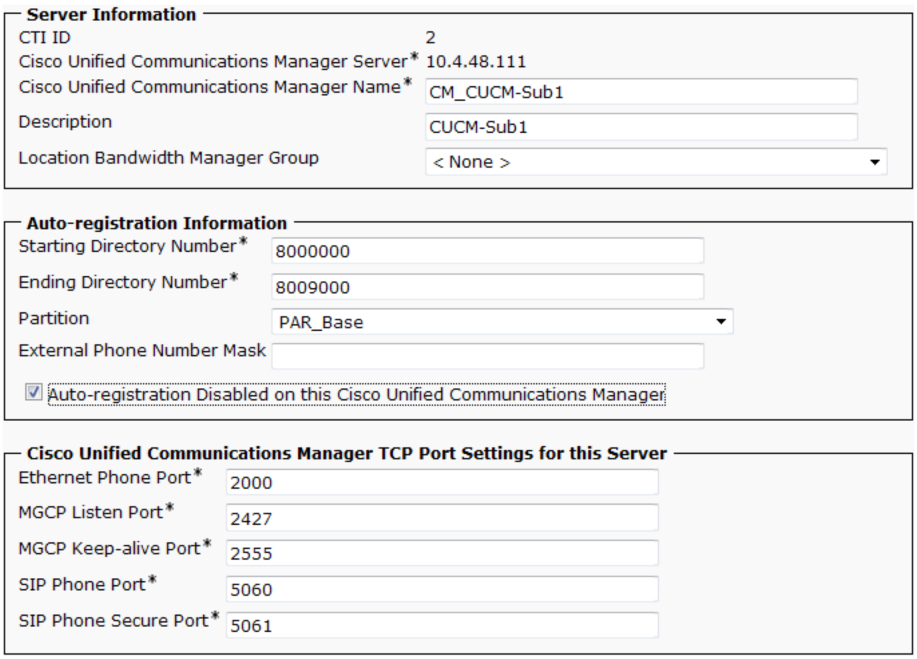
The easiest way to assign the directory number is to prepend 801 to the front of the four digit extension of the Cisco TelePresence System (CTS) endpoint. For example, if the CTS-500 has a four-digit extension of 4390, assign 8014390 as the directory number of the associated CP-7975 phone.

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.



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**.

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**.

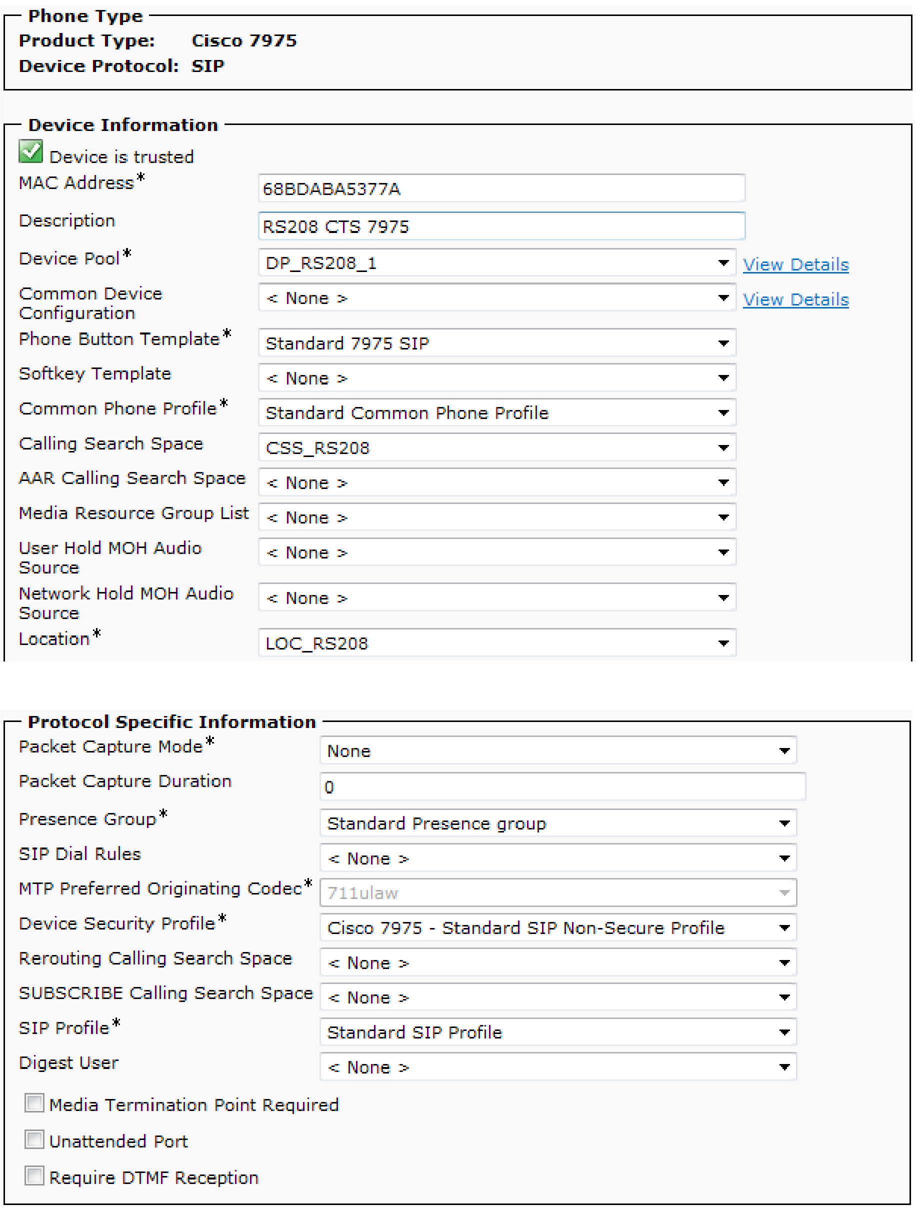
Step 6: On the Find and List Phones page, click **Add New.**

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 page, enter the following values, and then click **Save**. On the message page, click OK.

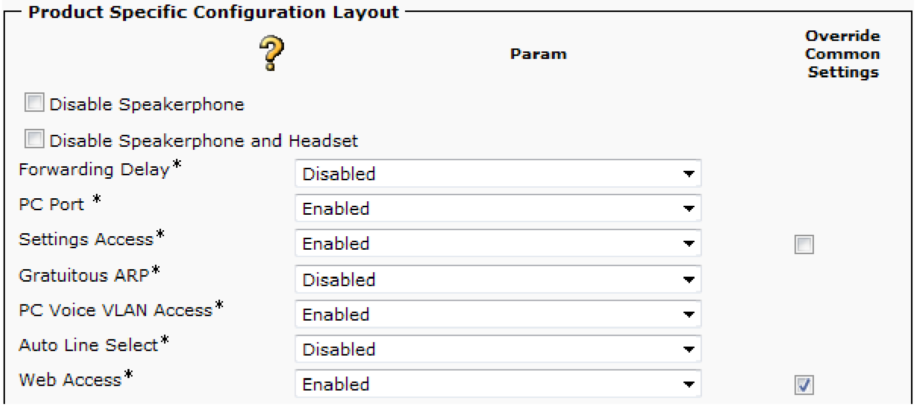
- MAC Address—**[MAC Address]**
- Description—**RS208 CTS 7975**
- Device Pool—**DP_RS208_1**
- Phone Button Template—**Standard 7975 SIP**
- Calling Search Space—**CSS_RS208**
- Location—**LOC_RS208**
- Device Security Profile—**Cisco 7975 - Standard SIP Non-Secure Profile**
- SIP Profile—**Standard 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

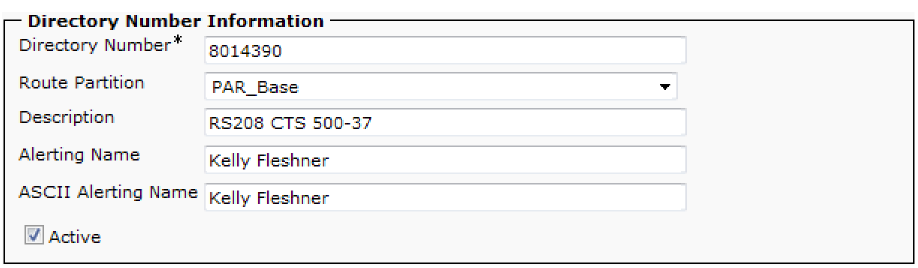


Step 9: After the Phone Configuration page reloads, click **Apply Config**. On the Apply Configuration page, click **OK**.

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

Step 11: On the Directory Number Configuration page, 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]**



Step 12: Repeat Procedure 2 through Procedure 4 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 5 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, login with your User ID, and then navigate to **Support > All Downloads**.

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

Step 3: Choose the latest release file, for example: **cmterm-CTS.1-9-2-19R-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. For example: **10.4.48.120**

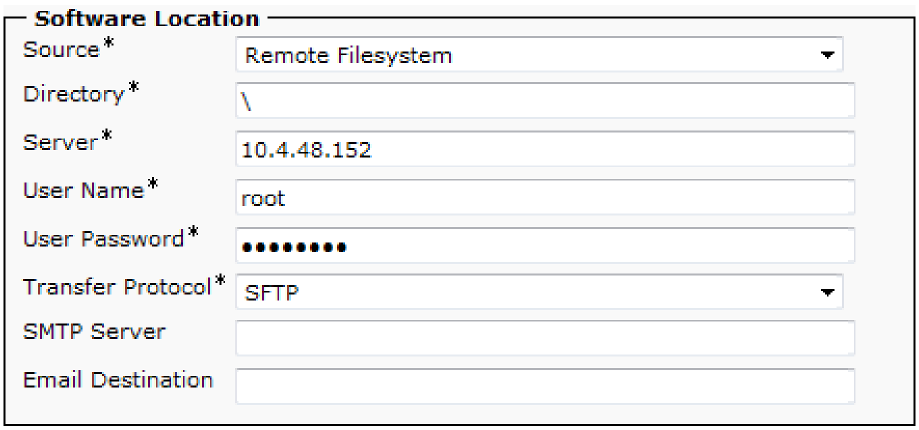
Step 6: In the center of the page under Installed Applications, click the **Cisco Unified Communications Manager** link.

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 case-sensitive **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**



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

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

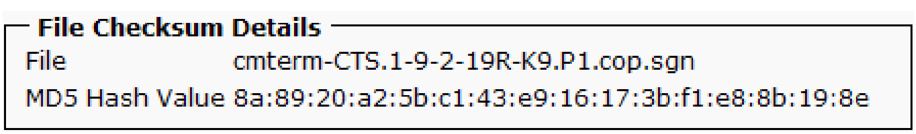
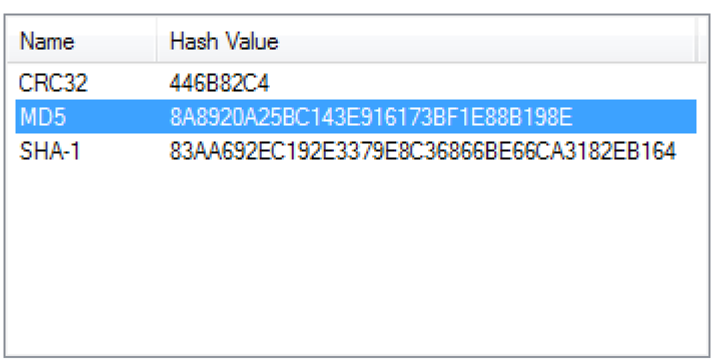


Figure 4 - MD5 Hash Value from PC running SFTP Server



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.1-9-2-19R-K9.P1.cop.sgn
Start Time	Wed Oct 31 14:03:54 PDT 2012
Status	Locale cmterm-CTS.1-9-2-19R-K9.P1.cop has been installed successfully.

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 **Cisco Tftp**, and then click **Restart**.

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

Procedure 6 Deploy the latest CTS software

Step 1: After the page refreshes on the final TFTP server, use your web browser to 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** for the application administrator, and then click **Login**.

Step 4: Navigate to **Device > Device Settings > Device Defaults**, enter the downloaded file name without the leading "cmterm-" and trailing ".cop" in the Load Information column for each CTS endpoint, and then click **Save**. For example: **CTS.1-9-2-19R-K9.P1**

Cisco TelePresence 1000	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 1100	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 1300-47	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 1300-65	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 1310-65	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 3000	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 3200	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 500-32	SIP	CTS.1-9-2-19R-K9.P1
Cisco TelePresence 500-37	SIP	CTS.1-9-2-19R-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.** On the Device Reset page, click **Reset,** and then click **Close**.

The CTS endpoint may take up to an hour to upgrade the software depending on the speed of your network.

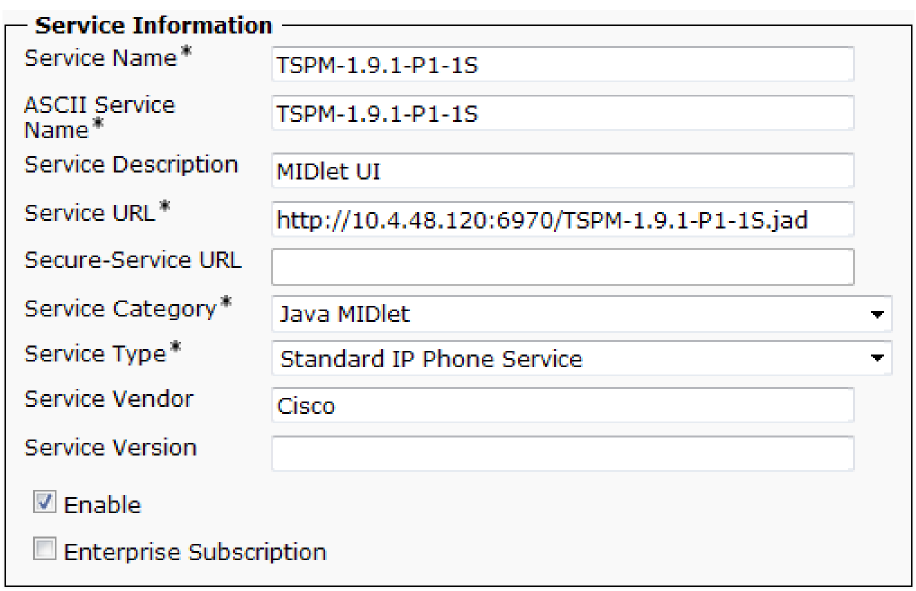
Step 7: Repeat Step 5 and Step 6 for each CTS endpoint.

