



Avaya Solution & Interoperability Test Lab

Configuring SIP Connectivity between the Avaya Meeting Exchange S6200 Conferencing Server R5.2 and Cisco Unified Communications Manager R6. 1 – Issue 1.0

Abstract

These Application Notes present the procedures for configuring SIP connectivity between the Avaya Meeting Exchange S6200 Conferencing Server and Cisco Unified Communications Manager. SIP connectivity is enabled via directly connected SIP trunking between Avaya Meeting Exchange and Cisco Unified Communications Manager.

Testing was conducted via the Internal Interoperability Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Meeting Exchange Enterprise S6200 Conferencing Server (MX S6200) and Cisco Unified Communications Manager using SIP trunks. The sample configuration shown in **Figure 1** will be used to compliance test Cisco Unified Communications Manager interoperability with Avaya Meeting Exchange Enterprise S6200.

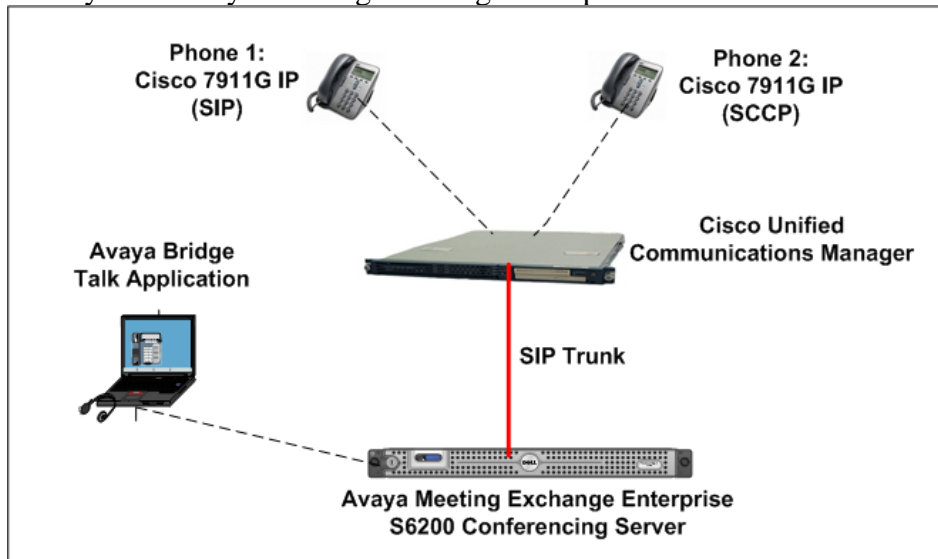


Figure 1 - Avaya Meeting Exchange Enterprise Interoperability Network Topology

The configuration in **Figure 2** will be used to compliance test Cisco Unified Communications Manager interoperability with the Distributed S6200 system. The Cisco Unified Communications Manager supports the Cisco 7911G IP Telephone (SIP) and the Cisco 7911G IP Telephone (SCCP).

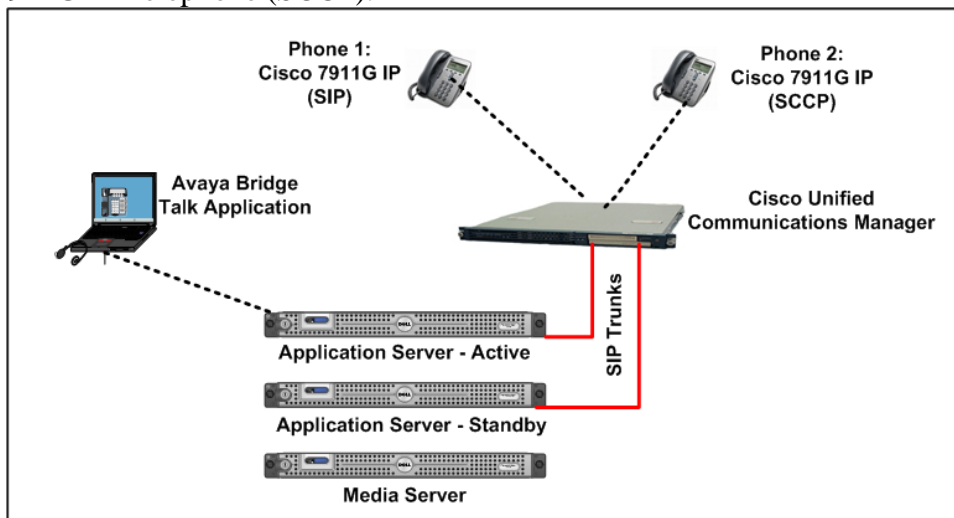


Figure 2 – Distributed Avaya Meeting Exchange Interoperability Network Topology

2. Equipment and Software Validated

The following equipment and software versions were used for the sample configuration provided in these Application Notes.

Equipment	Software
Avaya Meeting Exchange Enterprise Edition S6200	R5.2 (Build 5.2.0.0.22)
Cisco Unified Communications Manager	6.1.2.1000-13
Avaya Bridge Talk (BT)	5.2.0.0.7
Cisco 7911G SIP Telephone	SIP 11.8-4-3S
Cisco 7911G SCCP Telephone	SCCP 11.8-3-4SR1S

Table 1: Equipment and Software Versions

3. Configure Avaya Meeting Exchange Enterprise S6200 Conferencing Server

This section describes the steps for configuring the Avaya Meeting Exchange Enterprise S6200 to interoperate Cisco Unified Communications Manager via SIP trunking. It's assumed that the Meeting Exchange is installed configured and licensed as described in the product documentation (see **reference [1]**). The following steps describe the administrative procedures for configuring the Meeting Exchange:

- Configure SIP Connectivity
- Configure Dialout
- Map DNIS Entries
- Configure Audio Preferences
- Configure Application Server
- Configure Bridge Talk

The following instructions assume having logged in to the Meeting Exchange console using ssh connection to access the Command Line Interface (CLI) with the appropriate credentials.

3.1. Configuring SIP Connectivity

Login in to the Meeting Exchange server console (PuTTY) using ssh to access the Command Line Interface (CLI) with the appropriate credentials. Configure settings that enable SIP connectivity between the Meeting Exchange Enterprise server and other devices by editing the **system.cfg** file as follows:

- Edit **/usr/ipcb/config/system.cfg**
- Add Meeting Exchange S6200 server IP address
 - **IPAddress=(135.64.186.98)**
- Depending on the SIP signalling protocol, TCP or UDP, add one of the following lines to populate the From Header Field in SIP INVITE messages:
 - **MyListener=<sip:6000@135.64.186.98:5060;transport=tcp>**
 - **MyListener=<sip:6000@135.64.186.98:5060;transport=udp>**

Note: The user field 6000, defined for this SIP URI must conform to RFC 3261. For consistency, it is selected to match the user field provisioned for the **respContact** entry (see below).
- Depending on the SIP signalling protocol, TCP or UDP , add one of the following lines to provide SIP Device Contact address to use for acknowledging SIP messages from the Meeting Exchange server:
 - **respContact=<sip:6000@135.64.186.98:5060;transport=tcp>**
 - **respContact=<sip:6000@135.64.186.98:5060;transport=udp>**
- Add the following lines to set the Min-SE timer to **900** seconds in SIP INVITE messages from the Meeting Exchange server:
 - **sessionRefreshTimerValue= 900**
 - **minSETimerValue= 900**

3.2. Configure Dialout

To enable Dial-Out from the Avaya Meeting Exchange Enterprise S6200 Conferencing Server to the Cisco Unified Communications Manager, edit the **telnumToUri.tab** file as follows:

- Edit **/usr/ipcb/config/telnumToUri.tab** file with a text editor
- Add a line to the file to route outbound calls from the Avaya Meeting Exchange Enterprise S6200 Conferencing Server to the Cisco Unified Communications Manager

6000 sip:\$1@135.64.186.107:5060;transport=tcp

3.3. Map DNIS Entries

To map DNIS entries, run the **cbutil** utility on Meeting Exchange. Log in to the Meeting Exchange with an ssh connection using PuTTY with the appropriate credentials. Enable Dial-In access (via passcode) to conferences provisioned on the Meeting Exchange as follows:

- Add a DNIS entry for a **scan call function** corresponding to DID **11111** by entering the following command at the command prompt:
cbutil add <dnis> <rg> <msg> <ps> <ucps> <func> [-o <of> -l <ln> -c <cn> -crs <n> -cre

where the variables for add command is defined as follows:

- o **<dnis>** DNIS
- o **<rg>** Reservation Group
- o **<msg>** Annunciator message number
- o **<ps>** Prompt Set number (0-20)
- o **<ucps>** Use Conference Prompt Set (y/n)
- o **<func>** One of: DIRECT/SCAN/ENTER/HANGUP/AUTOVL/FLEX
- o **-o <of>** Optional On-failure function – one of: ENTER/HANGUP
- o **-l <"ln">** Optional line name to associate with caller
- o **-c <"cn">** Optional company name to associate with caller
- o **-crs <n>** Optional conference room start number
- o **-cre <n>** Optional conference room end number

In this sample configuration, the DNIS entry for a **scan call function** was added corresponding to DNIS 11111 by entering the following command at the command prompt:

```
[MXSIL]# cbutil add 11111 0 247 1 N SCAN
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.
```

At the command prompt, enter **cbutil list** to verify the DNIS entries provisioned.

```
[MXSIL]# cbutil list
cbutil
Copyright 2004 Avaya, Inc. All rights reserved.

DNIS   Grp Msg PS   CP Function On Failure Line Name Company Name Room Start
Room End
-----
11111          0   247 1   Y  SCAN      DEFAULT      SILTest
```

3.4. Configure Audio Preferences file

The **audioPreference.cfg** file is located at **/usr/ipcb/config/** specifies the order in which codecs are offered in the Session Description Protocol.

```
# audioPreferences.cfg
# This table is an ordered list of MIME subtypes specifying the codecs
# supported
# by this media server. The list is specified in the order in which an SDP
# offer
# will list the various MIME subtypes on the m=audio line.
# For static payload type numbers (i.e. numbers between 0 - 96) please use the
# iana registered numbering scheme.
# See: http://www.iana.org/assignments/rtp-parameters

mimeSubtype      payloadType
PCMU              0
PCMA              8
G722              9
G729              18
iLBC30            97
iLBC20            98
wbPCMU            102
wbPCMA            103
telephone-event  120
iSAC              104
G726_16           105
G726_24           106
G726_32           107
G726_40           108
```

3.5. Configure Application Server

To configure the Meeting Exchange server, edit the **processTable.cfg** file as follows:

- Edit the **/usr/ipcb/config/processTable.cfg** file with a text editor.

Note: Replacing aps1-IP with IP address of Application server and replacing ms-IP with IP address of the Media Server

processName	ipcKeyNumber	autoStart	ProcessExe	ipAddress	route	ProcessArgs
initipcb	100	0	noexecute	0.0.0.0		
bridget700	102	0	noexecute	0.0.0.0		
				dspEvents/msDispatcher,netEvents/sipAgent		
commsProcess	101	1	/usr/dcb/bin/serverComms	0.0.0.0		
sipAgent	131	1	/usr/dcb/bin/sipagent	<aps1-IP>		
				dspEvents/msDispatcher,appEvents/bridget700		
msDispatcher	132	1	/usr/dcb/bin/msdispatcher	<aps1-IP>		
				netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer		
mediaServer	120	1	/usr/dcb/bin/msInterface	<aps1-IP>		
				appEvents/msDispatcher,netEvents/msDispatcher		1
mediaServer	121	1	/usr/dcb/bin/msInterface	<aps1-ip>		
				appEvents/msDispatcher,netEvents/msDispatcher		2
mediaServer	122	1	/usr/dcb/bin/msInterface	<aps1-ip>		
				appEvents/msDispatcher,netEvents/msDispatcher		3
mediaServerExt	140	1	/usr/dcb/bin/softms	<ms-IP>		
				appEvents/msDispatcher,netEvents/msDispatcher		1
mediaServerExt	141	1	/usr/dcb/bin/softms	<ms-IP>		
				appEvents/msDispatcher,netEvents/msDispatcher		2
mediaServerExt	142	1	/usr/dcb/bin/softms	<ms-IP>		
				appEvents/msDispatcher,netEvents/msDispatcher		3

3.6. Bridge Talk

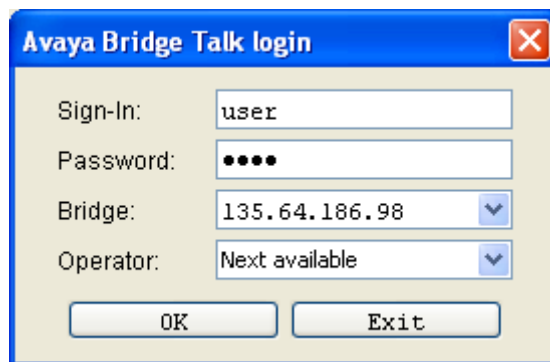
The following steps utilize the Avaya Bridge Talk application to provision a sample conference on the Meeting Exchange. This sample conference enables both Dial-In and Dial-Out access to audio conferencing for endpoints on the Public Switched Telephone Network.

Note: If any of the features displayed in the Avaya Bridge Talk screen captures are not present, contact an authorized Avaya Sales representative to make the appropriate changes.

3.6.1. Initializing Bridge Talk

Invoke the Avaya Bridge Talk application as follows:

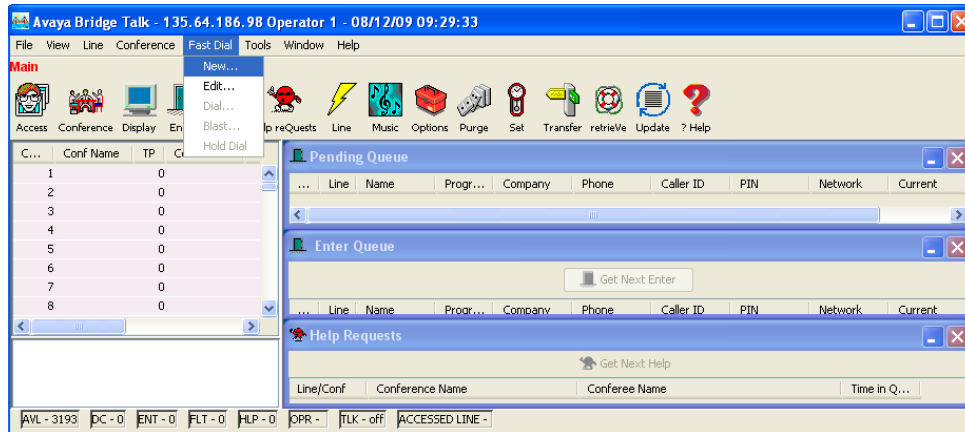
- Double-click on the desktop icon from a Personal Computer loaded with the Avaya Bridge Talk application and with network connectivity to the Meeting Exchange. (Not shown)
- Enter the appropriate credentials in the **Sign-In** and **Password** fields.
- Enter the IP address of the Meeting Exchange server (**135.64.186.98** for this sample configuration) in the **Bridge** field as shown below.

A screenshot of the 'Avaya Bridge Talk login' dialog box. The dialog has a blue title bar with the text 'Avaya Bridge Talk login' and a red close button. The main area is white and contains four labeled input fields: 'Sign-In:' with the text 'user', 'Password:' with four black dots, 'Bridge:' with the IP address '135.64.186.98' and a dropdown arrow, and 'Operator:' with the text 'Next available' and a dropdown arrow. At the bottom, there are two buttons: 'OK' and 'Exit'.

3.6.2. Creating a Dial Out list

Provision a dial list that is utilized for Dial-Out (e.g., Blast dial and Fast dial) from the Meeting Exchange.

- From the Avaya Bridge Talk Menu Bar, click **Fast Dial** → **New**.

