



**Avaya Solution & Interoperability Test Lab**

---

## **Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager, and Cisco Unified Communications Manager – Issue 1.0**

### **Abstract**

These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager and Cisco Unified Communications Manager using SIP trunks.

For the sample configuration, Avaya Aura™ Session Manager runs on an Avaya S8510 Server, Avaya Aura™ Communication Manager runs on an Avaya S8300 Server with Avaya G430 Media Gateway, and Cisco Unified Communications Manager runs on Cisco network appliance. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura™ Communication Manager.

## 1. Introduction

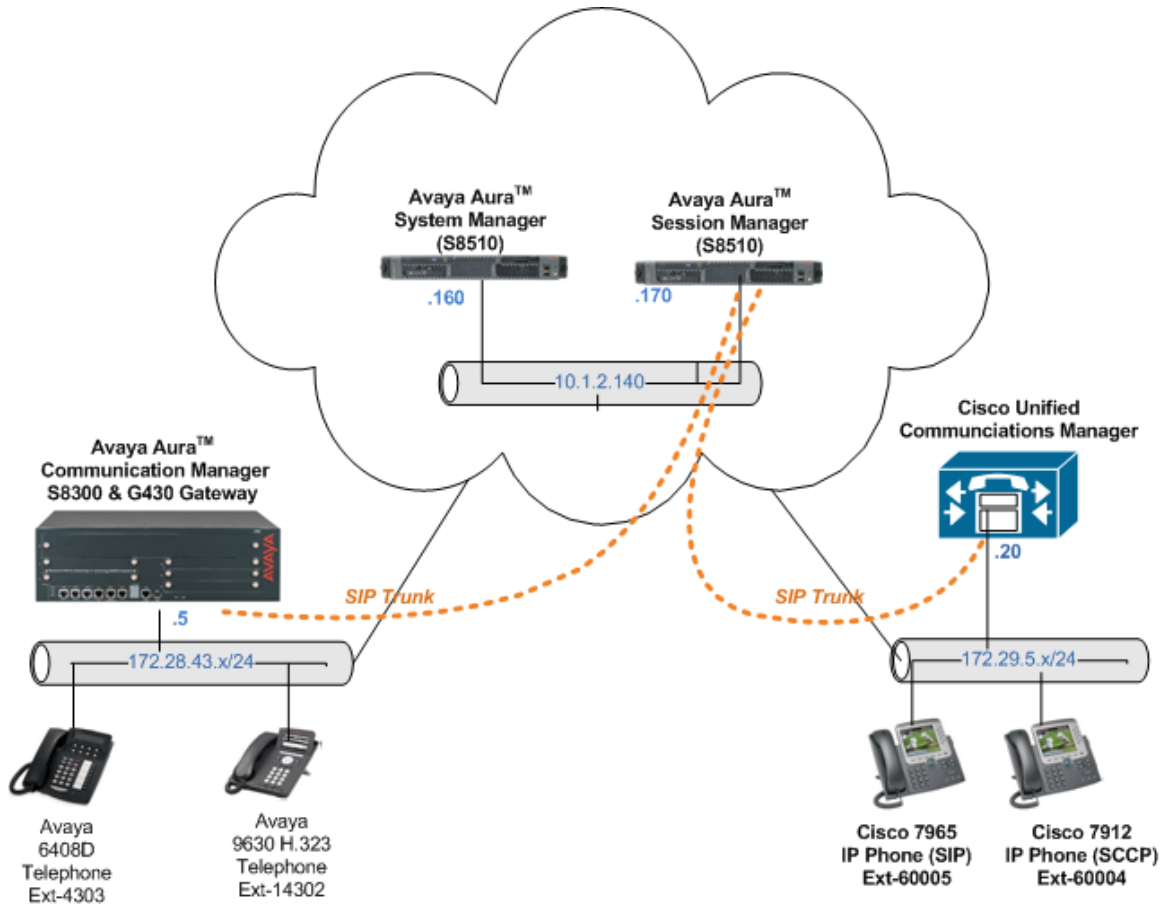
These Application Notes present a sample configuration for a network that uses Avaya Aura™ Session Manager to connect Avaya Aura™ Communication Manager and Cisco Unified Communications Manager (Cisco UCM) using SIP trunks.