Procedure 7 Deploy the CTS phone application software

Step 1: Navigate to **Device > Device Settings > Phone Services**, and then click **Add New**.

Step 2: On the **IP Phone Services Configuration** page, enter the following values, and then click **Save**:

- Service Name—**TSPM-1.9.1-P1-1S**
- ASCII Service Name—**TSPM-1.9.1-P1-1S**
- Service Description—**MIDlet UI**
- Service URL—**http://10.4.48.120:6970/TSPM-1.9.1-P1-1S.jad** (IP address of TFTP server)
- Service Category—**Java MIDlet**
- Service Type—**Standard IP Phone Service**
- Service Vendor—**Cisco**
- Enable—**Select**

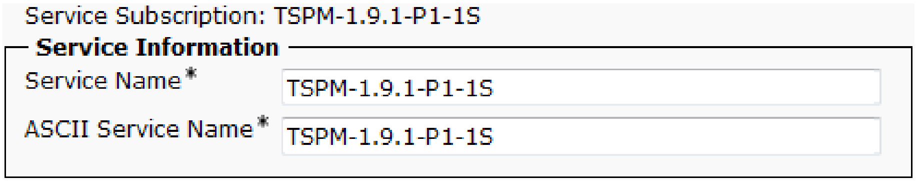


Step 3: Navigate to **Device > Phone,** click **Find**, and then click the MAC address of a phone associated with a CTS endpoint.

Step 4: In the Related Links list, choose **Subscribe/Unsubscribe Services**, and then click **Go**.

Step 5: In the Select a Service list, choose the service you configured in Step 2, and then click **Next**.

Step 6: On the next page, click **Subscribe**.



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

Step 7: Repeat Step 3 through Step 6 for each phone associated with a CTS endpoint.

Procedure 8 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.

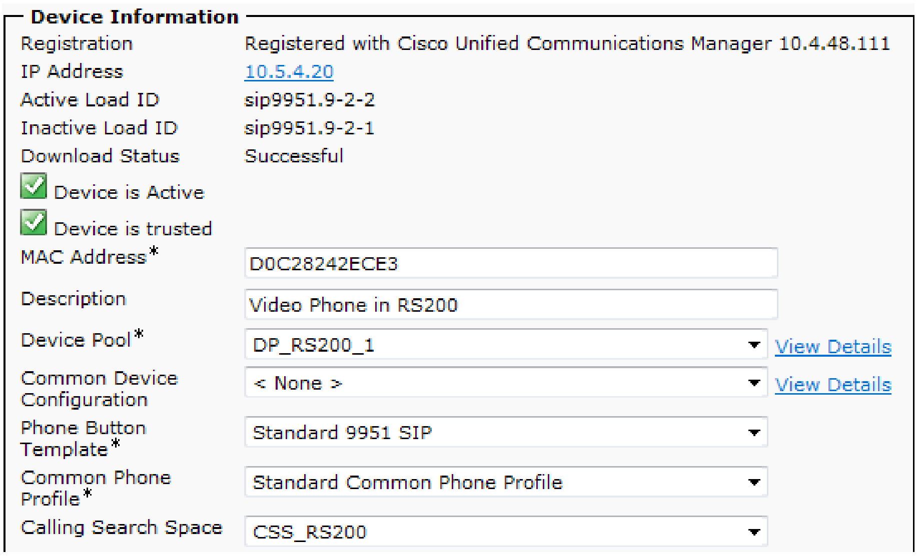
The following steps are required to assign the correct device pool, calling search space and to prepare the phone for sending and receiving video calls.

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.

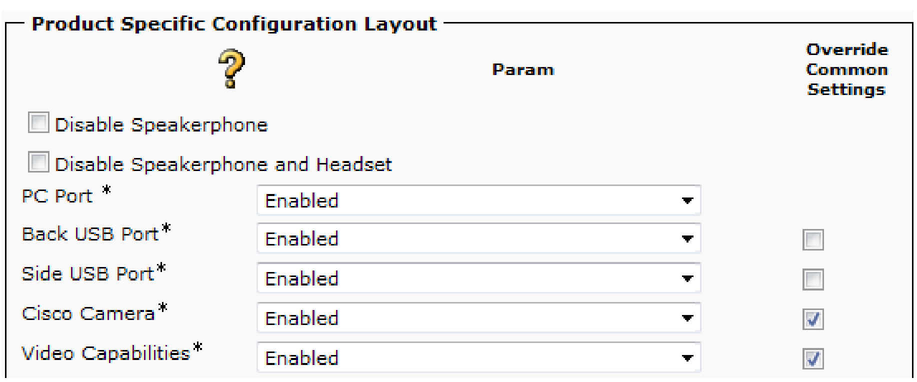
Step 3: On the **Phone Configuration** page under the Device Information section, enter the following values.

- Description—**Video Phone in RS200**
- Device Pool—**DP_RS200_1**
- Calling Search Space—**CSS_RS200**



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

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



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

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

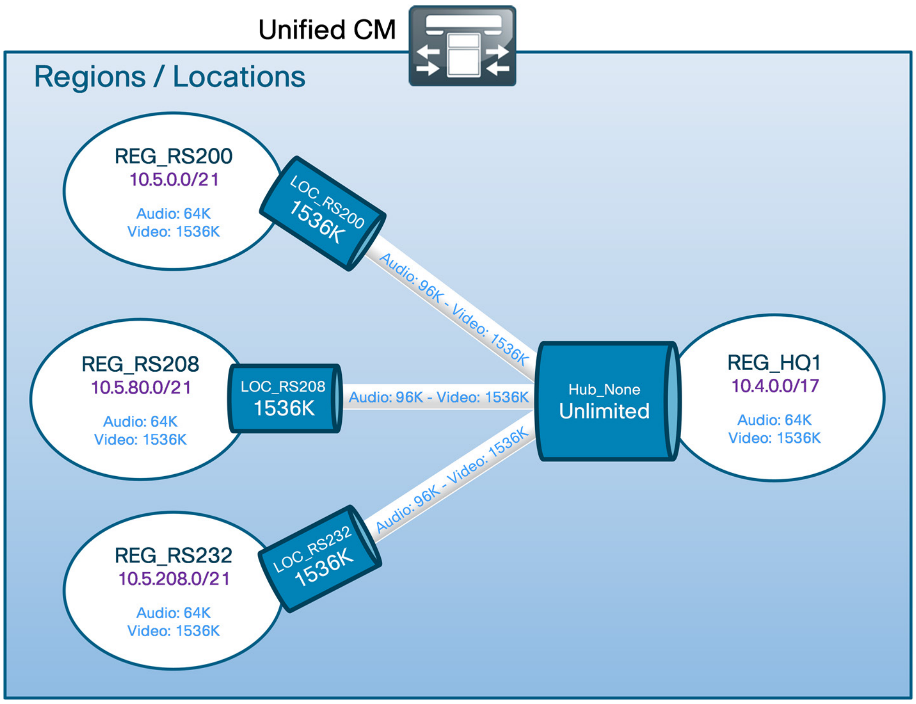
Step 6: On the Directory Number Configuration page, enter the following values, and then click **Save:**

- Directory Number—**82004019** (Access code, site code and extension)
- Route Partition—**PAR_Base**

Step 7: Repeat this procedure for each video phone.

Procedure 9 Configure Unified CM regions

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 installation 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 maximum 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.

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

Step 2: Under Modify Relationship to other Regions on the bottom of the page, select each region that has CTS video endpoints, change the following values in their respective columns, and then click **Save**:

- Maximum Audio Bit Rate (pull down)—**64 kbps (G.722, G.711)**
- Maximum Session Bit Rate for Video Calls kbps (radio button)—**Select**
- Maximum Session Bit Rate for Video Calls—**1536**

Step 3: After all of the region relationships are modified, click **Reset.**

Reset Information

Selected Device: 256 devices selected

If a device is not registered with Cisco Unified Communications Manager, you cannot restart it. If a device is registered, to restart a device without shutting it down, click the **Restart** button. To return to the previous window without 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 4: On the Device Reset page, click **Restart**, and then click **Close**.

Region Information

Name* REG_RS208

Region Relationships

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls
REG_HQ1	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	1536
REG_RS200	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	1536
REG_RS208	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	1536
REG_RS232	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	1536
NOTE: Regions not displayed	Use System Default	Use System Default	Use System Default

Step 5: Repeat Procedure 9 for each region with CTS endpoints.

Procedure 10 Configure Unified CM locations

The Location Video Bandwidth and Immersive Bandwidth are set to the same value of 1536 kbps because by default they are not tracked separately.

If you want to track immersive and non-immersive calls individually, you will need to change the **System > Service Parameter > Publisher IP > Cisco CallManager** parameter called "Use Video BandwidthPool for Immersive Video Calls" to False. For this guide, you will leave the parameter set to the default setting of **True**.

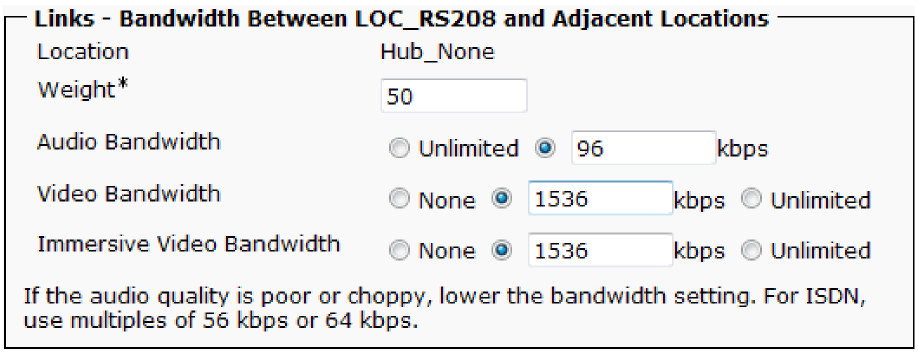
The Location configuration audio bandwidth is set to at least 96 kbps because video calls from multipurpose endpoints to CTS endpoints are initially audio-only calls and they will be rejected if the bandwidth is less than 96 kbps.

You will also set the intra-location video bandwidth and immersive bandwidth for devices within the location to 1536 kbps.

Step 1: Navigate to **System > Location Info > Location**, click **Find**, and then click the name of a remote-site location with CTS endpoints. For example: **LOC_RS208**

Step 2: From the Location Information page, click on the **Hub_None** location, enter the following values, and then click **Save**:

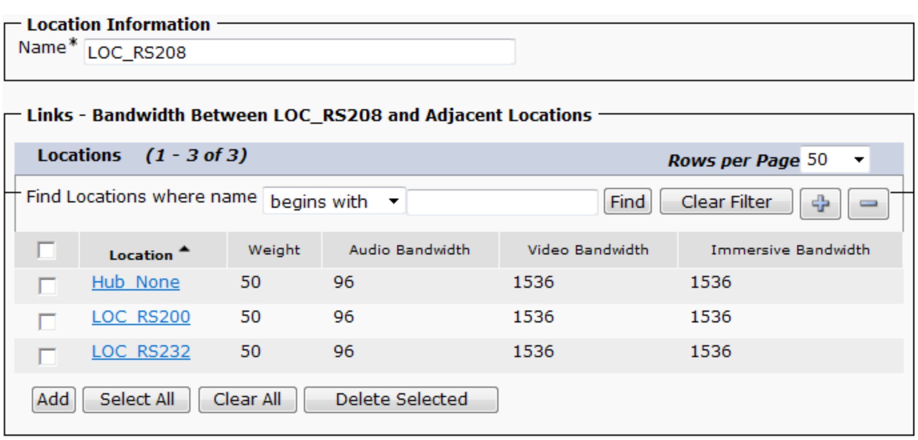
- Audio Bandwidth radio button—**Select**
- Audio Bandwidth in kbps—**96** (must be at least 96)
- Video Bandwidth radio button—**Select**
- Video Bandwidth in kbps—**1536** (set both video bandwidths to the same value)
- Immersive Video Bandwidth radio button—**Select**
- Immersive Video Bandwidth in kbps—**1536** (set both video bandwidths to the same value)



Step 3: For each additional remote-site location with CTS or video telephony endpoints, click **Add**, enter the following values, and then click **Save**:

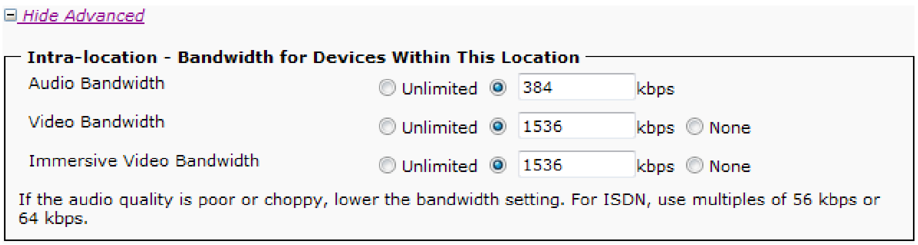
- Audio Bandwidth radio button—**Select**
- Audio Bandwidth in kbps—**96** (must be at least 96)
- Video Bandwidth radio button—**Select**
- Video Bandwidth in kbps—**1536** (set both video bandwidths to the same value)
- Immersive Video Bandwidth radio button—**Select**
- Immersive Video Bandwidth in kbps—**1536** (set both video bandwidths to the same value)

Step 4: After all the locations with CTS or video telephony endpoints have been added, click **Close**.



Step 5: Click **Show Advanced** above the Location RSVP Setting section, enter the following values, and then click **Save**:

- Audio Bandwidth radio button—**Select**
- Audio Bandwidth in kbps—**384** (must be at least 96)
- Video Bandwidth radio button—**Select**
- Video Bandwidth in kbps—**1536** (set both video bandwidths to the same value)
- Immersive Video Bandwidth radio button—**Select**
- Immersive Video Bandwidth in kbps—**1536** (set both video bandwidths to the same value)



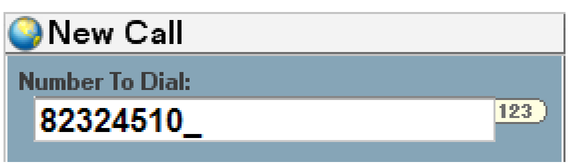
Step 6: Repeat Procedure 10 for each remote-site location with CTS or video telephony endpoints.