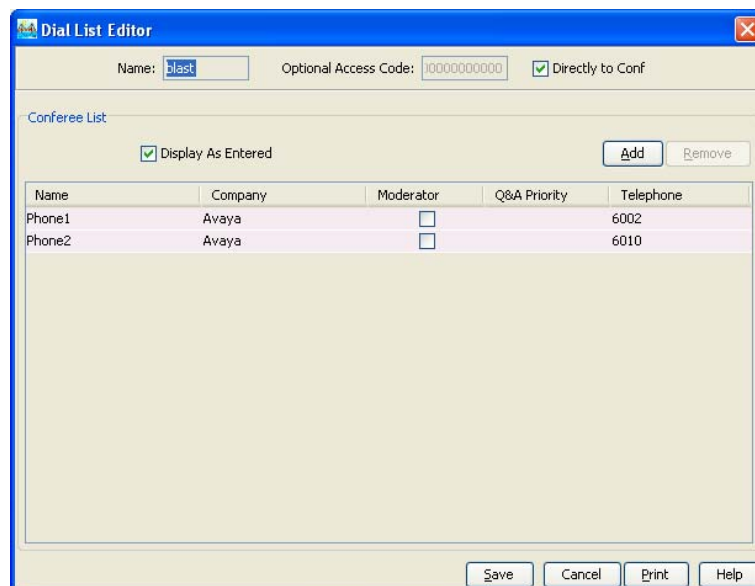


3.6.3. Creating a Dial List

From the **New Dial List** → **Dial List Editor** window that is displayed below:

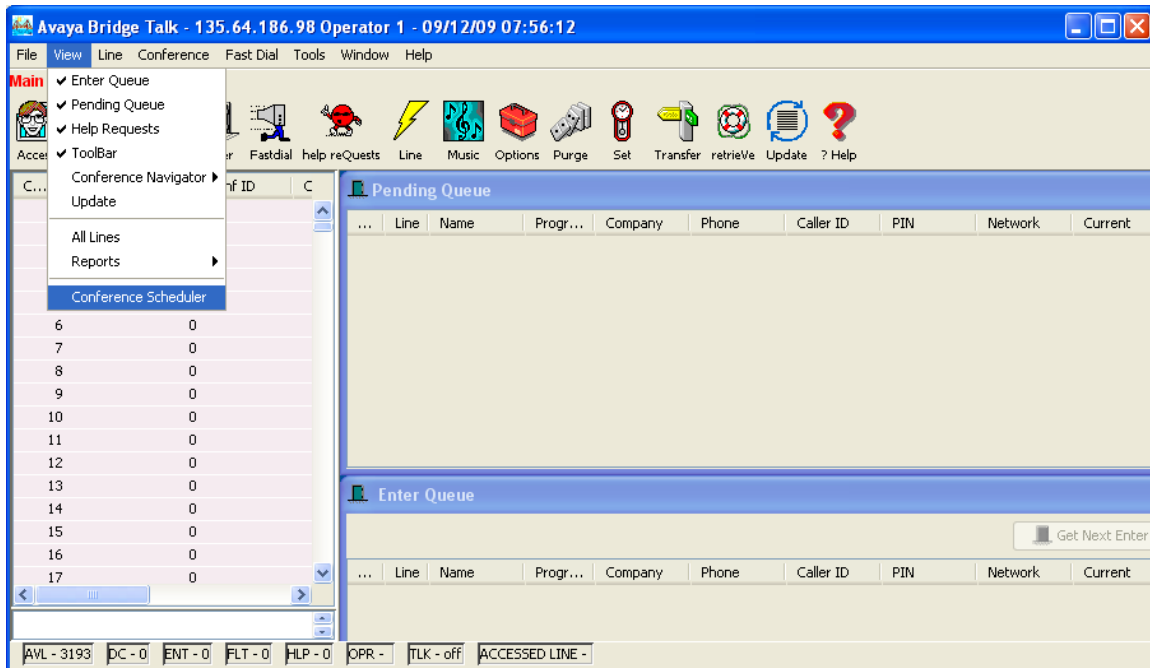
- Enter a descriptive label in the **Name** field.
- Enable conference participants on the dial list to enter the conference without a passcode by selecting the **Directly to Conf** box as displayed.
- Add entries to the dial list by clicking on the **Add** button and enter **Name**, **Company** and **Telephone** number for dial out for each participant. [Optional] Moderator privileges may be granted to a conference participant by checking the **Moderator** box.

When finished, click on the **Save** button on the bottom of the screen.



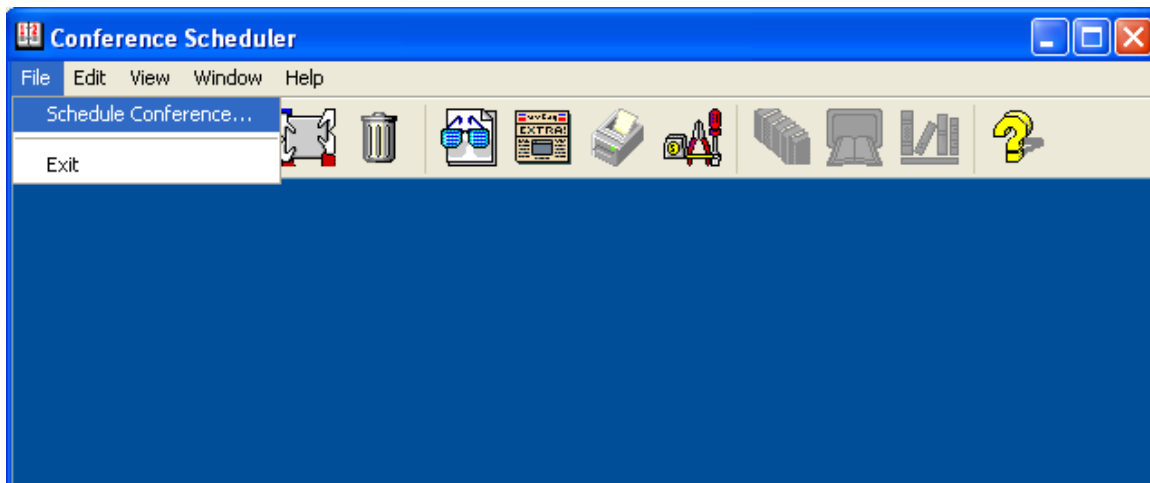
3.6.4. Conference Scheduler

From the **Avaya Bridge Talk** menu bar, click **View → Conference Scheduler** to provision a conference.



3.6.5. Scheduling a Conference

From the **Conference Scheduler** window, click **File → Schedule Conference**.



3.6.6. Provision a Conference

From the **Schedule Conference** window that is displayed, provision a conference as follows:

- Enter a unique **Conferee Code** to allow participants access to this conference.
- Enter a unique **Moderator Code** to allow participants access to this conference with moderator privileges.
- Enter a descriptive label in the **Conference Name** field.
- Administer settings to enable an **Auto Blast** dial by setting Auto Blast/Manual depending on this test.
- Select a dial list by clicking on the **Dial List** button (not shown), select a dial list from the **Create, Select or Edit Dial List** window that is displayed, and click on the **Select** button (to verify Dial out and Blast Dial out).
- When finished, click on the **Ok** button on the bottom of the screen.

Schedule Conference [Administrator Access]

Conference Information

Status: Mode: Conference Type:

Confirmation No.: Conference ID: Weekend:

Name: Billing Code Prompt:

Telephone: Accounting Code: Start Date (dd/mm/yyyy):

Sign-in Name: Security Passcode: End Date (dd/mm/yyyy):

Res Group: Change Conf Opt:

Conferee Code: Op Help Available: Name Record/Play:

Moderator Code: Block Dialout: NRP Annunciator:

Conference Name: Auto Blast: PIN Mode:

Blast Annunciator: PIN List:

Conference Features

Start Time: End Time: Code Duration:

Entry Tone: Exit Tone: Maximum Lines:

Hang up: Music: Security:

Auto Extend Duration: Auto Extend Ports:

Prompt Set: Conference Viewer:

4.0. Configure Cisco Unified Communications Manager

This section provides the procedures for configuring Cisco Unified Communications Manager. These Application Notes assumed that the basic configuration needed to support Cisco IP telephones has been completed. For further information on Cisco Unified Communications Manager, please consult **References** [3] and [4]. The procedures include configuration of the following items:

- Login to Cisco Unified Communications Manager
- Administer SIP Trunk Security Profile
- Administer SIP Trunk
- Administer Route Pattern
- Administer Phone

4.1. Login to Cisco Unified Communications Manager

Open Cisco Unified Communications Manager Administration web interface by using the URL “<http://<ip-address>>” in an Internet browser window, where “<ip-address>” is the IP address of the Cisco Unified Communications Manager. Click on Cisco Unified Communications Manager Administration at the bottom of the screen.