## 2. Overview

The sample network is shown in **Figure 1**. Avaya Aura™ Communication Manager is supporting the Avaya 9630 IP Telephone (H.323) and 6408D+ Digital Telephone. The Cisco UCM supports the Cisco 7965 IP Telephone (SIP) and the Cisco 7912 IP Telephone (SCCP). SIP trunks are used to connect these two systems to Avaya Aura™ Session Manager. All inter-system calls are carried over these SIP trunks. Avaya Aura™ Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow for multi-vendor systems to interoperate. The Avaya Aura™ Session Manager is managed by a separate Avaya Aura™ System Manager, which can manage multiple Avaya Aura™ Session Managers.

### 3. Configuration

**Figure 1** illustrates the configuration used in these Application Notes. All telephones in the 172.28.10.0/24 IP network are either registered with Avaya Aura™ Communication Manager and uses extension 143xx. All IP telephones in the 172.29.5.0/24 IP network are registered with Cisco UCM and uses extension 60xxx. A single SIP trunk is provisioned from Avaya Aura™ Communication Manager and Cisco UCM to Avaya Aura™ Session Manager to manage call control for calls between the two systems.



**Figure 1: Sample Network Configuration**

## 4. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration:

DEVICE DESCRIPTION	VERSION TESTED
Avaya Aura™ Communication Manager - Running on an Avaya S8300 Server with an Avaya G430 Media Gateway	R 5.2 (R015x.02.0.947.3) SP0 (02.0.947.3-17250)
Avaya Aura™ System Manager - Running on an Avaya S8510 Server	1.0
Avaya Aura™ Session Manager - Running on an Avaya S8510 Server	1.1
Avaya 9630 IP Telephone (H.323)	3.0
Avaya 6402D Digital Telephone	-
Cisco Unified Communications Manager	7.0.1.1.11000-2 or 7.0.2.2000-5
Cisco 7965 Unified IP Phone (SIP)	SIP45.8-4-1S
Cisco 7912 Unified IP Phone (SCCP)	App Load ID CP7912080003SCCP070409A Boot Load ID LD0100BOOT021112A

## 5. Configure Avaya Aura™ Communication Manager

This section shows the configuration of Avaya Aura™ Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Avaya Aura™ Communication Manager, please consult with references [4] and [5]. The procedures include the following areas:

- Verify Avaya Aura™ Communication Manager license
- Administer system parameters features
- Administer IP nodes names
- Administer IP interface
- Administer IP codec set and network region
- Administer SIP trunk group and signaling group
- Administer SIP trunk group members and router patterns
- Administer location and public unknown numbering
- Administer uniform dial plan and AAR analysis

1. Use the “display system-parameter customer options” command to verify whether the **Maximum Administered SIP Trunks** field value with the corresponding value in the USED column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

```

display system-parameters customer-options                               Page 2 of 10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 50                          6
      Maximum Concurrently Registered IP Stations: 450                1
      Maximum Administered Remote Office Trunks: 450                 0
Maximum Concurrently Registered Remote Office Stations: 450         0
      Maximum Concurrently Registered IP eCons: 0                    0
      Max Concur Registered Unauthenticated H.323 Stations: 0        0
      Maximum Video Capable Stations: 100                           0
      Maximum Video Capable IP Softphones: 100                       0
      Maximum Administered SIP Trunks: 100                          20

```

2. Use the “change system-parameters features” command to allow for trunk-to-trunk transfers.

This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis.