Procedure 11 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: From the TelePresence phone service interface on the associated phone, tap **New Call**.

Enter the eight digit extension of another CTS endpoint at a different location, for example: **82324510** and then tap **Dial**.



To view the status of the call in progress, follow the steps below.

Step 2: From your web browser, access the CTS endpoints administrative interface, for example: **https://10.4.84.50/** and log in using the SSH admin username and password you configured in Step 7 under Procedure 3 of this process.

Step 3: On the Cisco TelePresence Systems Administration page, 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 9 match the available bandwidth for the link.

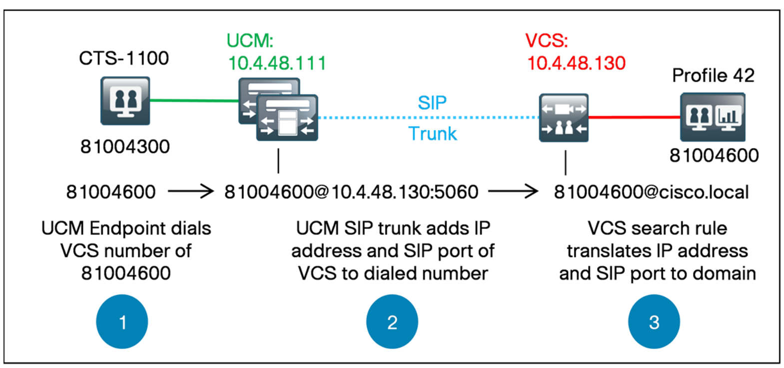
Real Time Call Statistics	
Call Connected	Yes
Registered to Cisco Unified Communications Manager	Yes
Local Number	82084390
Audio/Video Call	
Call Start Time	Thu Nov 1 14:52:24 2012
Call Duration	78 seconds
Call Type	Incoming
Remote Number	82324510
Call State	Answered
Security Level	Non-Secure
Actual Bit Rate	972000 bps, 1280x720
Negotiated Bit Rate	972000 bps
Historical Call Statistics (Not including current call, if any)	
Call Statistics Clear Time	Wed Oct 31 14:37:27 2012
Last Call Start Time	Thu Nov 1 14:51:31 2012
Last Call Duration	27 seconds
Number of Calls Since System Setup	26
Time in Calls Since System Setup (seconds)	1776
Number of Calls Since Last Reboot	6
Time in Calls Since Last Reboot (seconds)	890
Registered to Cisco Unified Communications Manager	Yes
Configured Bit Rate	Not Available

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

Procedure 12 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.

Figure 5 - Unified CM to VCS call flow



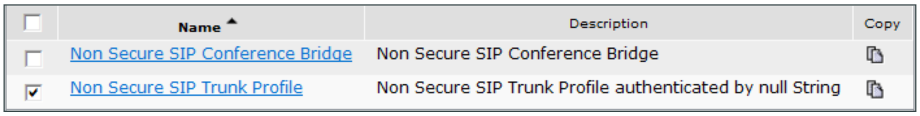
A SIP trunk, route group, route list and route pattern send the calls to the IP address of the VCS. Before adding the SIP trunk, you will also create a non-secure SIP trunk security profile for VCS. After you finalize the Unified CM dial plan, you perform additional steps in the subsequent process to 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 **System > Security > SIP Trunk Security Profile**, click **Find**, and then select the checkbox next to the **Non Secure SIP Trunk Profile**.

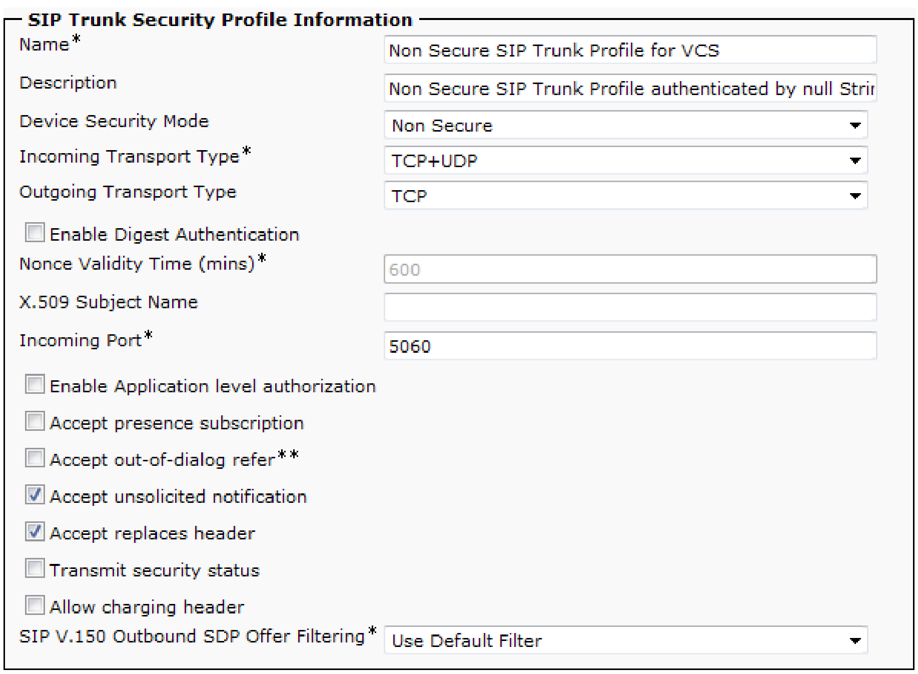


☐	Name ▲	Description	Copy
☐	Non Secure SIP Conference Bridge	Non Secure SIP Conference Bridge	
☑	Non Secure SIP Trunk Profile	Non Secure SIP Trunk Profile authenticated by null String	

Step 5: Click **Copy** to create a new security profile from the default Non Secure Trunk Profile.

Step 6: From the SIP Trunk Security Profile Configuration page, enter the following values, and then click **Save**:

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



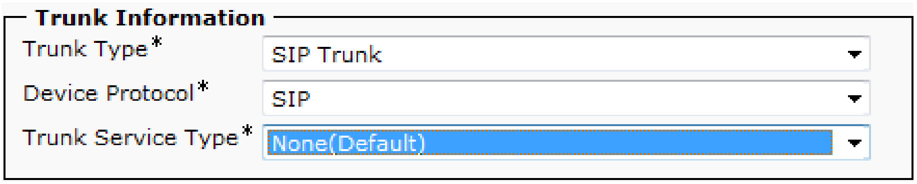
SIP Trunk Security Profile Information

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

Step 7: Navigate to **Device > Trunk**, and then click **Add New**.

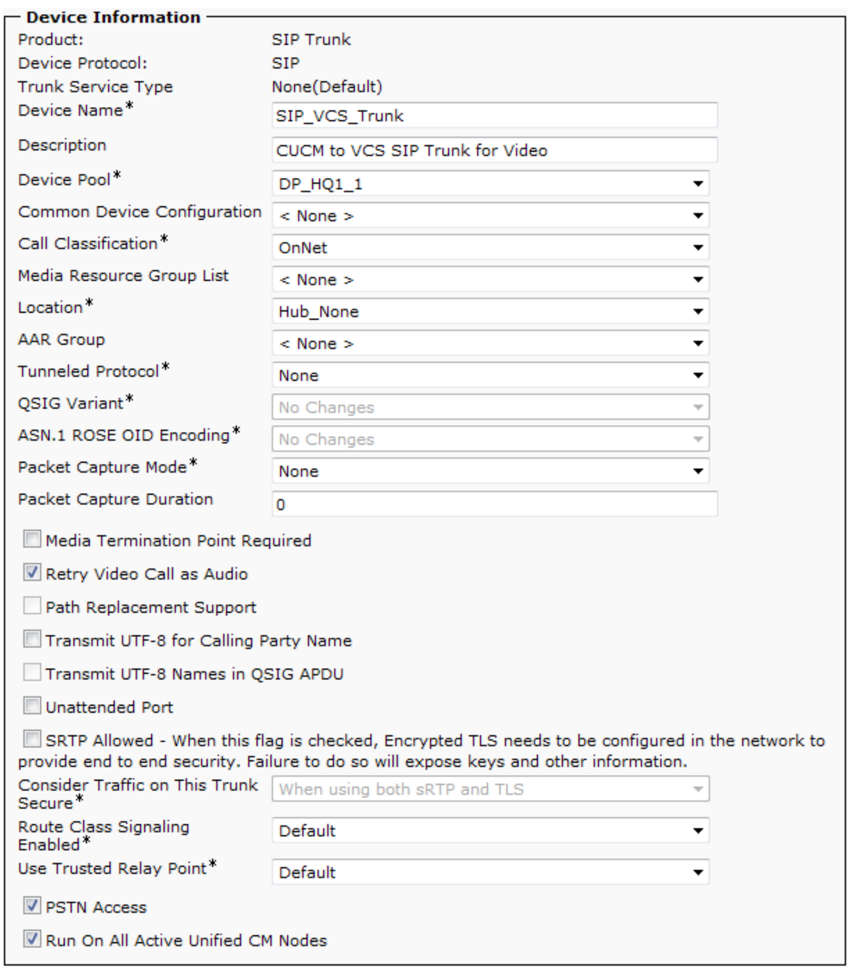
Step 8: On the Trunk Configuration page, enter the following values, and then click **Next**:

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



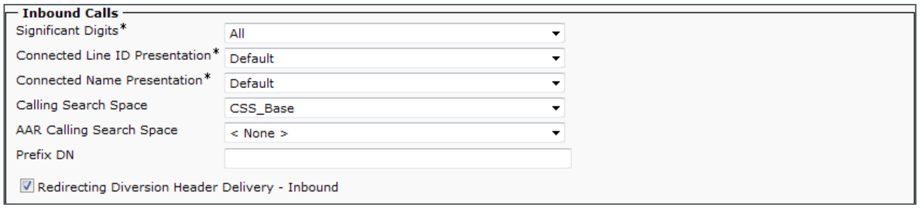
Step 9: On the next page in the Device Information section, enter the following values.

- 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—**Select**
- Run On All Active Unified CM Nodes—**Select**



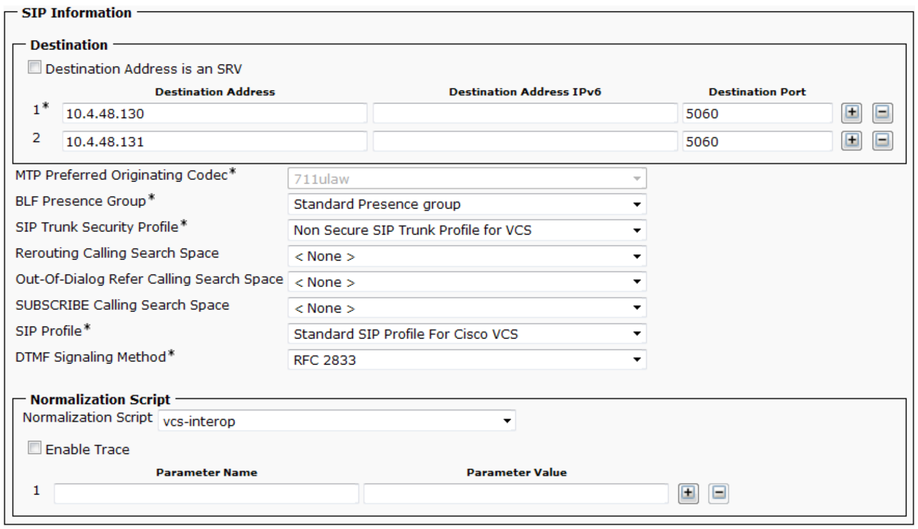
Step 10: In the Inbound Calls section, enter the following values.

- Significant Digits—**All**
- Calling Search Space—**CSS_Base**
- Redirecting Diversion Header Delivery Inbound—**Select**



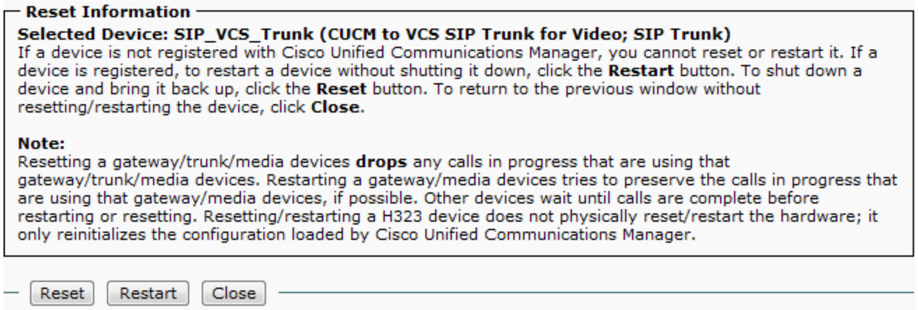
Step 11: In the SIP Information section, enter the following values, and then click Save. On the message page, click OK.

- 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 Cisco VCS**
- DTMF Signaling Method—**RFC 2833**
- Normalization Script—**vcs-interop**



Step 12: On the Trunk Configuration page, click Reset.

Step 13: From the Device Reset page, click **Reset**, and then click **Close**.