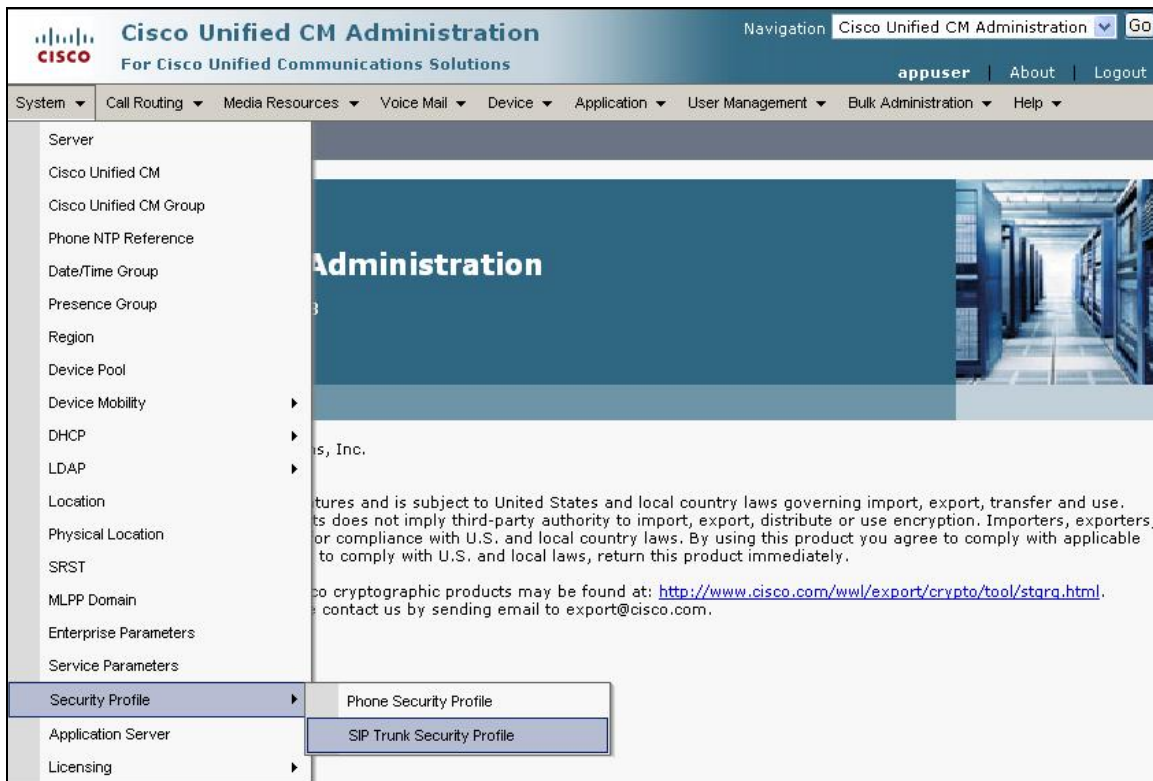


The **Cisco Unified CM Administration** screen is displayed, select **Cisco Unified CM Administration** from the **Navigation** drop-down list, and log in with appropriate credentials.



4.2. Administer SIP Trunk Security Profile

Scroll to the top of the screen, and select **System** → **Security Profile** → **SIP Trunk Security Profile** as shown below.



The **SIP Trunk Security Profile** screen is displayed. Click **Add New** to add a new SIP Trunk Security Profile.

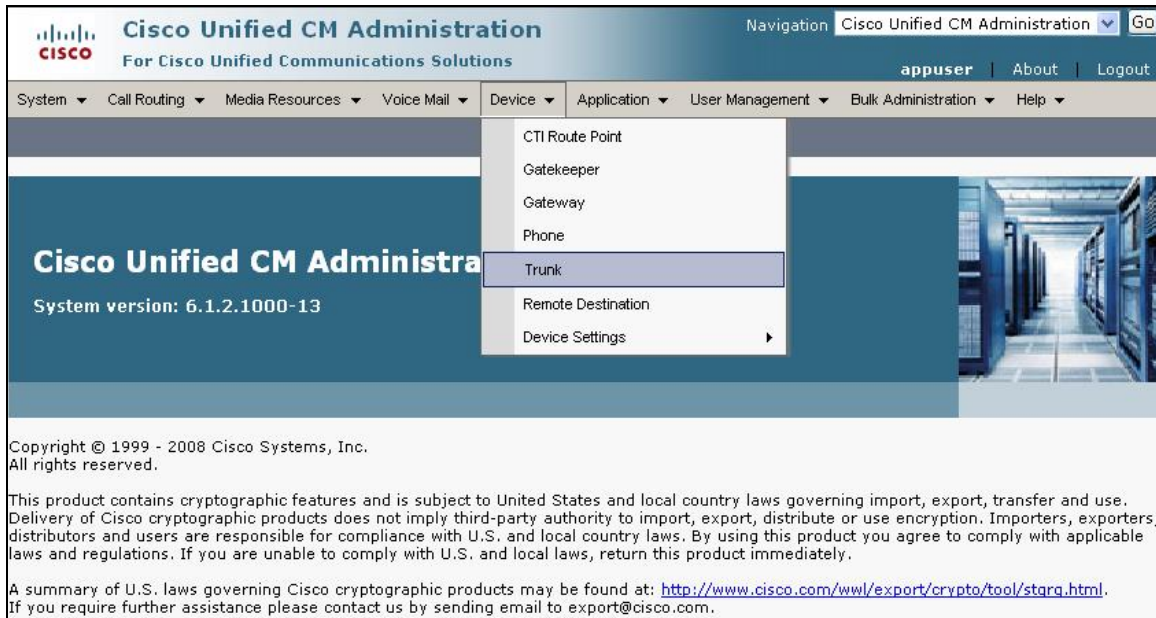
The screenshot shows the 'Find and List SIP Trunk Security Profiles' page in the Cisco Unified CM Administration interface. The page has a header with the Cisco logo and navigation links. Below the header, there is a search bar with a dropdown menu for 'Name' and a text input for 'begins with'. There are buttons for 'Find', 'Clear Filter', and '+'. Below the search bar, there is a message: 'No active query. Please enter your search criteria using the options above.' At the bottom, there is an 'Add New' button.

The **SIP Trunk Security Profile Information** configuration screen is displayed which was used in the sample network. Configure the highlighted areas as shown, and retain the default values for the remaining fields. Click **Save** to commit the changes.

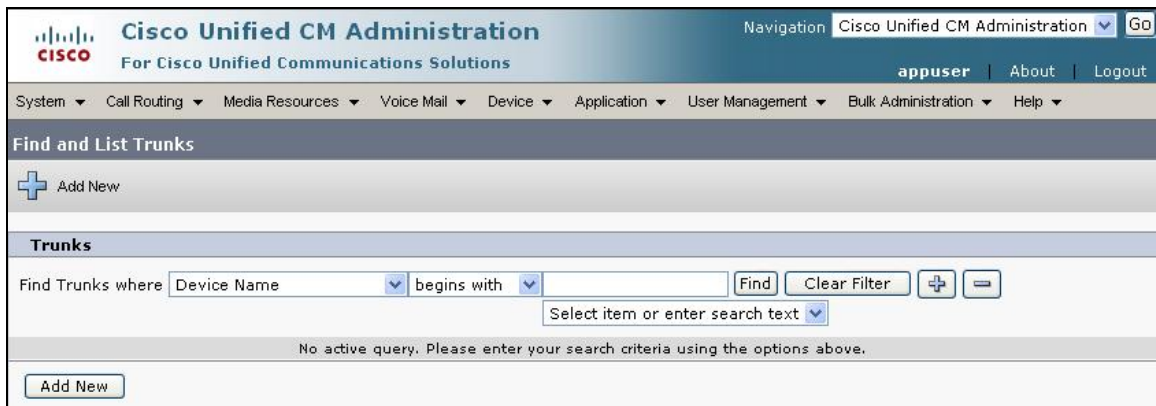
The screenshot shows the 'SIP Trunk Security Profile Configuration' page. The page has a header with 'SIP Trunk Security Profile Configuration' and 'Related Links: Back To Find/List'. Below the header, there are buttons for 'Save', 'Delete', 'Copy', 'Reset', and 'Add New'. The main section is titled 'SIP Trunk Security Profile Information'. It contains several fields: 'Name' (MXSIL), 'Description' (SIP Connection to MX), 'Device Security Mode' (Non Secure), 'Incoming Transport Type*' (TCP+UDP), 'Outgoing Transport Type' (TCP), 'Enable Digest Authentication' (unchecked), 'Nonce Validity Time (mins)*' (600), 'X.509 Subject Name' (empty), and 'Incoming Port*' (5060). Below these fields, there is a section for 'Enable Application Level Authorization' with four checkboxes: 'Accept Presence Subscription' (checked), 'Accept Out-of-Dialog REFER' (checked), 'Accept Unsolicited Notification' (checked), and 'Accept Replaces Header' (checked). At the bottom, there are buttons for 'Save', 'Delete', 'Copy', 'Reset', and 'Add New'.