Note: This feature poses significant security risk, and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels.

```

change system-parameters features                                     Page 1 of 18
                                FEATURE-RELATED SYSTEM PARAMETERS
                                Self Station Display Enabled? n
                                Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
      Music/Tone on Hold: music Type: ext 14383
      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attd
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred

```

- Use the “change node-names ip” command to add entries for the “procr” and Avaya Aura™ Communication Manager that will be used for connectivity. In the sample network, “procr” and “172.28.43.5” are entered as Name and IP Address for the Avaya Aura™ Communication Manager running on the Avaya S8300 Server. In addition, “ASM” and “10.1.2.170” are entered for Avaya Aura™ Session Manager.

```
change node-names ip                                     Page 1 of 2
                                     IP NODE NAMES
Name                                IP Address
ASM                                10.1.2.170
default                              0.0.0.0
msgserver                             172.28.43.9
procr                              172.28.43.5
```

- Use the “change ip-network-region n” command, where “n” is the network region number to configure the network region being used. In the sample network ip-network-region 1 is used. For the Authoritative Domain field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec-Set** to 1 to use ip-codec-set 1.

```
change ip-network-region 1                             Page 1 of 19
                                     IP NETWORK REGION
Region: 1
Location: Authoritative Domain: avaya.com
Name: ASM-to-Cisco
MEDIA PARAMETERS                                     Intra-region IP-IP Direct Audio: yes
Codec Set: 1                                       Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                   IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                             RTCP Reporting Enabled? y
Call Control PHB Value: 46                           RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46                                  Use Default Server Parameters? y
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

- Use the “change ip-codec-set n” command, where “n” is the existing codec set number to configure the desired audio codec.

**Note:** In addition to the “G.711MU” codec shown below, “G.729” and “G.729AB” have also been verified to be interoperable with Cisco UCM via SIP trunks.

```
change ip-codec-set 1 Page 1 of 2

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU      n            2          20
2:
```

- In the test configuration, signal group 25 along with trunk group 25 were used to reach Avaya Aura™ Session Manager. Use the “add signaling-group n” command, where “n” is the signaling-group number being added to the system. The “Far-end Domain” is left blank so that the signaling group accepts any authoritative domain.

```
SIGNALING GROUP

Group Number: 25                Group Type: sip
                                Transport Method: tls

IMS Enabled? n
IP Video? n

Near-end Node Name: procr       Far-end Node Name: ASM
Near-end Listen Port: 5061     Far-end Listen Port: 5061
                                Far-end Network Region: 1

Far-end Domain:

                                Bypass If IP Threshold Exceeded? n

DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3  IP Audio Hairpinning? n
Enable Layer 3 Test? n        Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n  Alternate Route Timer(sec): 6
```

- Use the “add trunk-group n” command, where “n” is the new trunk group number being added to the system.

The following screens show the settings used for trunk group 25.

```
Add trunk-group 25 Page 1 of 21

                                TRUNK GROUP

Group Number: 25                Group Type: sip                CDR Reports: y
Group Name: To-ASM              COR: 1                        TN: 1                    TAC: 125
Direction: two-way              Outgoing Display? n
Dial Access? n                  Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n

                                Signaling Group: 25
                                Number of Members: 10
```

```

add trunk-group 25                                     Page 3 of 21
                                     TRUNK FEATURES
      ACA Assignment? n                Measured: none
                                     Maintenance Tests? y

      Numbering Format: public
                                     UUI Treatment: service-provider
                                     Replace Restricted Numbers? y
                                     Replace Unavailable Numbers? y

      Show ANSWERED BY on Display? Y

```

```

add trunk-group 25                                     Page 4 of 21
                                     PROTOCOL VARIATIONS

      Mark Users as Phone? n
      Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
      Network Call Redirection? n
      Send Diversion Header? n
      Support Request History? y
      Telephone Event Payload Type: 101

```

- Use the “change public-unknown-numbering” command to define the calling party number to be sent out to through the SIP trunk. Add an entry for the trunk group defined in **Step 7**. In the sample network configuration below, all calls originating from a 5-digit extension beginning with 143 and routed to trunk group 25 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

```

change public-unknown-numbering 0                     Page 1 of 2
                                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                     Total
Ext  Ext      Trk      CPN      CPN
Len  Code     Grp(s)  Prefix  Len
-----
5    143       25      5
                                     Total Administered: 3
                                     Maximum Entries: 240

```

- Configure the dial plan for dialing 5-digit extensions beginning with “60” to stations registered with Cisco UCM. Use the “change dialplan analysis” command to define dialed string 60 as an aar call type.