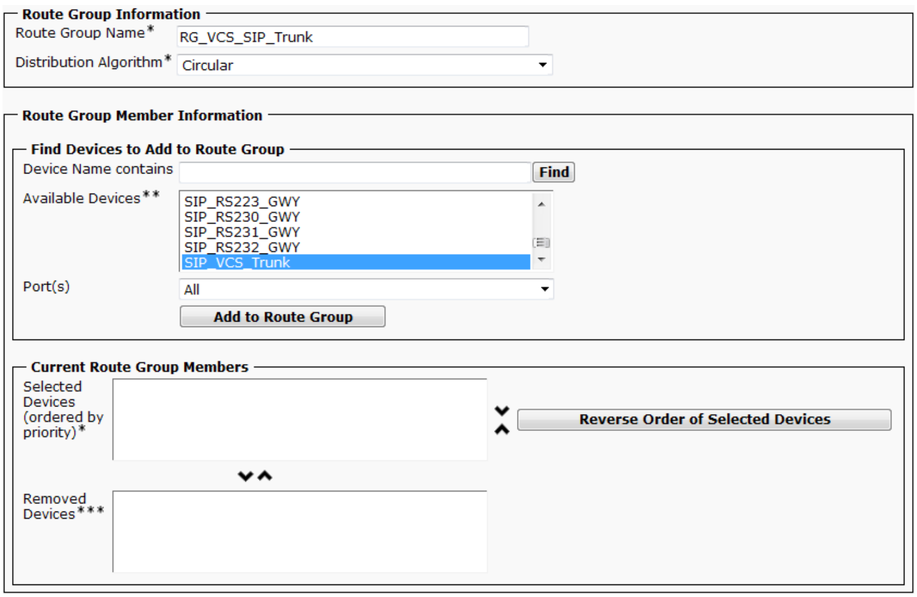


Step 14: Navigate to **Call Routing > Route / Hunt > Route Group**, and then click **Add New.**

Step 15: On the Route Group Configuration page, enter the Route Group Name **RG_VCS_SIP_Trunk**.

Step 16: From the Available Devices, enter the following values, click **Add to Route Group**, and then click **Save**:

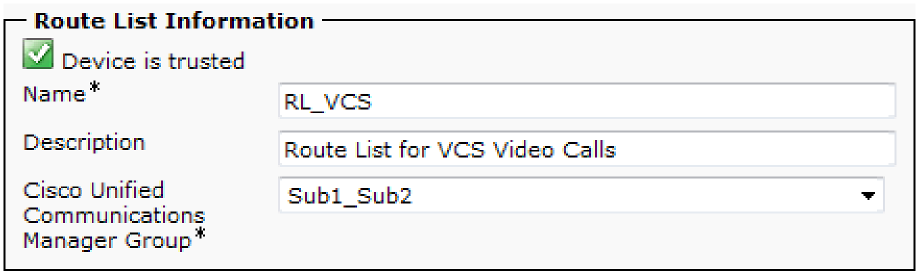
- Available Devices—**SIP_VCS_Trunk**
- Port(s)—**All**



Step 17: Navigate to **Call Routing > Route / Hunt > Route List**, and then click **Add New.**

Step 18: On the Route List Configuration page, enter the following values, and then click **Save**:

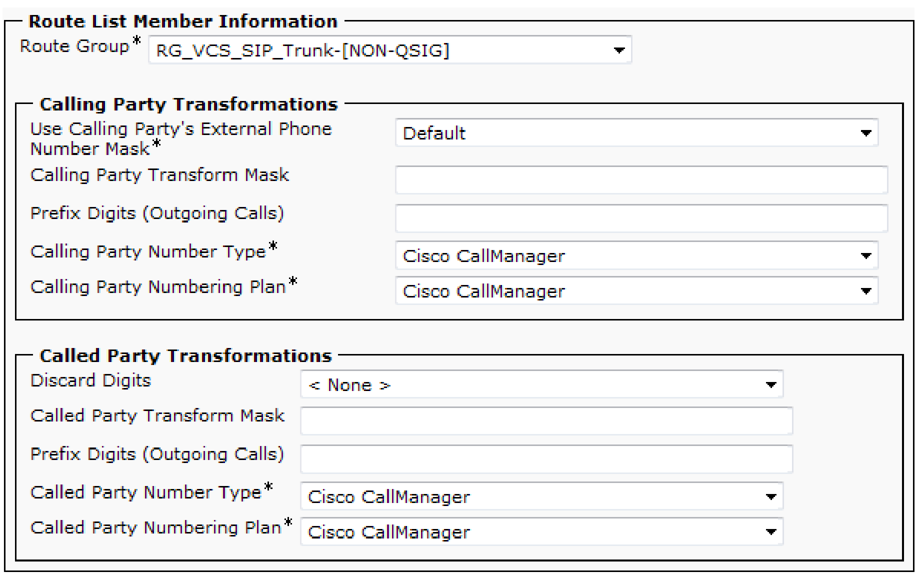
- Name—**RL_VCS**
- Description—**Route List for VCS Video Calls**
- Cisco Unified Communications Manager Group—**Sub1_Sub2**



Step 19: In the Route List Member Information section, click **Add Route Group**.

Step 20: On the Route List Detail Configuration page, enter the following value, and then click **Save**. On the message page, click **OK**.

- Route Group—**RG_VCS_SIP_Trunk [NON-QSIG]**

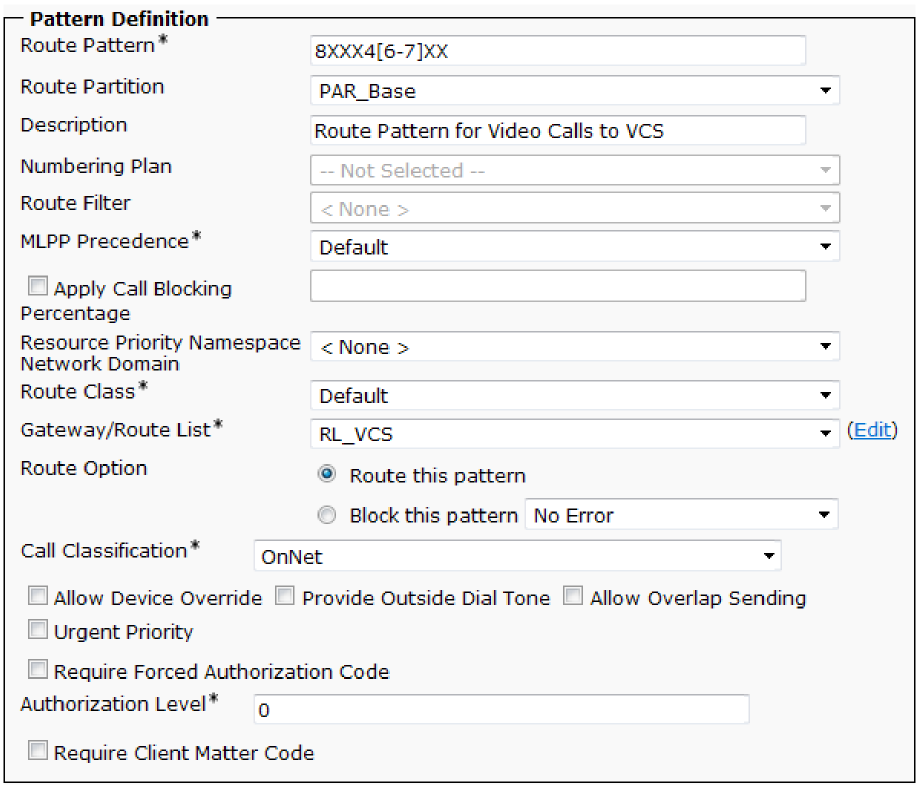


Step 21: Click **Reset**. On the Device Reset page, click **Reset**, and then click **Close**.

Step 22: Navigate to **Call Routing > Route/Hunt > Route Pattern**, and then click **Add New.**

Step 23: On the Route Pattern Configuration page, enter the following values, and then click **Save**. On the two message pages, click **OK**.

- 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**
- Provide Outside Dial Tone—**Clear** (Unchecked)



PROCESS

Configuring Cisco TelePresence VCS

1. Configure VCS inbound calls
2. Configure VCS outbound calls
3. Configure VCS pipes
4. Configure VCS links
5. VCS to Unified CM dialing
6. 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.

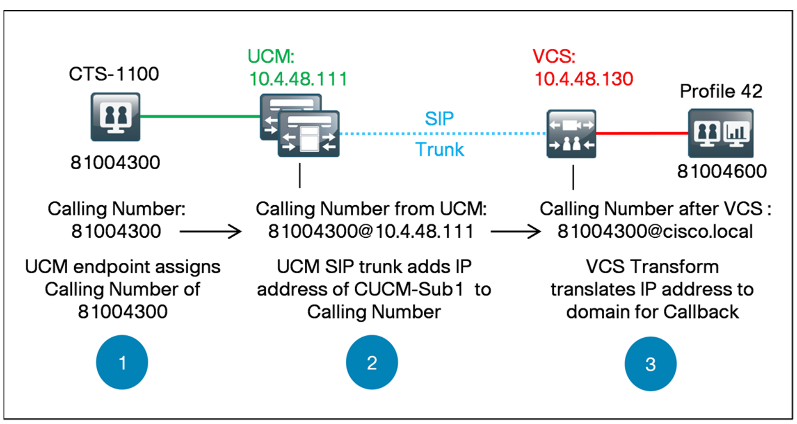
Procedure 1 Configure VCS inbound calls

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 81004600 arrives as 81004600@10.4.48.130:5060. The VCS translates the called number to 81004600@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.

Figure 6 - Unified CM to VCS calling name translation



For example, a Unified CM endpoint call from 81004300 arrives as 81004300@10.4.48.111. The VCS translates the calling number to 81004300@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**.

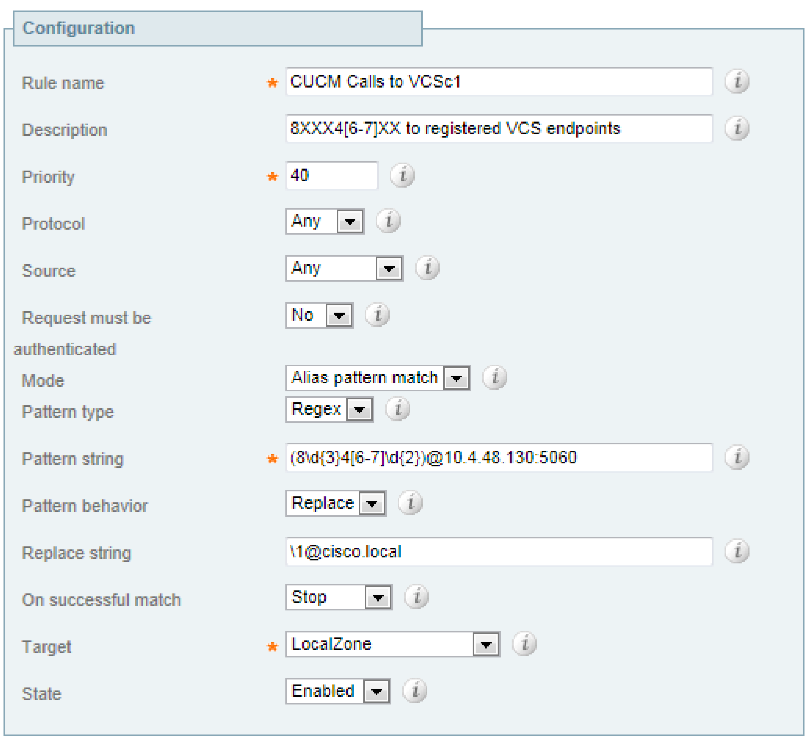
Step 2: Enter the following values and click **Login**:

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

Step 3: Navigate to **VCS configuration > Dial plan > 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**
- Protocol—**Any**
- 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 plan > 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**

<table>
<tr><th colspan="2">Configuration</th></tr>
<tr><td>Priority</td><td>* 3</td></tr>
<tr><td>Description</td><td>CUCM_Sub1 IP Address to Domain Name</td></tr>
<tr><td>Pattern type</td><td>Regex</td></tr>
<tr><td>Pattern string</td><td>* (.*)@10.4.48.111((:|;).*)?</td></tr>
<tr><td>Pattern behavior</td><td>Replace</td></tr>
<tr><td>Replace string</td><td>\1@cisco.local\2</td></tr>
<tr><td>State</td><td>Enabled</td></tr>
</table>

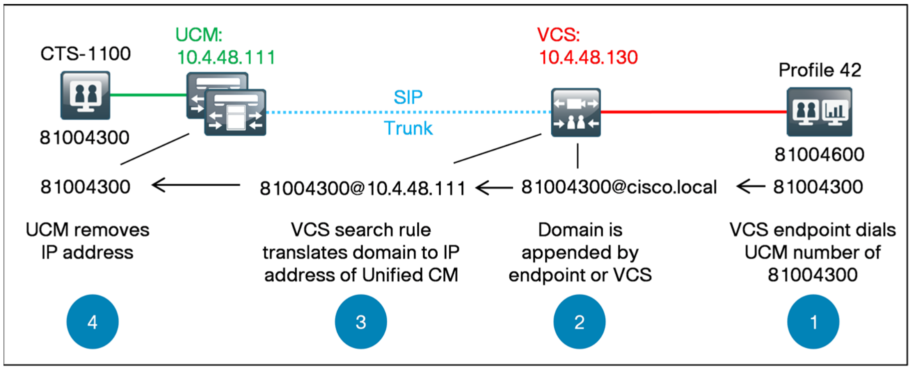
Step 8: Repeat Step 6 and Step 7 for every subscriber IP address in your Unified CM cluster. Change the Description, Pattern string's IP address and increase the Priority by 1 each time.

<table>
<tr><td>3</td><td>✔ Enabled</td><td>CUCM_Sub1 IP Address to Domain Name</td><td>(.*)@10.4.48.111((:|;).*)?</td><td>Regex</td><td>Replace</td><td>\1@cisco.local\2</td></tr>
<tr><td>4</td><td>✔ Enabled</td><td>CUCM_Sub2 IP Address to Domain Name</td><td>(.*)@10.4.48.112((:|;).*)?</td><td>Regex</td><td>Replace</td><td>\1@cisco.local\2</td></tr>
<tr><td>5</td><td>✔ Enabled</td><td>CUCM_Sub3 IP Address to Domain Name</td><td>(.*)@10.4.48.113((:|;).*)?</td><td>Regex</td><td>Replace</td><td>\1@cisco.local\2</td></tr>
<tr><td>6</td><td>✔ Enabled</td><td>CUCM_Sub4 IP Address to Domain Name</td><td>(.*)@10.4.48.114((:|;).*)?</td><td>Regex</td><td>Replace</td><td>\1@cisco.local\2</td></tr>
</table>

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.