4.3. Administer SIP Trunk

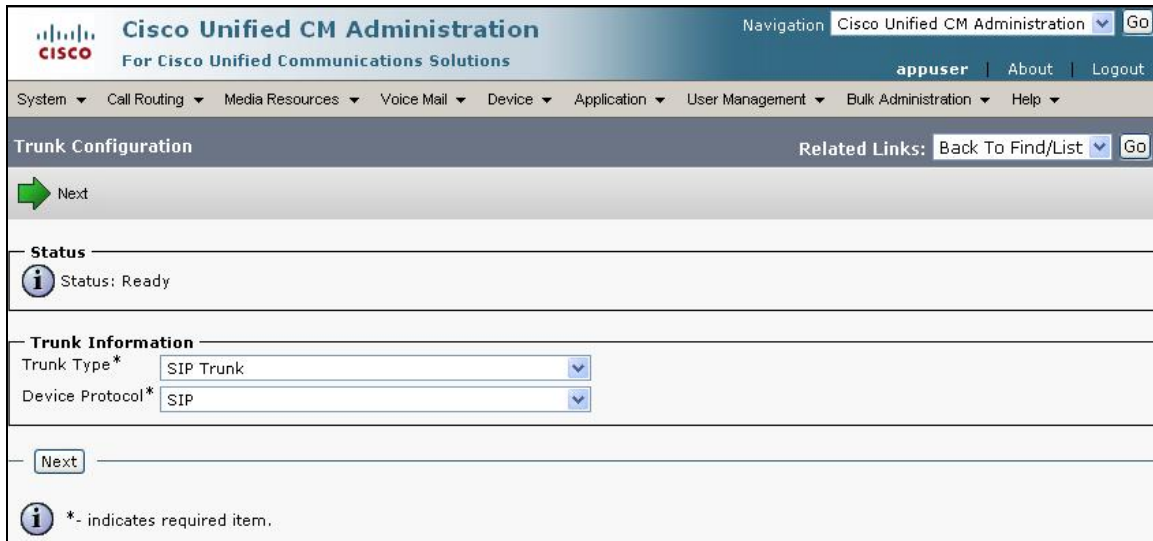
Scroll to the top of the screen, and select **Device** → **Trunk** as shown below.



The **Find and List Trunks** screen is displayed. Click **Add New** to add a new SIP Trunk.



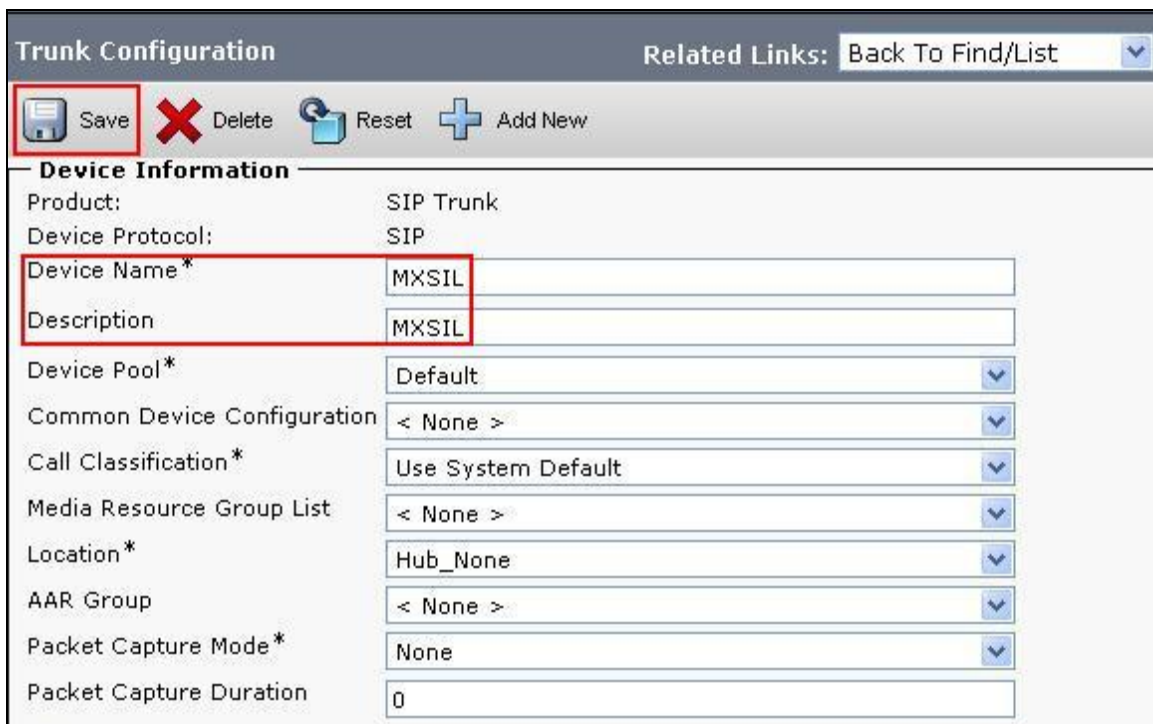
Select **SIP Trunk** as the **Trunk Type** and the **Device Protocol** field will automatically be changed to **SIP**. Click **Next** to continue.



The screenshot shows the 'Trunk Configuration' page in the Cisco Unified CM Administration interface. The page has a navigation bar at the top with the Cisco logo and 'Cisco Unified CM Administration' text. Below the navigation bar is a breadcrumb trail: System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Administration > Help. The main heading is 'Trunk Configuration'. To the right of the heading is a 'Related Links' section with a dropdown menu showing 'Back To Find/List' and a 'Go' button. Below the heading is a 'Next' button with a green arrow. The 'Status' section shows 'Status: Ready'. The 'Trunk Information' section contains two dropdown menus: 'Trunk Type*' set to 'SIP Trunk' and 'Device Protocol*' set to 'SIP'. At the bottom of the section is a 'Next' button. A note at the bottom left states: '* - indicates required item.'

The **SIP Trunk Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields. Click **Save** to commit the changes.

- **Device Name** An informative name
- **Description** Any note for this trunk



The screenshot shows the 'SIP Trunk Configuration' page in the Cisco Unified CM Administration interface. The page has a navigation bar at the top with the Cisco logo and 'Cisco Unified CM Administration' text. Below the navigation bar is a breadcrumb trail: System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Administration > Help. The main heading is 'Trunk Configuration'. To the right of the heading is a 'Related Links' section with a dropdown menu showing 'Back To Find/List' and a 'Go' button. Below the heading is a 'Save' button with a floppy disk icon, a 'Delete' button with a red X icon, a 'Reset' button with a circular arrow icon, and an 'Add New' button with a plus icon. The 'Device Information' section contains the following fields: 'Product:' set to 'SIP Trunk', 'Device Protocol:' set to 'SIP', 'Device Name*' set to 'MXSIL', 'Description' set to 'MXSIL', 'Device Pool*' set to 'Default', 'Common Device Configuration' set to '< None >', 'Call Classification*' set to 'Use System Default', 'Media Resource Group List' set to '< None >', 'Location*' set to 'Hub_None', 'AAR Group' set to '< None >', 'Packet Capture Mode*' set to 'None', and 'Packet Capture Duration' set to '0'.