```

change dialplan analysis                             Page 1 of 12
                                     DIAL PLAN ANALYSIS TABLE
                                     Location: all          Percent Full: 2

      Dialed  Total  Call  Dialed  Total  Call  Dialed  Total  Call
      String  Length Type  String  Length Type  String  Length Type
      -----
      1        3     dac
      143      5     ext
      60      5     aar
      8        1     fac
      9        1     fac
      *        3     fac
      #        3     fac

```

10. Use the “change aar analysis n” command where “n” is the dial string pattern to configure an aar entry for Dialed String 60 to use Route Pattern 25.

```
change aar analysis 60                                     Page 1 of 2
AAR DIGIT ANALYSIS TABLE
Location: all                                           Percent Full: 2
Dialed      Total      Route      Call      Node      ANI
String      Min  Max  Pattern  Type      Num      Reqd
60          5   5   25      aar       n        n
7           7   7   254     aar       n        n
8           7   7   254     aar       n        n
9           7   7   254     aar       n        n
```

11. Configure a route pattern to correspond to the newly added SIP trunk group. Use the “change route-pattern n” command, where “n” is the route pattern number specified in Step 10. Configure this route pattern to route calls to trunk group number 25 configured in Step 7.

```
change route-pattern 25                                   Page 1 of 3
Pattern Number: 25  Pattern Name: To-ASM
SCCAN? n           Secure SIP? n
Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/ IXC
No   Mrk Lmt List Del  Digits      QSIG
1: 25  0                                     n   user
2:                                     n   user
3:                                     n   user
BCC VALUE  TSC CA-TSC  ITC BCIE Service/Feature PARM No. Numbering LAR
0 1 2 M 4 W      Request      Dgts Format
1: y y y y y n  n          rest
2: y y y y y n  n          rest
```

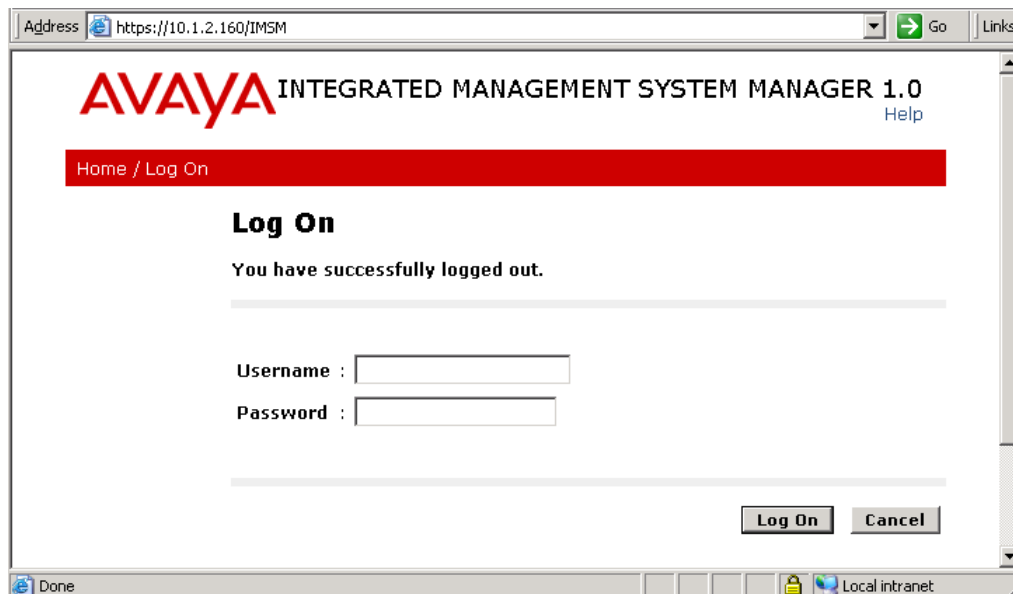
12. Use the “save translation” command to save all changes.