Figure 7 - VCS to Unified CM call flow



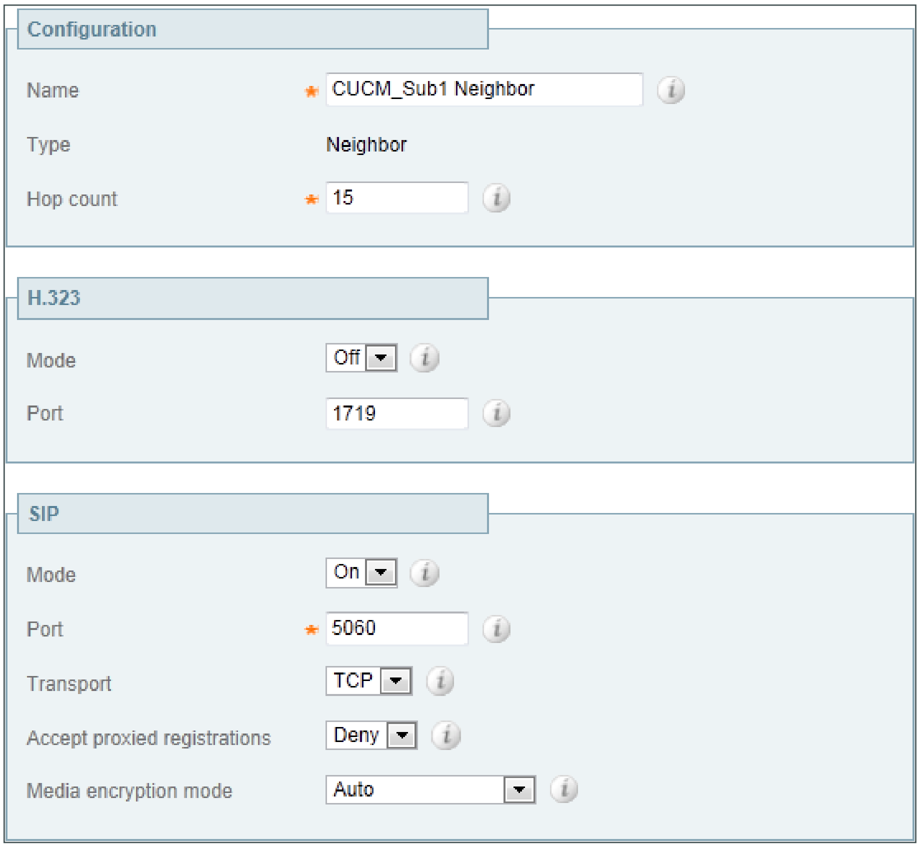
You configure a different neighbor zone for each subscriber to provide signaling redundancy. You create search rules with the same priority to send calls to the neighbor zones defined for the Unified CM cluster. The local domain name is replaced with the IP address of the specified Unified CM subscriber.

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 > Zones**, and then click **New**.

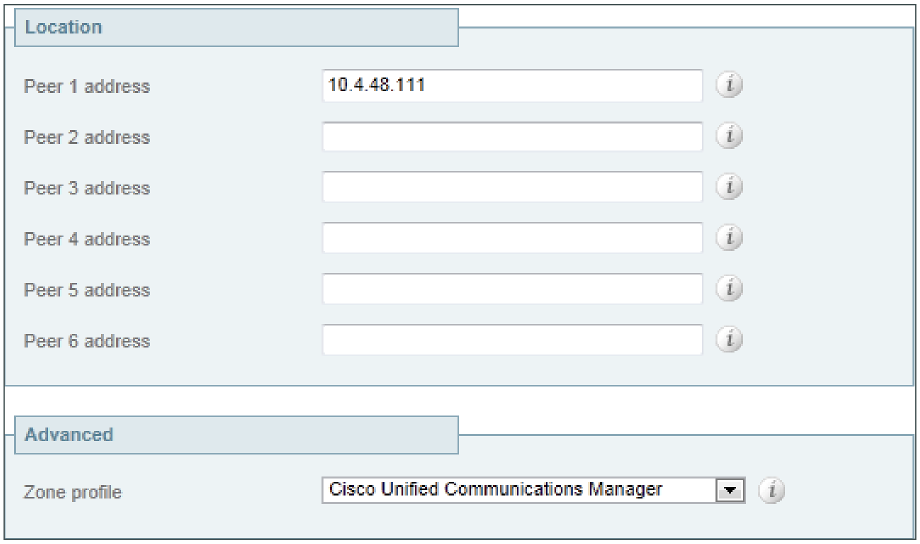
Step 2: On the Create Zone page, under the Configuration, H.323 and SIP sections enter the following values.

- Name—**CUCM_Sub1 Neighbor**
- Type—**Neighbor**
- H.323 Mode—**Off**
- SIP Mode—**On**
- SIP Port—**5060**
- SIP Transport—**TCP**
- Accept proxied registrations—**Deny**
- Media encryption mode—**Auto**



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**



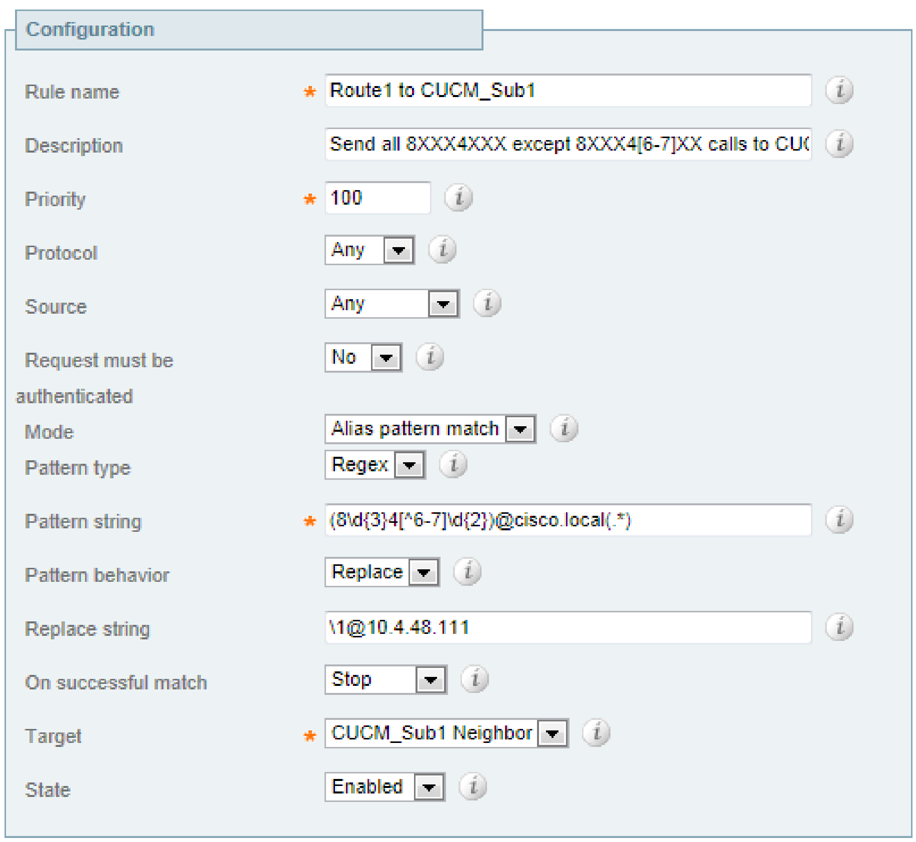
Step 4: Repeat Step 1 through Step 3 for each subscriber in the Unified CM cluster. Change the Name and Peer 1 Address for each zone.

DefaultZone	Default Zone	0	0 kbps	On	On	
CUCM_Sub1 Neighbor	Neighbor	0	0 kbps	Off	Active	No search rules configured
CUCM_Sub2 Neighbor	Neighbor	0	0 kbps	Off	Active	No search rules configured
CUCM_Sub3 Neighbor	Neighbor	0	0 kbps	Off	Active	No search rules configured
CUCM_Sub4 Neighbor	Neighbor	0	0 kbps	Off	Active	No search rules configured

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

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

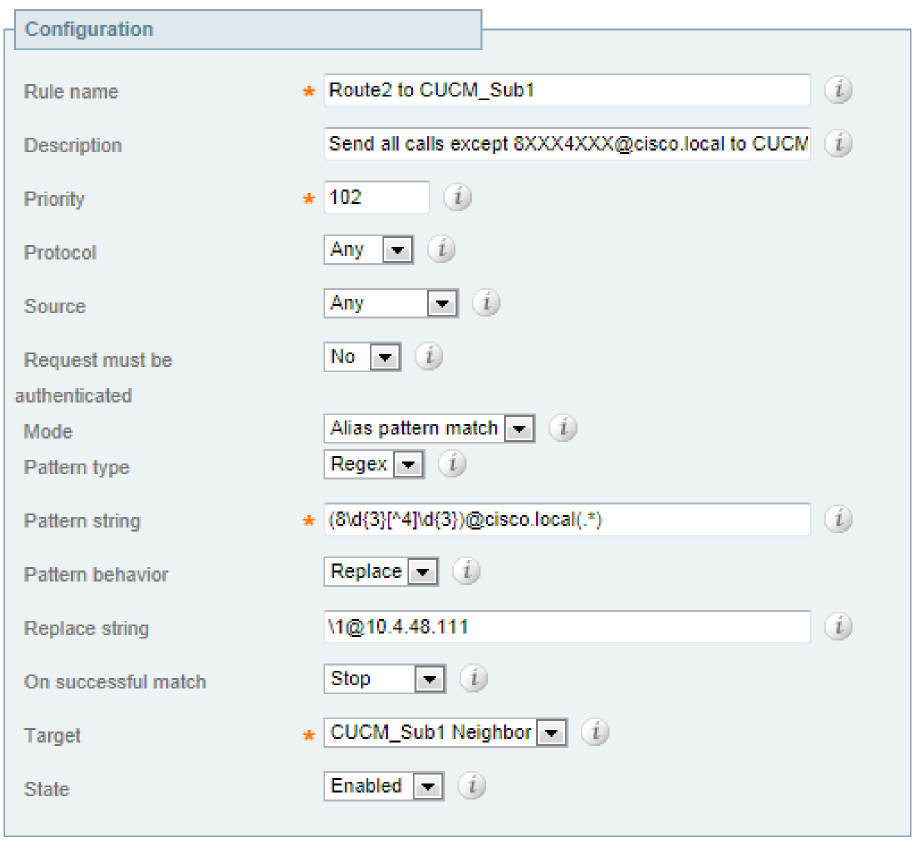
- Rule name—**Route1 to CUCM_Sub1**
- Description—**Send all 8XXX4XXX except 8XXX4[6-7]XX calls to CUCM**
- Priority—**100** (same priority for all subscribers)
- Protocol—Any
- Source—**Any**
- Request must be Authenticated—**No**
- Mode—**Alias Pattern Match**
- Pattern Type—**Regex**
- Pattern String—**(8\d{3}4[^6-7]\d{2})@cisco.local(.*)**
- Pattern behavior—**Replace**
- Replace String—**\1@10.4.48.111**
- On successful match—**Stop**
- Target—**CUCM_Sub1 Neighbor**
- State—**Enabled**



Step 7: Navigate to **VCS configuration > Dial plan > 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)
- Protocol—**Any**
- 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**



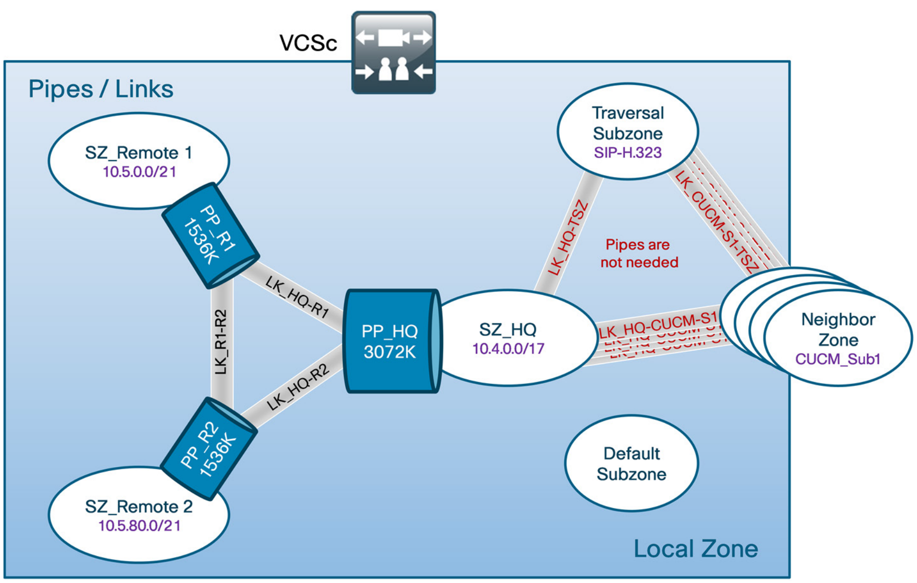
Step 9: Repeat Step 5 through Step 8 for each subscriber in the Unified CM cluster. Change the Rule name, Replace string's IP address and Target for each set of search rules.

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 pipes

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 headquarters site allows two calls at 1536 kbps. The additional WAN bandwidth permits higher quality video and audio between the locations.