Navigate to SIP Information section and enter following configuration:

- **Destination Address** IP address of the Avaya Meeting Exchange
- **Destination Port** Destination port number use for SIP Communications
- **SIP Trunk Security Profile** Profile configured at **Section 4.2**
- **DTMF Signaling Method** Select **RFC 2833**

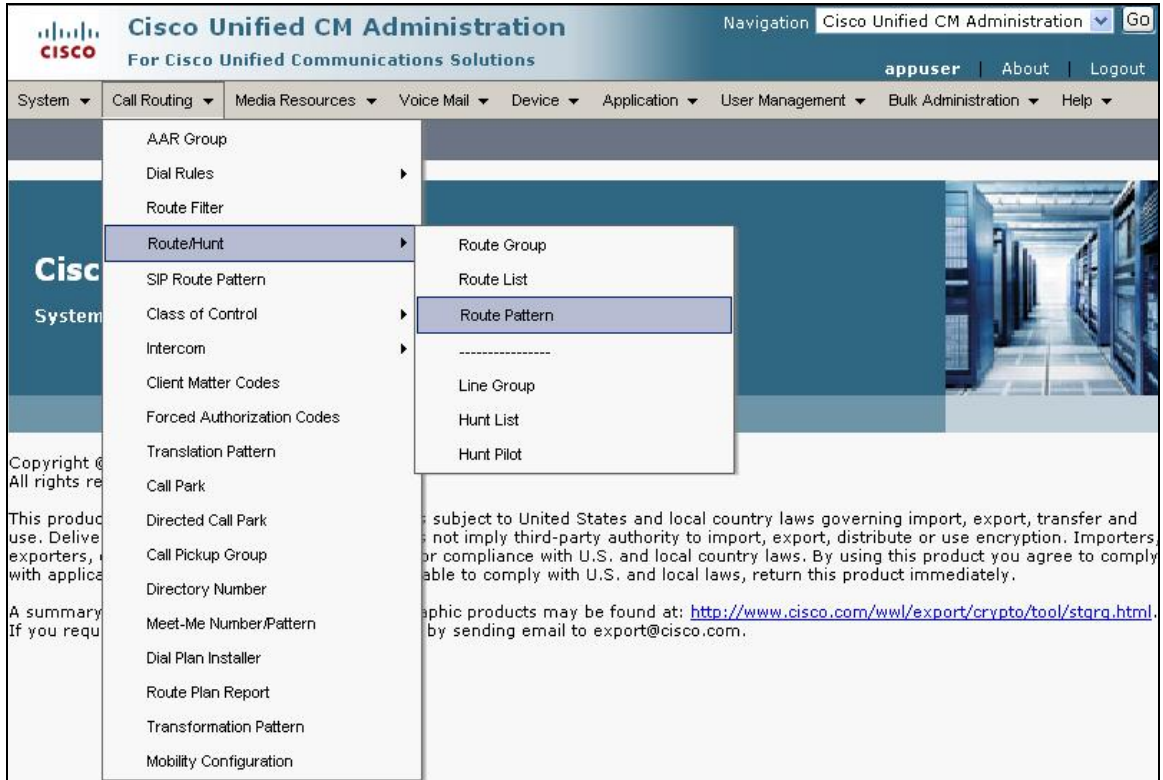
Click **Save** to commit the changes.

SIP Information	
Destination Address*	135.64.186.98
<input type="checkbox"/> Destination Address is an SRV	
Destination Port*	5060
MTP Preferred Originating Codec*	711u aw
Presence Group*	Standard Presence group
SIP Trunk Security Profile*	MXSIL
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	RFC 2833

Save **Delete** **Reset** **Add New**

4.4. Administer Route Pattern

Scroll to the top of the screen, and select **Call Routing** → **Route/Hunt** → **Route Pattern** as shown below.



The **Find and List Route Patterns** screen is displayed. Click **Add New** to add a new Route Pattern.

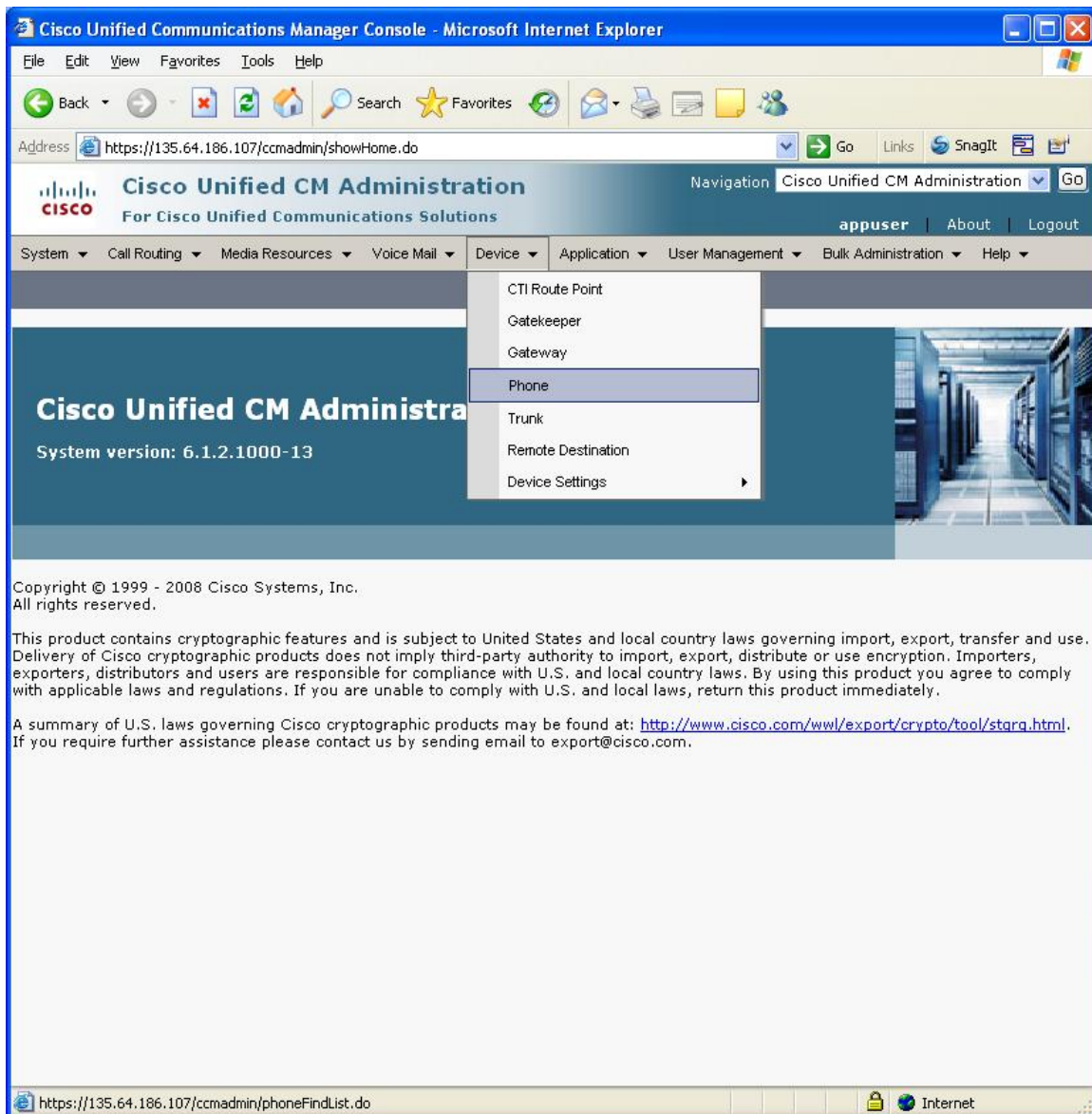
The following screen shows the route pattern used in the sample network. The route pattern **11111** will cause all 5 digit calls to be routed through the MX SIP Trunk defined in **Section 4.3**. Click **Save** to commit the changes (Not shown).