```
save translation
SAVE TRANSLATION
Command Completion Status      Error Code
Success                        0
```

## 6. Configuring Avaya Aura™ Session Manager

This section provides the procedures for configuring Avaya Aura™ Session Manager. For further information on Avaya Aura™ Communication Manager, please consult with references [1], [2], and [3]. The procedures include the following areas:

- SIP domain
  - Adaptations
  - SIP Entities corresponding to the SIP telephony systems and Avaya Aura™ Session Manager
  - Entity Links, which define the SIP trunk parameters used by Avaya Aura™ Session Manager when routing calls to/from SIP Entities
  - Time Ranges during which routing policies are active
  - Routing Policies, which control call routing between the SIP Entities
  - Dial Patterns, which govern how a call is routed
  - Avaya Aura™ Session Manager, corresponding to the Avaya Aura™ Session Manager Server to be managed by Avaya Aura™ System Manager
1. Access the Avaya Aura™ System Manager using a Web Browser and entering <http://<ip-address>/IMSM>, where <ip-address> is the IP address of Avaya Aura™ System Manager. Log in using appropriate credentials and accept the subsequence Copyright Legal Notice.



2. Begin configuration by selecting **Network Routing Policy** from the left panel menu. A short procedure for configuring Network Routing Policy is shown on the right panel.

Home / Network Routing Policy

- ▶ Asset Management
- ▶ User Management
- ▶ Monitoring
- ▼ Network Routing Policy
  - Adaptations
  - Dial Patterns
  - Entity Links
  - Locations
  - Regular Expressions
  - Routing Policies
  - SIP Domains
  - SIP Entities
  - Time Ranges
  - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

**Shortcuts**

- [Change Password](#)
- [Landing Page](#)
- [Import All Data field descriptions](#)
- [Export All Data field descriptions](#)
- [Saving Committing Synchronizing configuration changes](#)

### Welcome to the Network Routing Policy Application

AIM System Manager contains several NRP applications like "SIP Domains", "Locations", "SIP Entities", etc.

The recommended order to use the NRP applications (that means the overall NRP workflow) to configure the customer network configuration is as follows:

- Step 1: Create "SIP Domains"
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
  - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
  - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
  - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "EntityLinks"
  - Between Session Managers
  - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
  - Matching to the tariff information got from the Service Providers
- Step 7: Create "Routing Policies"
  - Assign the appropriate "Routing Destination" and "Time Of Day" (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 8: Create "Dial Pattern"
  - Assign the appropriate "Locations" and "Routing Policies" to the "Dial Pattern"
- Step 9: Create "Regular Expressions"
  - Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

**IMPORTANT:** the appropriate dial pattern are defined and assigned afterwards with the help of NRP application "Dial pattern". That's why this overall NRP workflow can be interpreted as

### "Dial Pattern driven approach to define routing policies"

That means (with regard to steps listed above):

- Step 7: "Routing Polices" are defined
- Step 8: "Dial Pattern" are defined and assigned to "Routing Policies" and "Locations" (one step)
- Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

3. Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting SIP Domains on the left panel menu and clicking the **New** button (not shown) to create a new SIP domain entry. The following screen will be shown after clicking **New**. Click **Commit** to save changes.

**Name** The authoritative domain name (e.g., “avaya.com”)  
**Notes** Description for the domain (optional)

Note: Since the sample network does not deal with any foreign domains, no additional SIP Domains entry is needed.