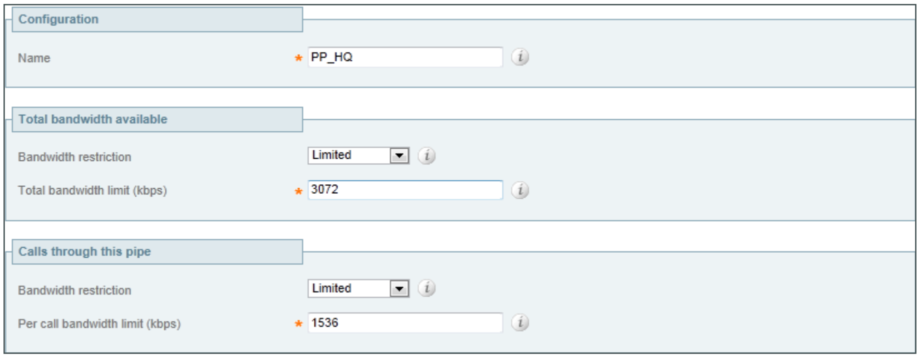
A link is automatically created between the traversal subzone and the Unified CM neighbor zone, which permits H.323 calls to CTS endpoints. However, a link is needed between the neighbor zone and the headquarters subzone to allow SIP calls between the two systems. The bandwidth is controlled by the remote-site 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 page, enter the following values, and then click **Save**:

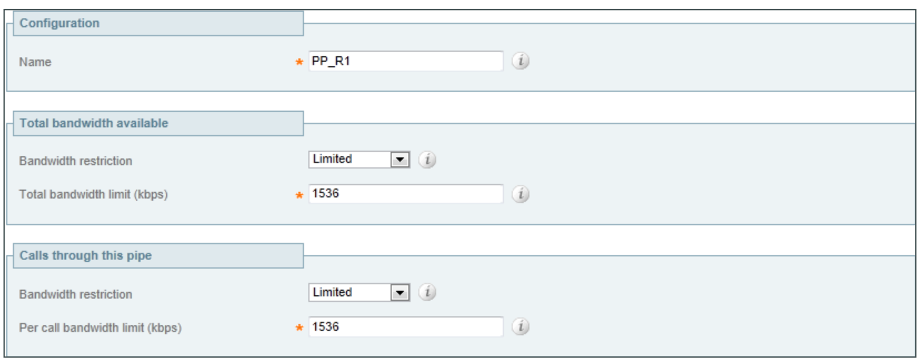
- Bandwidth restriction—**Limited**
- Total bandwidth limit (kbps)—**3072** (two 1.5 Mbps calls)
- Bandwidth restriction—**Limited**
- Per call bandwidth limit (kbps)—**1536**



Step 3: On the Pipes page, click the name of the remote site pipe—PP_R1

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

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



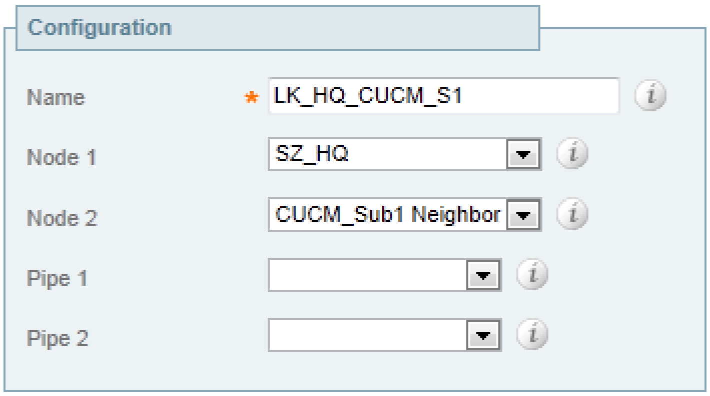
Step 5: Repeat Step 3 and Step 4 for all remote-site locations.

Procedure 4 Configure VCS links

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

Step 2: On the Create link page, enter the following values, and then click **Create link**:

- Name—**LK_HQ_CUCM_S1**
- Node 1—**SZ_HQ**
- Node 2—**CUCM_Sub1 Neighbor**



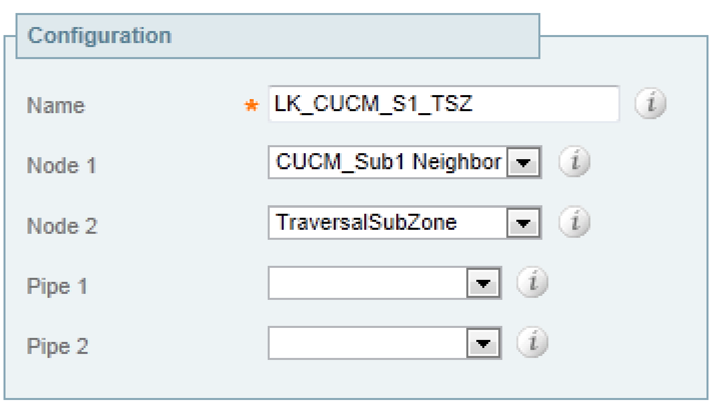
Step 3: Repeat Step 1 and Step 2 for each subscriber neighbor zone in the VCS cluster. Change the Name and Node 2 for each Link.

LK_HQ_CUCM_S1	SZ_HQ	CUCM_Sub1 Neighbor	0	0 kbps
LK_HQ_CUCM_S2	SZ_HQ	CUCM_Sub2 Neighbor	0	0 kbps
LK_HQ_CUCM_S3	SZ_HQ	CUCM_Sub3 Neighbor	0	0 kbps
LK_HQ_CUCM_S4	SZ_HQ	CUCM_Sub4 Neighbor	0	0 kbps

VCS creates default links to the CUCM Neighbor Zone. Step 4 and Step 5 modify the name of the Traversal Subzone link to make it more readable. Step 7 deletes the links to the Default Zone because it is not needed.

Step 4: From the Links page, click **Zone001ToTraversalSZ**.

Step 5: From the Edit link page, change the name of the link to **LK_CUCM_S1_TSZ**, and then click **Save**.



Step 6: Repeat Step 4 and Step 5 for each Unified CM subscriber neighbor zone in the VCS cluster. Change the Name and Node 1 for each Link.

LK_CUCM_S1_TSZ	CUCM_Sub1 Neighbor	TraversalSubZone	0	0 kbps
LK_CUCM_S2_TSZ	CUCM_Sub2 Neighbor	TraversalSubZone	0	0 kbps
LK_CUCM_S3_TSZ	CUCM_Sub3 Neighbor	TraversalSubZone	0	0 kbps
LK_CUCM_S4_TSZ	CUCM_Sub4 Neighbor	TraversalSubZone	0	0 kbps

Step 7: From the Links page, choose the following links, and then click **Delete.** On the Confirm page, click **Yes**.

- Zone001ToDefaultSZ—**Select**
- Zone002ToDefaultSZ—**Select**
- Zone003ToDefaultSZ—**Select**
- Zone004ToDefaultSZ—**Select**

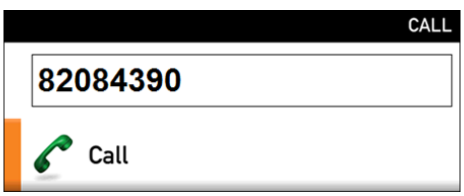
☑	Zone001ToDefaultSZ	CUCM_Sub1 Neighbor	DefaultSubZone	0	0 kbps
☑	Zone002ToDefaultSZ	CUCM_Sub2 Neighbor	DefaultSubZone	0	0 kbps
☑	Zone003ToDefaultSZ	CUCM_Sub3 Neighbor	DefaultSubZone	0	0 kbps
☑	Zone004ToDefaultSZ	CUCM_Sub4 Neighbor	DefaultSubZone	0	0 kbps

Procedure 5 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 display, press the **Home** button on the remote.

Step 2: Enter the extension of a CTS endpoint **82084390** and press the green **Call** button.



Step 3: To view the call in progress, use the remote to navigate to **Home > Settings > System Information,** and on the Systems Information page, 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**

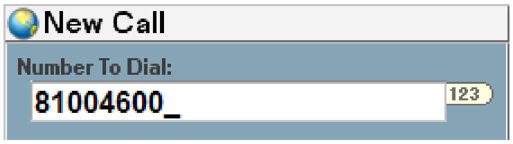
Step 4: Press the red **End call** button to hang up the call.

Procedure 6 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 extension of a multipurpose endpoint **81004600,** and then select **Dial**.



Step 3: To view the call in progress, use your web browser to access the CTS endpoints administrative interface, and then log in using the SSH admin username and password. For example: **https://10.5.84.50/**

Step 4: On the Cisco TelePresence Systems Administration page, 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.

Real Time Call Statistics	
Call Connected	Yes
Registered to Cisco Unified Communications Manager	Yes
Local Number	82084390
Audio/Video Call	
Call Start Time	Thu Nov 1 17:45:43 2012
Call Duration	280 seconds
Call Type	Outgoing
Remote Number	81004600
Call State	Answered
Security Level	Non-Secure
Actual Bit Rate	1227000 bps, 1280x720
Negotiated Bit Rate	727000 bps
Historical Call Statistics (Not including current call, if any)	
Call Statistics Clear Time	Wed Oct 31 14:37:27 2012
Last Call Start Time	Thu Nov 1 17:30:52 2012
Last Call Duration	821 seconds
Number of Calls Since System Setup	30
Time in Calls Since System Setup (seconds)	10833
Number of Calls Since Last Reboot	1
Time in Calls Since Last Reboot (seconds)	821
Registered to Cisco Unified Communications Manager	Yes
Configured Bit Rate	Not Available

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

The Cisco TelePresence Server, also known as a Multipoint Control Unit (MCU), is used for 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.

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	CVD 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 -7	
SNMP read-only community	cisco	
SNMP read/write community	cisco123	
SNMP trap community	cisco	
Remote syslog server	10.4.48.35	

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.