Click OK on the two subsequent pop up dialog boxes.

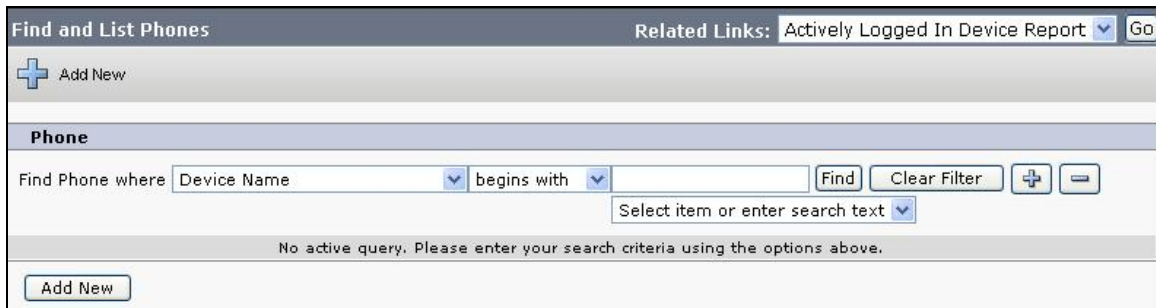


4.5. Administer Phone

Scroll to the top of the screen, and select **Device** → **Phone** as shown below.

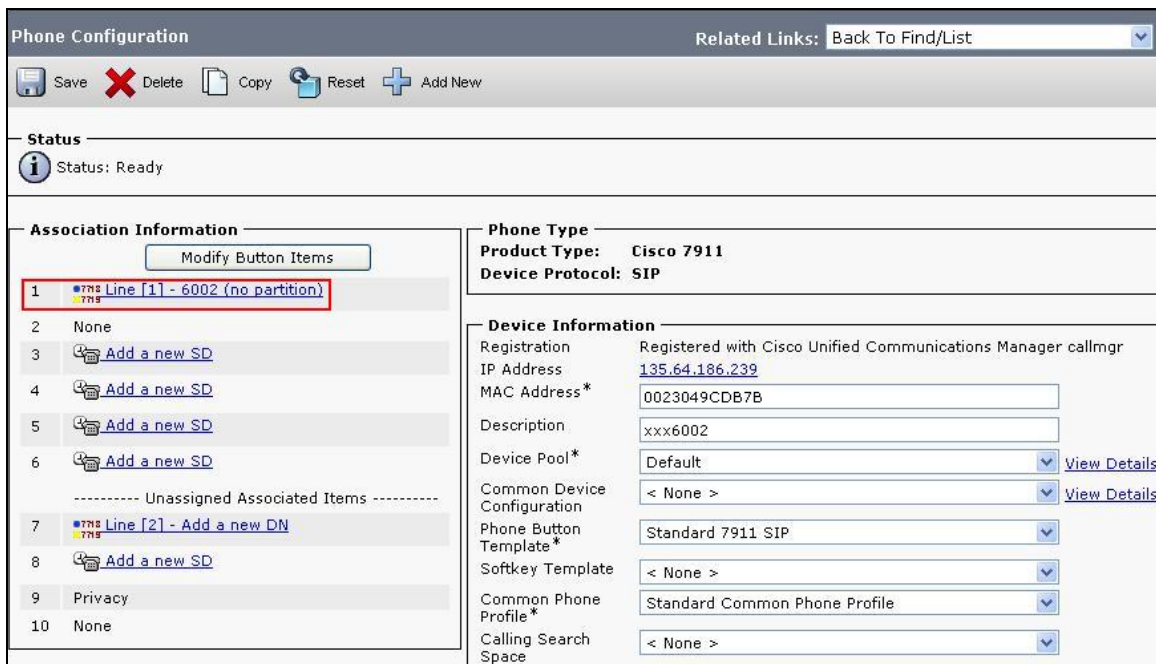


The **Find and List Phones** screen is displayed.



The 'Find and List Phones' screen features a header with the title and a 'Related Links' section containing 'Actively Logged In Device Report' and a 'Go' button. Below the header is an 'Add New' button. The main section is titled 'Phone' and contains a search area with a 'Find Phone where' dropdown set to 'Device Name', a 'begins with' dropdown, and a text input field. To the right of the input field are 'Find', 'Clear Filter', and '+'/'-' buttons. Below the search area is a message: 'No active query. Please enter your search criteria using the options above.' At the bottom is another 'Add New' button.

The following screen shows the display after a device has been selected. Click on the line for the device as highlighted in the screen below.



The 'Phone Configuration' screen has a header with the title and a 'Related Links' section with 'Back To Find/List'. Below the header is a toolbar with 'Save', 'Delete', 'Copy', 'Reset', and 'Add New' buttons. The main content is divided into two columns. The left column, titled 'Association Information', contains a list of 10 items. Item 1, 'Line [1] - 6002 (no partition)', is highlighted with a red box. Item 7, 'Line [2] - Add a new DN', is also highlighted. The right column, titled 'Phone Type', shows 'Product Type: Cisco 7911' and 'Device Protocol: SIP'. Below this is the 'Device Information' section, which includes fields for 'Registration' (Registered with Cisco Unified Communications Manager callmgr), 'IP Address' (135.64.186.239), 'MAC Address*' (0023049CDB7B), 'Description' (xxx6002), 'Device Pool*' (Default), 'Common Device Configuration' (< None >), 'Phone Button Template*' (Standard 7911 SIP), 'Softkey Template' (< None >), 'Common Phone Profile*' (Standard Common Phone Profile), and 'Calling Search Space' (< None >). Each field in the 'Device Information' section has a 'View Details' link.

The following screen shows the display after the line has been selected. Enter information for **Directory Number**, **Alerting Name** and **ASCII Alerting Name**.

Directory Number Configuration

Related Links: [Configure Device \(SEP0023049CDB7B\)](#)

Save

Delete

Reset

Add New

Status

Status: Ready

Directory Number Information

Directory Number*

6002

Route Partition

< None >

Description

Alerting Name

Cisco SIP

ASCII Alerting Name

Cisco SIP

☒ Allow Control of Device from CTI

Associated Devices

SEP0023049CDB7B

Edit Device

Edit Line Appearance

▼

▲

Dissociate Devices

Navigate to **Line 1 on Device** section and enter information for **Display (Internal Caller ID)** and **ASCII Display (Internal Caller ID)**. This will be displayed on the called party phone on all outgoing calls. Check all boxes in **Forwarded Call Information Display on Device** section. Click **Save** to complete.

Line 1 on Device SEP0023049CDB7B	
Display (Internal Caller ID)	Cisco SIP
Display text for a line appearance is intended for displaying text such as a name instead of a directory number for internal calls. If you specify a number, the person receiving a call may not see the proper identity of the caller.	
ASCII Display (Internal Caller ID)	Cisco SIP
Line Text Label	
ASCII Line Text Label	
External Phone Number Mask	
Visual Message Waiting Indicator Policy*	Use System Policy
Audible Message Waiting Indicator Policy*	Default
Ring Setting (Phone Idle)*	Ring
Ring Setting (Phone Active)	Use System Default
Applies to this line when any line on the phone has a call in progress.	
Call Pickup Group	Use System Default
Audio Alert Setting (Phone Active)	
Recording Option*	Call Recording Disabled
Recording Profile	< None >
Monitoring Calling Search Space	< None >
Multiple Call/Call Waiting Settings on Device SEP0023049CDB7B	
Note: The range to select the Max Number of calls is: 1-6	
Maximum Number of Calls*	4
Busy Trigger*	2 (Less than or equal to Max. Calls)
Forwarded Call Information Display on Device SEP0023049CDB7B	
<input checked="" type="checkbox"/> Caller Name	
<input checked="" type="checkbox"/> Caller Number	
<input checked="" type="checkbox"/> Redirected Number	
<input checked="" type="checkbox"/> Dialed Number	
Users Associated with Line	
Associate End Users	
<input type="button" value="Save"/> <input type="button" value="Delete"/> <input type="button" value="Reset"/> <input type="button" value="Add New"/>	

5. Verification Steps

The following steps were used to verify the administrative steps presented in these Application Notes and are applicable for similar configurations in the field. The verification steps in this section validated the following:

- The Avaya Meeting Exchange Enterprise S6200 Conferencing Server configuration
- Verify Cisco Unified Communications Manager

5.1. Avaya Meeting Exchange Enterprise S6200 Conferencing Server Processes

Verify all conferencing related processes are running on the Avaya Meeting Exchange Enterprise S6200 Conferencing Server as follows:

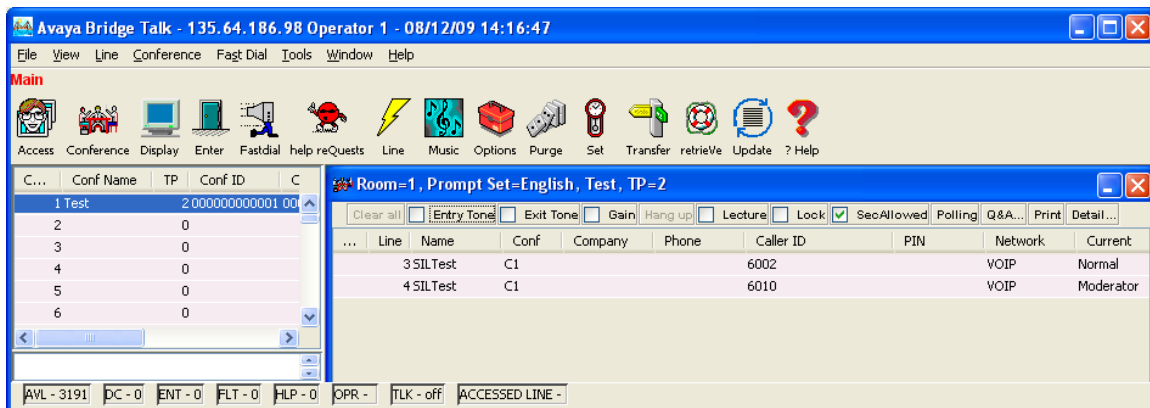
- Log in to the Meeting Exchange server console to access the CLI with the appropriate credentials.
- cd to **/usr/dcb/bin**
- At the command prompt, run the script **service mx-bridge status** and confirm all processes are running by verifying an associated Process ID (PID) for each process.

```
[sroot@MXSIL ~]# service mx-bridge status
5042 ?      00:00:01 initdcb
5604 ?      00:00:00 log
5607 ?      00:00:00 bridgeTranslato
5608 ?      00:00:00 netservices
5626 ?      00:00:00 timer
5627 ?      00:00:00 traffic
5628 ?      00:00:00 chdbased
5629 ?      00:00:00 startd
5630 ?      00:00:00 cdr
5631 ?      00:00:00 modapid
5632 ?      00:00:00 schapid
5633 ?      00:00:01 callhand
5634 ?      00:00:00 initipcb
5644 ?      00:00:00 sipagent
5645 ?      00:00:00 msdispatcher
5646 ?      00:00:00 serverComms
5648 ?      00:00:00 softms
5649 ?      00:00:00 softms
5650 ?      00:00:00 softms
5651 ?      00:00:00 softms
5652 ?      00:00:00 softms
5653 ?      00:00:00 softms
4022 ?      00:00:00 postmaster with 9 children
```

5.1.1. Verify Call Routing

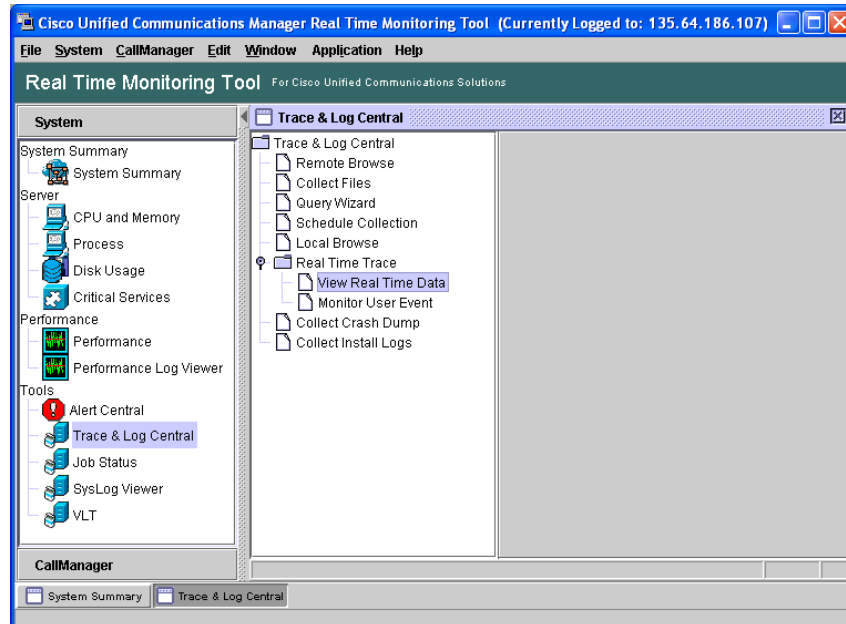
Verify end to end signalling/media connectivity between the Meeting Exchange and the Cisco Unified Communications Manager. This is accomplished by placing calls from the Cisco end points to the Meeting Exchange. This step utilizes the Avaya Bridge Talk application to verify calls to and from the Meeting Exchange are managed correctly, e.g., callers are added/removed from conferences. This step will also verify the conferencing applications provisioned.

- Configure a conference with Auto Blast enabled and provision a dial list. From an endpoint on the Public Switch Telephone Network, dial a number that corresponds to DNIS **11111** to enter a conference as **Moderator** (with passcode) and blast dial is invoked automatically. When answered these participants should enter the conference.
- If not already logged on, log in to the Avaya Bridge Talk application with the appropriate credentials
- **Double-Click on the** highlighted **Conf #** to open a **Conference Room** window
- Verify conference participants are added/removed from conferences by observing the Conference Navigator and/or Conference Room windows.



5.2. Verify Cisco Unified Communications Manager

The **Real Time Monitoring Tool** (RTMT) can be used to monitor events on Cisco Unified Communications Manager. This tool can be downloaded by selecting **Application → Plugins** from the top menu of the Cisco Unified Communications Manager Administration Web interface. For further information on this tool, please consult with **Reference 5**. The following screen shows where user can view and perform real time data capture.



5.3. Verified Scenarios

The following scenarios have been verified for the configuration described in these Application Notes.

- Place a call from the 7911G IP Telephone (SIP) and the Cisco 7911G IP Telephone (SCCP) to a scheduled conference on the Meeting Exchange.
- Ensure the welcome message is played from the Conferencing Bridge and there is audio between callers in the conference.
- Initiate dial out by dialling *1 on the phone's touch pad. You will be asked to enter the phone number you wish to dial. Enter the number and press 1 to make the call. When the callers answer dial *2 to return them to the main conference.

6. Conclusion

As illustrated in these Application Notes, Avaya Meeting Exchange Enterprise S6200 Conferencing Server can interoperate with Cisco Unified Communications Manager using SIP trunks. No verification of TLS was performed between Avaya Meeting Exchange Enterprise S6200 Conferencing Server and Cisco Unified Communications Manager.

The following interoperability items were observed during testing:

- SRTP is not supported in Cisco Unified CM 6.1.2.1000-13
- No outgoing audio from Cisco SIP phone with codec ILBC30
- G.726 is not supported by Call Manager in 6.1.2.1000-13

7. Additional References

Avaya Meeting Exchange references are available at <http://support.avaya.com>

[1] *Administering Meeting Exchange™ Servers, Release 5.2, 04-603419, Issue 1*

[2] *Using Meeting Exchange, Release 5.2, 04-603422, Issue 1*

Product documentation for Cisco Systems products may be found at <http://www.cisco.com>

[3] *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition, Release 6.0(1), Part Number: OL-15405-01*

[4] *Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communications Manager Business Edition, Release 6.0(1), Part Number: OL-15409-01*

[5] *Cisco Unified Real-Time Monitoring Tool Administration Guide, Release 7.0(1), Part Number: OL-14994-01*

©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Applications Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Lab at interoplabnotes@list.avaya.com