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The header includes the Avaya logo, the text "INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0", and a welcome message for user "admin" last logged on at Apr. 23, 2009 16:31 PM. A navigation menu on the left lists various system management options, with "SIP Domains" highlighted in a red box. The main content area is titled "SIP Domains" and contains a table with one entry: "avaya.com". A red box highlights the "Commit" button at the bottom right of the page. A message "\* Input Required" is displayed at the bottom left.

4. Create 2 Adaptations entry. One for incoming call from Avaya Aura™ Communication Manager, and the other for incoming call from Cisco UCM.

For the Avaya Aura™ Communication Manager adaptation, enter the following information.

**Name** An informative name for the adaptation (e.g., Avaya-G430)

**Adaptation Module** Enter “DigitConversionAdapter avaya.com”

**Digit Conversion for incoming Calls**

Matching Pattern 143 with a minimum and maximum of 5 digits long, which is the dial pattern for station registered with Avaya Aura™ Communication Manager.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Apr. 23, 2009 16:31 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Adaptations / **Adaptation Details**

**Adaptation Details** [Commit](#) [Cancel](#)

**General**

Name	Adaptation Module	Egress URI Parameters	Notes
• Avaya-430	DigitConversionAdapter avaya.com		

**Digit Conversion for Incoming Calls**

[Add](#) [Remove](#)

1 Item | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	N
<input type="checkbox"/>	• 143	• 5	• 5	• 0		both ▼	

Select: All, None ( 0 of 1 Selected )

**Digit Conversion for Outgoing Calls**

[Add](#) [Remove](#)

0 Items | [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--------------------------	------------------	-----	-----	---------------	---------------	-------------------	-------

\* Input Required [Commit](#) [Cancel](#)

**Shortcuts**

- Change Password
- Adaptation Details field descriptions
- Saving Committing Synchronizing configuration changes

For the Cisco UCM adaptation, enter the following information.

- Name** CiscoUCM-7, an informative name for the adaptation
- Adaptation Module** Enter "CiscoAdapter avaya.com"
- Digit Conversion for incoming Calls**  
Matching Patterns 60 with a minimum and maximum of 5 digits long, which is the dial pattern for station registered with Cisco UCM.



Home / Network Routing Policy / Adaptations / Adaptation Details

- ▶ Asset Management
- ▶ User Management
- ▶ Monitoring
- ▼ Network Routing Policy
  - Adaptations
  - Dial Patterns
  - Entity Links
  - Locations
  - Regular Expressions
  - Routing Policies
  - SIP Domains
  - SIP Entities
  - Time Ranges
  - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

### Adaptation Details

#### General

Name	Adaptation Module	Egress URI Parameters	Note
CiscoUCM-7	CiscoAdapter avaya.com		

#### Digit Conversion for Incoming Calls

1 Item Refresh Filter: Enable

	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	
<input type="checkbox"/>	*60	*5	*5	*0		both	N

Select: All, None ( 0 of 1 Selected )

#### Digit Conversion for Outgoing Calls

1 Item Refresh Filter: Enable

	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	
<input type="checkbox"/>	*143	*5	*5	*0		both	N

Select: All, None ( 0 of 1 Selected )

- A SIP Entity must be added for Avaya Aura™ Session Manager for each SIP-based telephony system supported by a SIP Trunk. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown) on the right. Enter the following for each SIP Entity.

Under General:

**Name** An informative name (e.g., SM1)  
**FQDN or IP Address** IP address of the ASM or the signaling interface on the telephony system  
**Type** "Session Manager" for Avaya Aura™ Session Manager, "CM" for Avaya Aura™ Communication Manager, or "Other" for Cisco UCM  
**Time Zone** Time zone for this location

Under Port, click **Add**, and then edit the fields in the resulting new row

**Port** Port number on which the system listens for SIP requests  
**Protocol** Transport protocol to be used to send SIP requests

The following screen shows the SIP Entity for Avaya Aura™ Session Manager after clicking New.