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
```

Tech Tip

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

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 Campus Wired LAN Design 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 the 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)

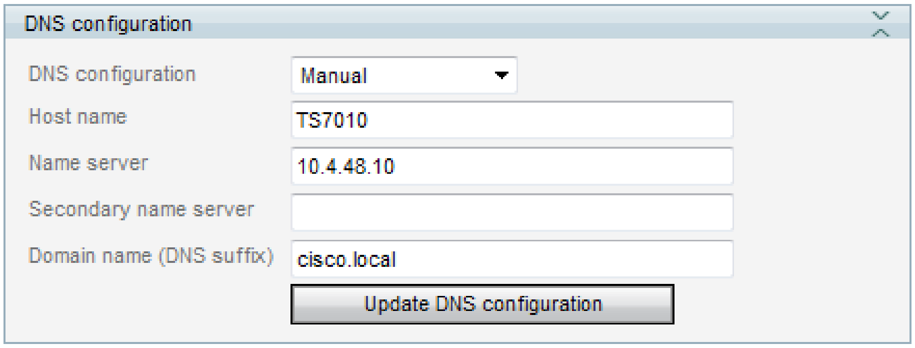
Step 3: Using the drop down menu navigate to **Configuration > Change password**.

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

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

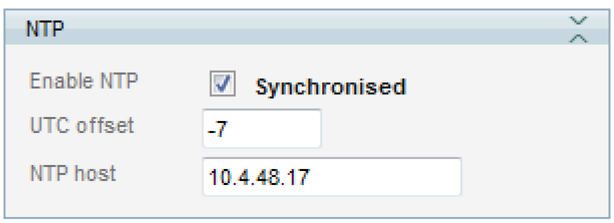
Step 5: Navigate to **Network > DNS**, enter the following values, and then click **Update DNS configuration**:

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



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**



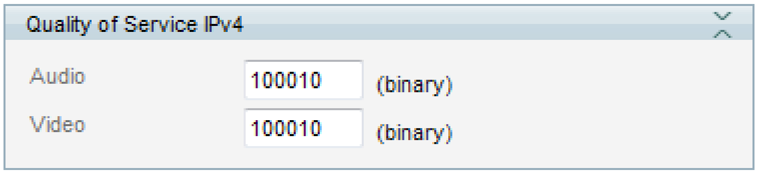
Tech Tip

QoS is needed to put the media and signaling traffic into the low-latency queues defined in the Campus Wired LAN Design 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.

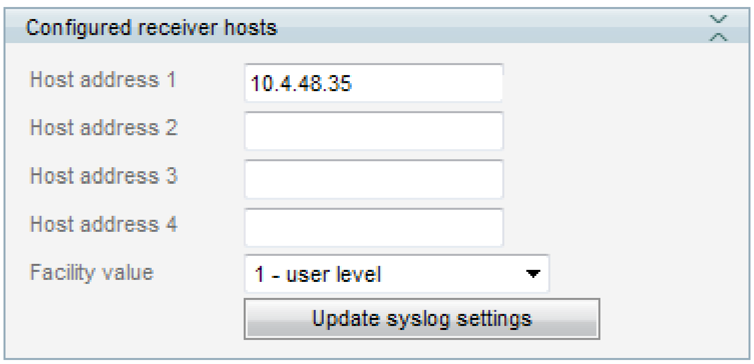
Step 7: Navigate to **Network > QoS**, enter the following values under Quality of Service IPv4, and then click **Update QoS settings**:

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



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.**



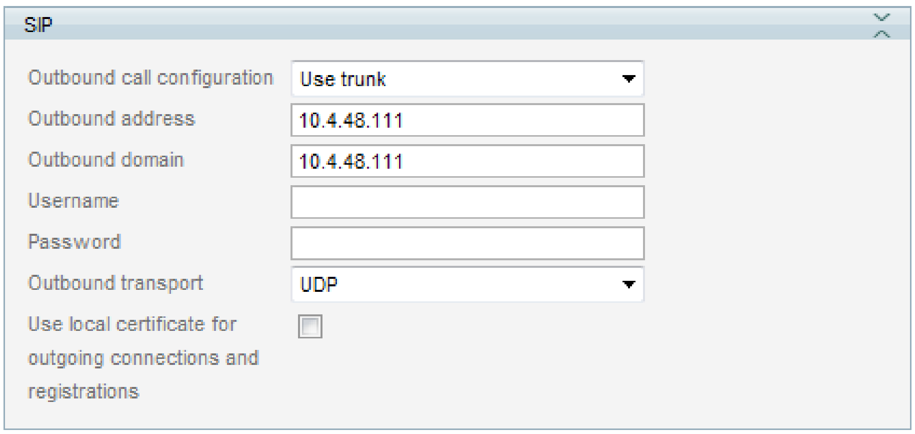
The platform configuration of the Cisco MCU is complete.

Procedure 4 Configure SIP Trunk from Unified CM

Configure the Cisco TelePresence Server with a SIP Trunk from Unified CM to allow the MCU to accept calls that are made using a service prefix. 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 > SIP settings,** enter the following values**,** 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 the **Key** icon to logout.

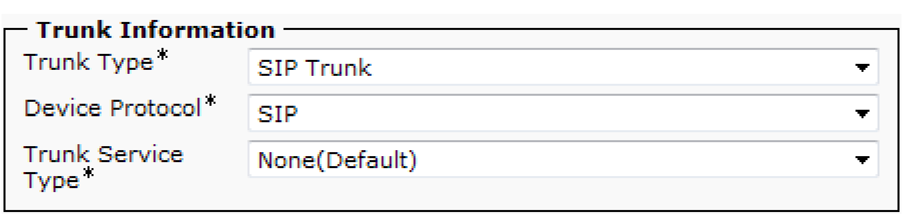
Step 3: Using your web browser, access the Unified CM Administration interface of the publisher in your cluster.

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**.

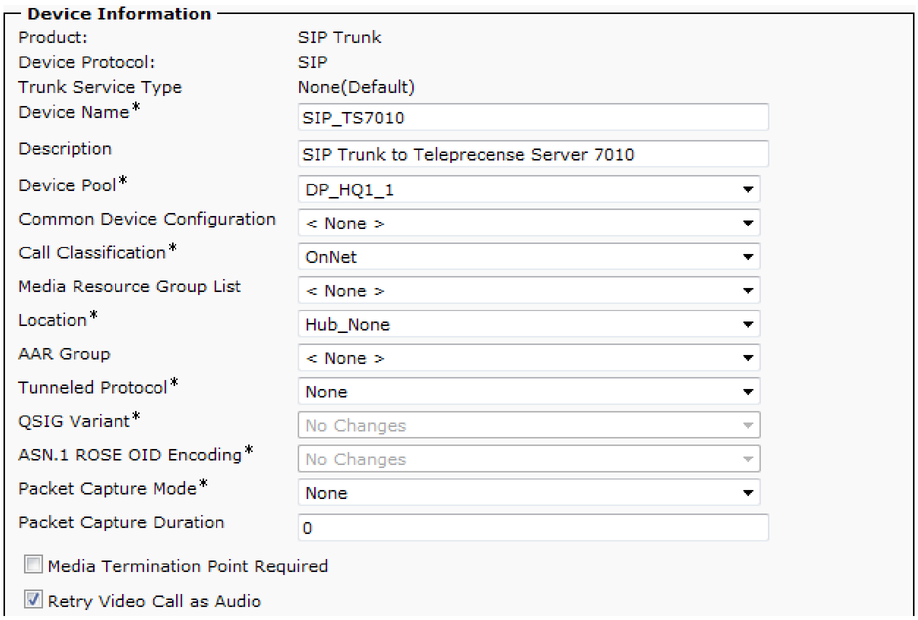
Step 6: Navigate to **Device > Trunk** and click **Add New**.

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

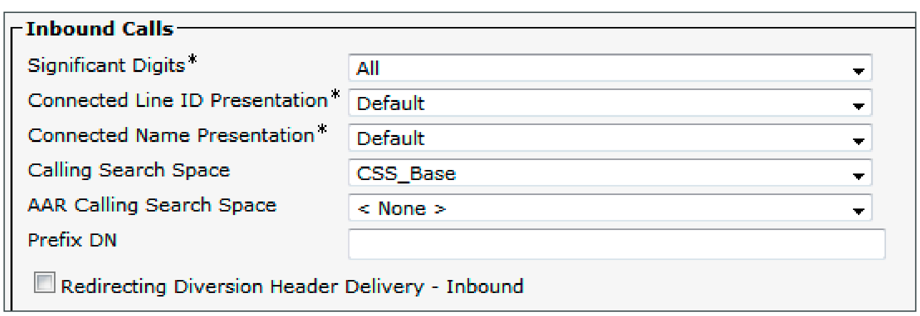


Step 8: Enter the following values in the **Device Information** configuration section.

- 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—**Select**

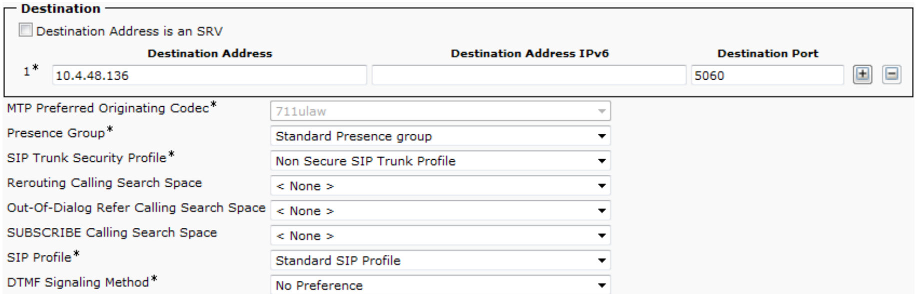


In the **Inbound Calls** section under the **Call Routing Information** section, use the drop down labeled **Calling Search Space** to select **CSS_Base**.



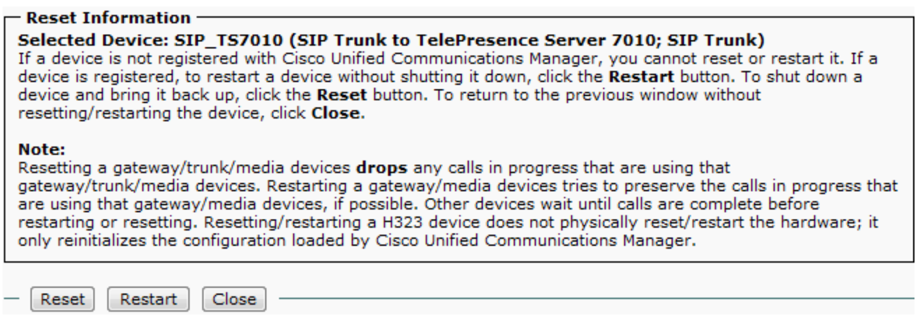
Step 9: Enter the following values in the **SIP Information** section, and then click **Save**. On the message page, click **OK**.

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



Step 10: On the Trunk Configuration page, click **Reset**.

Step 11: From the Device Reset page, click **Reset**, and then click **Close**.

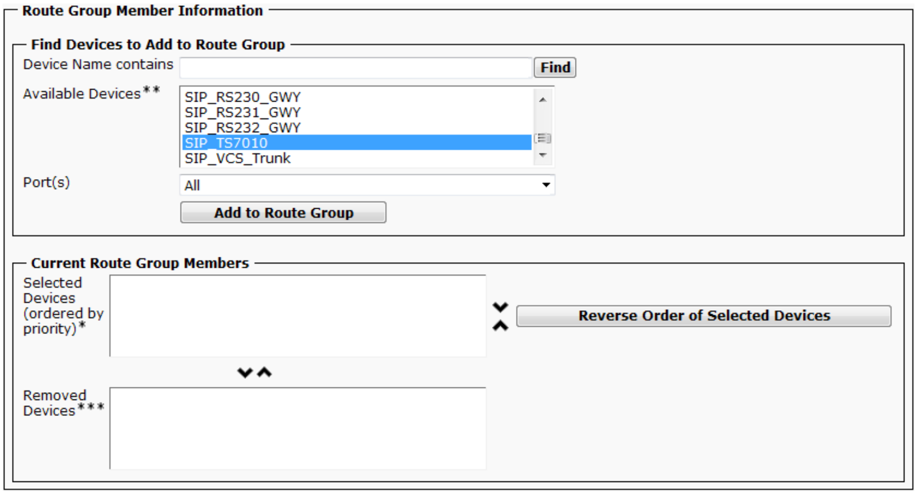


Step 12: Navigate to **Call Routing > Route/Hunt > Route Group** and click **Add New**.

Step 13: On the Route Group Configuration page, enter the Route Group Name: **RG_TS7010_SIP**.

Step 14: From the Available Devices, enter the following values, click **Add to Route Group**, and then click **Save**:

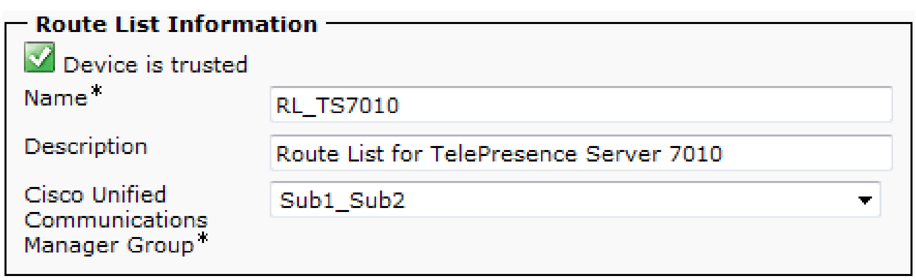
- Available Devices—**SIP_TS7010**
- Port(s)—**All**



Step 15: Navigate to **Call Routing > Route/Hunt > Route List** and click **Add New**.

Step 16: On the Route Group Configuration page, enter the following values, and then click **Save**:

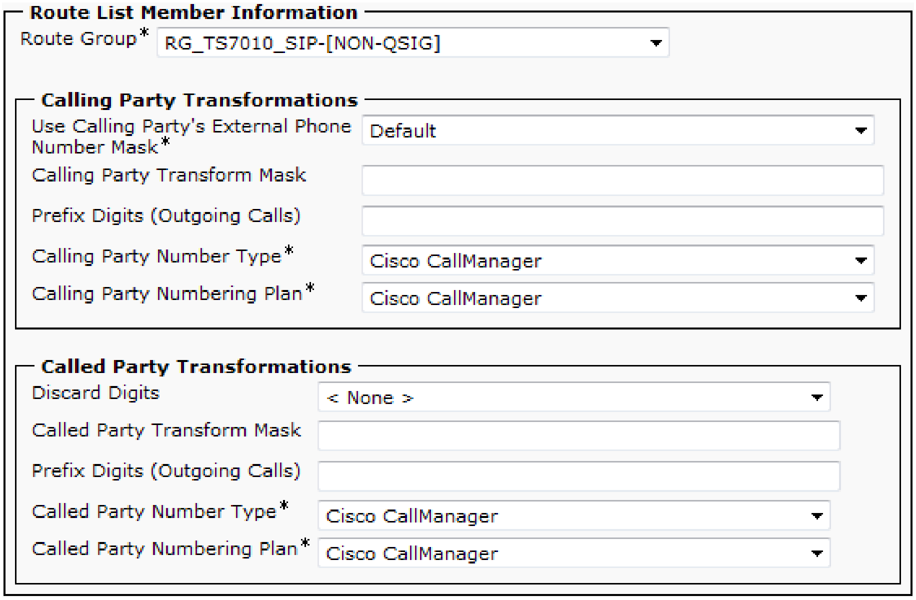
- Name—**RL_TS7010**
- Description—**Route List for TelePresence Server 7010**
- Cisco Unified Communications Manager Group—**Sub1_Sub2**



Step 17: In the Route List Member Information section, click **Add Route Group**.

Step 18: On the Route List Detail Configuration page, enter the following value, and then click **Save**. On the message page, click **OK**.

- Route Group—**RG_TS7010_SIP-[NON-QSIG]**



Step 19: On the Route List Configuration page, click **Reset**.

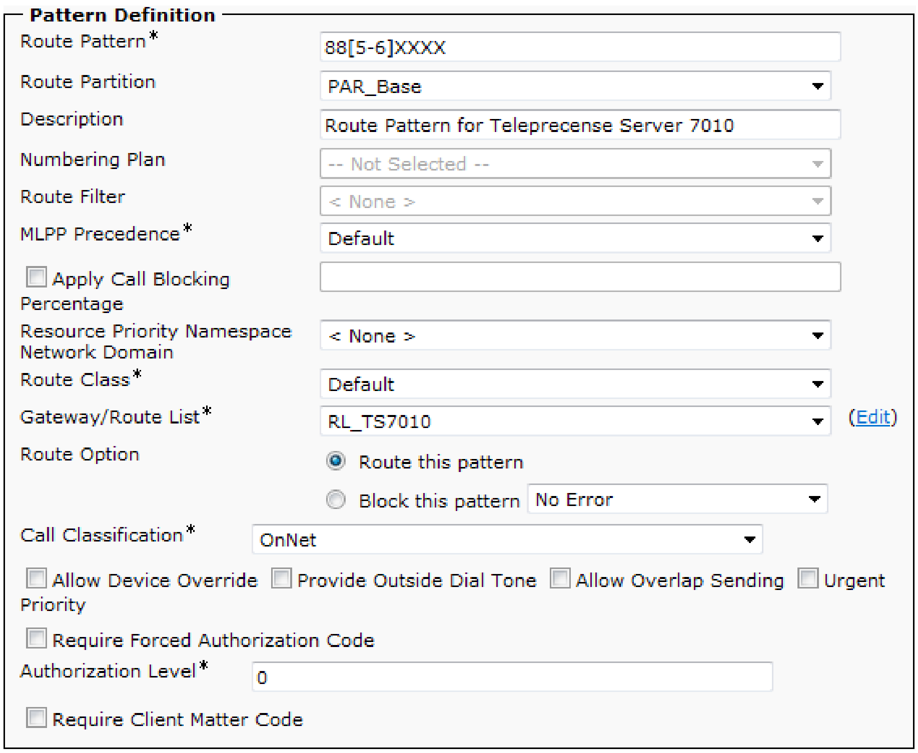
Step 20: From the Device Reset page, click **Reset**, and then click **Close**.

This design uses a 3 digit prefix and a 4 digit meeting identifier for a total of 7 digits. The 885 prefix and the 886 prefix are used for scheduled conferences on the TelePresence Server.

Step 21: Navigate to **Call Routing > Route/Hunt > Route Pattern** and click **Add New**.

Step 22: On the Route Pattern Configuration page, enter the following values, and then click **Save**. On the two message pages, click **OK**.

- 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—**Clear** (Unchecked)



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 and a 4 digit meeting identifier for a total of 7 digits. The 885 prefix and the 886 prefix are used 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**.

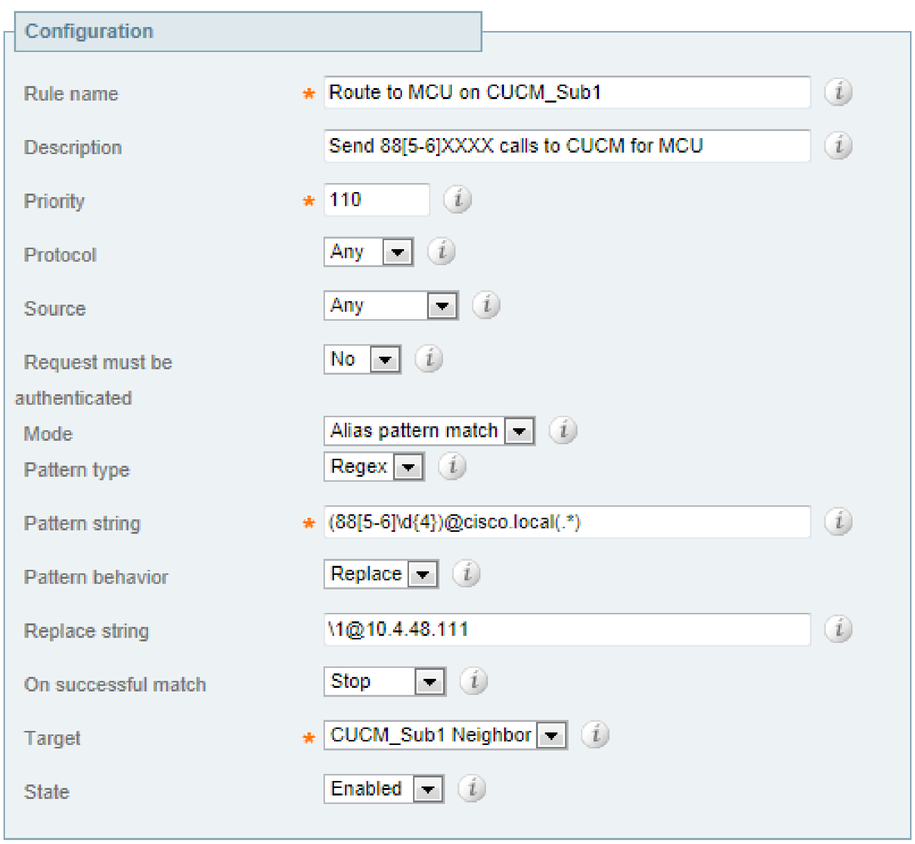
Step 2: Enter the following values, and then click **Login**:

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

Step 3: Navigate to **VCS configuration > Dial plan > 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**
- Protocol—**Any**
- 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	Route to MCU on CUCM_Sub1	Any	No	Alias pattern match	Regex	(88[5-6]\d{4})@cisco.local(.*)	Replace	Stop	CUCM_Sub1 Neighbor
110	✔ Enabled	Route to MCU on CUCM_Sub2	Any	No	Alias pattern match	Regex	(88[5-6]\d{4})@cisco.local(.*)	Replace	Stop	CUCM_Sub2 Neighbor
110	✔ Enabled	Route to MCU on CUCM_Sub3	Any	No	Alias pattern match	Regex	(88[5-6]\d{4})@cisco.local(.*)	Replace	Stop	CUCM_Sub3 Neighbor
110	✔ Enabled	Route to MCU on CUCM_Sub4	Any	No	Alias pattern match	Regex	(88[5-6]\d{4})@cisco.local(.*)	Replace	Stop	CUCM_Sub4 Neighbor

PROCESS

Configuring Conferences

1. Configure scheduled conferences

The scheduled conference configuration includes one type of conference where participants call in and another where the Cisco MCU calls each participant at the appointed time. Because the TelePresence Server does not support reservationless conferences, an administrator can either create a one-time call-out conference for the user or they can create a permanent call-in conference for users who require the functionality on an ongoing basis.

Procedure 1 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 885 or 886. In this example, a onetime call-out conference will use the ID of 8861234 and a permanent call-in conference will use 8856789.

If you want Cisco MCU to call the participants at the beginning of the meeting, the SIP or H323 endpoints are added to the MCU before creating the conferences.

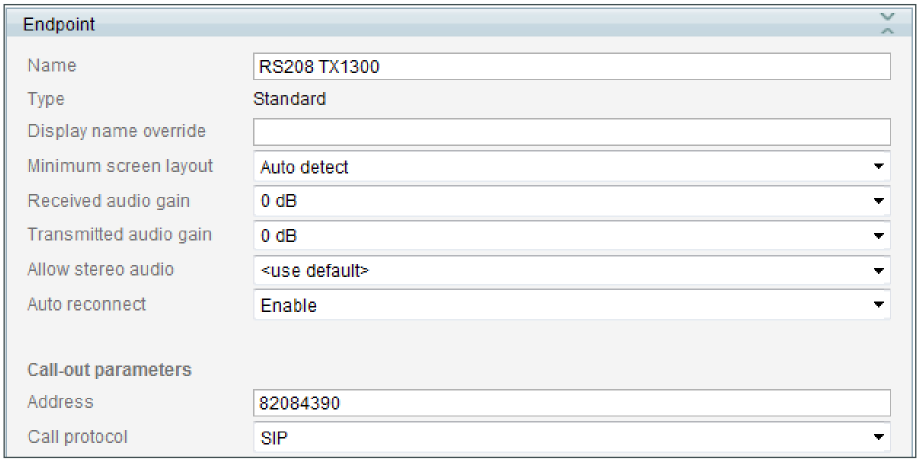
Step 1: Using your web browser, access the administrator login interface of the Cisco MCU.

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

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

Step 3: Navigate to **Endpoints > Add new endpoint**, enter the following values and click **Add new endpoint**.

- Name—**RS208 TX1300**
- Address—**82084390**
- Call Protocol—**SIP**



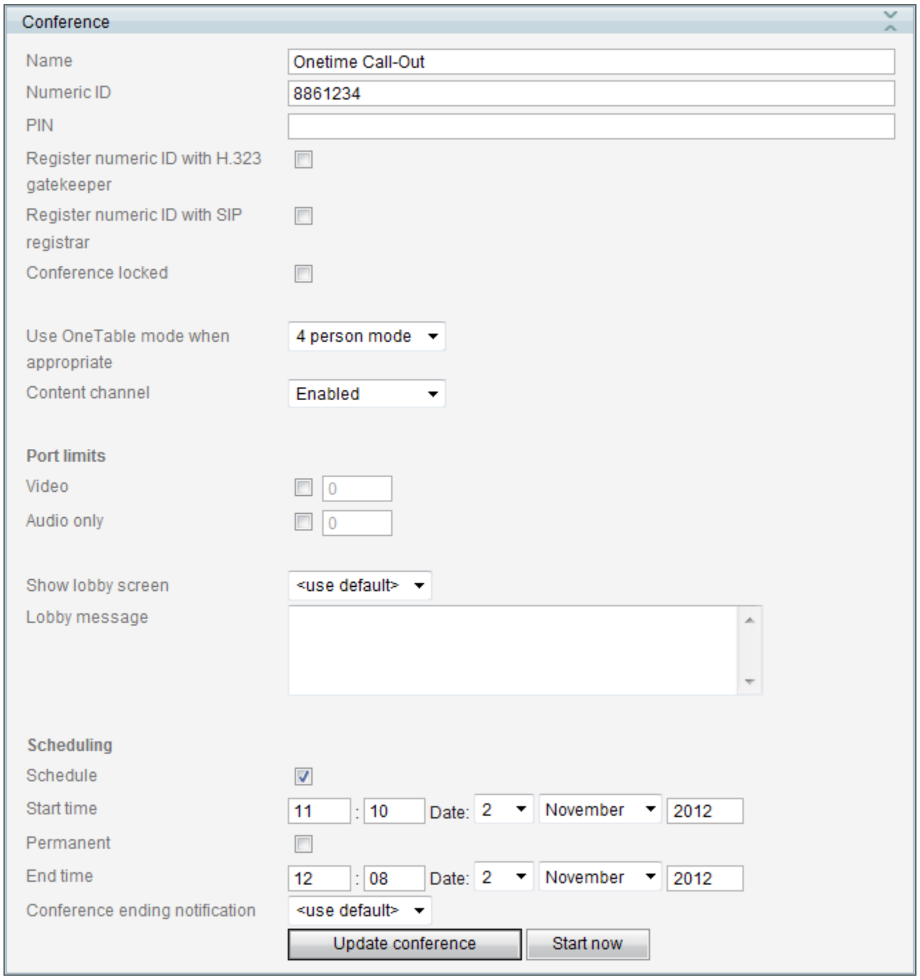
Step 4: Repeat Step 3 for additional endpoints. Change the Name and Address for each Endpoint.

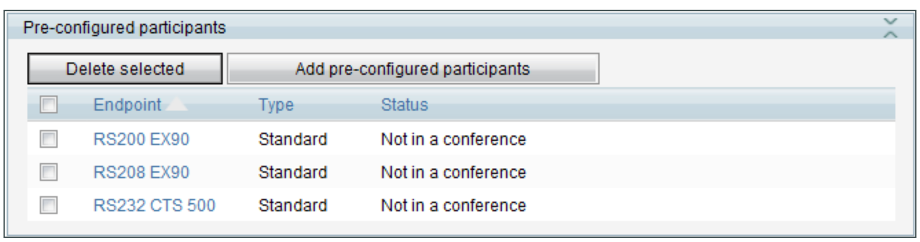
The next set of steps will create a onetime call-out conference.

Step 5: Navigate to **Conferences > Add new conference**, enter the following values, and then click **Add new conference**:

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

Step 6: Click **Add pre-configured participants,** for example, select: **RS200 EX90, RS232 CTS 500** and **RS208 EX90**, and then click **Update**.





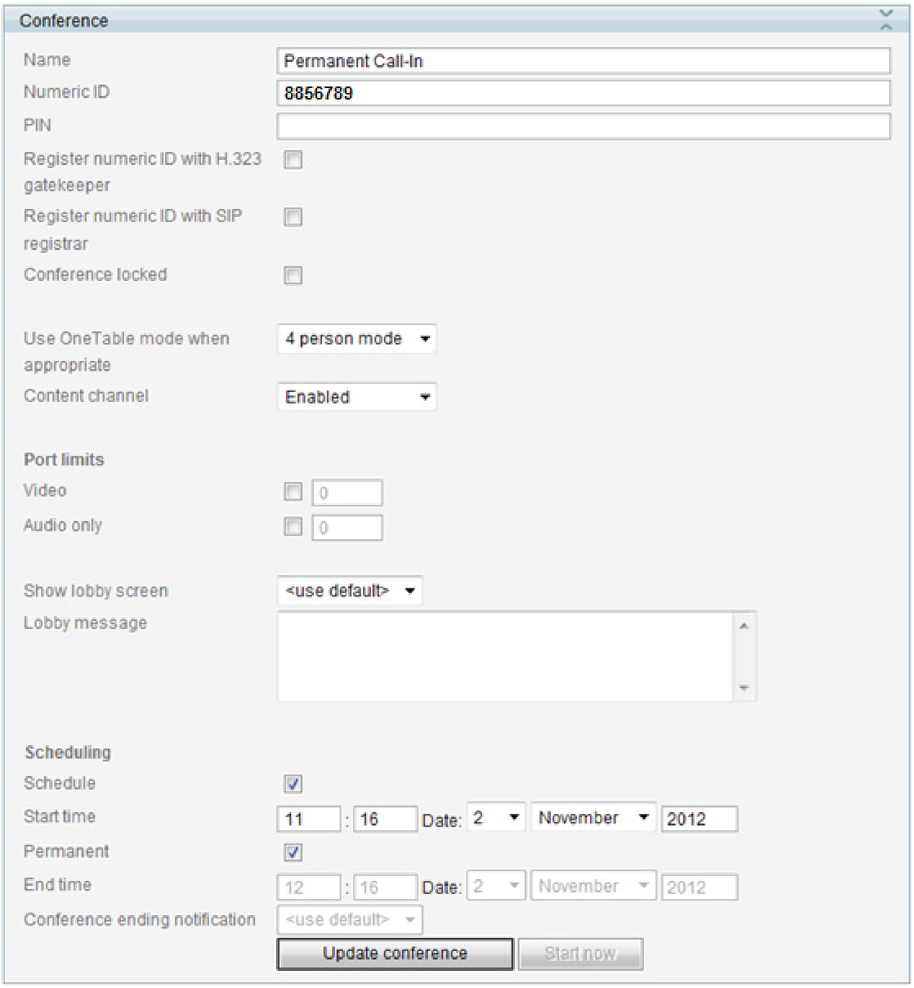
At the specified date and time, the MCU will call the participants listed and the conference will begin.

The next set of steps will create a permanent call-in conference, which can also be used as a reservationless conference when required.

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—**8856789**
- Schedule—**Select**
- Start time—**[current time and date]**
- Permanent—**Select**



The participants can call **8856789** at any time to access the conference.

The conference 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	X7.2.0
	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 UCS C240 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C240M3S	9.1(1a) ESXi 5.0
	Cisco UCS C220 M3 C-Series Solution Pak for unified communications applications	UCUCS-EZ-C220M3S	
	Cisco UCS C220 M3 for Business Edition 6000	UCSC-C220-M3SBE	
Multipoint Control Unit	Cisco TelePresence Server 7010	CTI-7010-TPSRV-K9	2.3(1.55)
	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	TC5.1.4
	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	

Functional Area	Product Description	Part Numbers	Software
Multipurpose Room System	Cisco TelePresence Profile 42 w PHD 1080p 12x Cam, NPP, Touch, 2 Mics	CTS-P42C40-K9	TC5.1.4
	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	
	XLR Table mic - for auto expand only	CTS-MIC-TABL20XLR+	
Video Telephones	Unified IP Phone with six lines, video, color, Wi-Fi, Bluetooth, USB	CP-9971	SIP9971.9-3-2-10
	Unified IP Phone with four lines, video, color	CP-8945	SIP8941_8945.9-3-2-12
CTS Immersive Endpoints	Cisco TelePresence System 1100	CTS-1100	CTS.1-9-2-19R-K9.P1
	Cisco TelePresence System 500 Series	CTS-500-32	
	Cisco TelePresence 500 Structure - Tabletop	CTS500-STRUC-TABL	
CTS Phone	Unified IP Phone with eight lines, color for CTS control	CP-7975G-CTS	SIP75.9-3-1SR1-1S

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 5.2(1)N1(3) 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	
	Cisco Nexus 5500 Layer 3 Enterprise Software License	N55-LAN1K9	
	Cisco Nexus 5500 Storage Protocols Services License, 8 ports	N55-8P-SSK9	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	–
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	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(2)SE2 IP Base license
	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(2)SE2 IP Base license
	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	3.4.0.SG(15.1-2SG) IP Base license
	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 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) IP Base license
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 IP Base license
	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(2)SE2 IP Base license
	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(2)SE2 LAN Base license
	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	

Feedback

Please use the feedback form to send comments and suggestions about this guide.

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.

B-0000435-1 08/13