The screenshot displays the Avaya Integrated Management System (IMS) interface. At the top, the Avaya logo is on the left, and the text 'INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0' is in the center. On the right, it says 'Welcome, admin Last Logged on at Apr. 23, 2009 16:31 PM' and 'Help | Log off'.

The main navigation bar shows 'Home / Network Routing Policy / SIP Entities / SIP Entity Details'. A sidebar on the left contains a tree view with 'SIP Entities' highlighted in red. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons.

The 'General' section contains a table with the following data:

Name	FQDN or IP Address	Type	Notes
SM1	10.1.2.170	Session Manager	

Below the table are several configuration fields, some of which are highlighted with red boxes:

- Entity Links**: Adaptation (dropdown), Location (Lincroft dropdown), Outbound Proxy (dropdown), Time Zone (America/New\_York dropdown).
- Override Port & Transport with DNS SRV**:
- SIP Timer B/F (secs)**: \* 4
- Credential name**: (text input)

The 'Monitoring' section has 'Monitoring on/off' set to 'Use Session Manager configuration'.

The 'Port' section has 'Add' and 'Remove' buttons. Below is a table with 2 items:

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	

At the bottom, it says 'Select: All, None ( 0 of 2 Selected )'.

The following screen shows the SIP Entity for Avaya Aura™ Communication Manager.



Home / Network Routing Policy / SIP Entities / SIP Entity Details

- ▶ Asset Management
- ▶ User Management
- ▶ Monitoring
- ▼ Network Routing Policy
  - Adaptations
  - Dial Patterns
  - Entity Links
  - Locations
  - Regular Expressions
  - Routing Policies
  - SIP Domains
  - SIP Entities**
  - Time Ranges
  - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

- Shortcuts**
- [Change Password](#)
  - [SIP Entity Details field descriptions](#)
  - [Saving Committing Synchronizing configuration changes](#)

## SIP Entity Details

### General

Name	FQDN or IP Address	Type	Notes
• Avaya-G430	• 172.28.43.5	CM	To Inte

### Entity Links

**Adaptation:** Avaya-430

**Location:**

**Time Zone:** America/New\_York

**Override Port & Transport with DNS SRV:**

**SIP Timer B/F (secs):** \* 4

**Credential name:**

**Call Detail Recording:** egress

### Monitoring

**Monitoring on/off:** Use Session Manager configuration

\* Input Required

The following screen shows the SIP Entity for Cisco UCM.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Apr. 30, 2009 18:21 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / SIP Entities / SIP Entity Details

**SIP Entity Details** Commit Cancel

**General**

Name	FQDN or IP Address	Type	Notes
* CiscoUCM-7	* 172.29.5.20	Other	To Interop CUCM

**Entity Links**

**Adaptation:** CiscoUCM-7

**Location:**

**Time Zone:** America/New\_York

**Override Port & Transport with DNS SRV:**

**SIP Timer B/F (secs):** \* 4

**Credential name:**

**Call Detail Recording:** egress

**Monitoring**

**Monitoring on/off:** Use Session Manager configuration

\* Input Required Commit Cancel

6. A SIP trunk between Avaya Aura™ Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed.

<b>Name</b>	An informative name
<b>SIP Entity 1</b>	Select SM1
<b>Port</b>	Port number to which the other system sends its SIP requests
<b>SIP Entity 2</b>	The other SIP Entity for this link, created in <b>Step 5</b>
<b>Port</b>	Port number to which the other system expects to receive SIP requests
<b>Trusted</b>	Whether to trust the other system
<b>Protocol</b>	Transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in the sample network.

AVAYA INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at May. 01, 2009 10:47 AM

Help | Log off

Home / Network Routing Policy / Entity Links

**Entity Links**

Edit New Duplicate Delete More Actions Commit

2 Items Refresh Filter: Enable

<input type="checkbox"/>	State	Name	SIP Entity 1	Port	SIP Entity 2	Port	Trusted	Protocol	Notes
<input type="checkbox"/>	Sync	<a href="#">Avaya-G430</a>	SM1	5061	Avaya-G430	5061	<input checked="" type="checkbox"/>	TLS	
<input type="checkbox"/>	Sync	<a href="#">CiscoUCM7</a>	SM1	5060	CiscoUCM-7	5060	<input checked="" type="checkbox"/>	TCP	

Select: All, None ( 0 of 2 Selected )

- Before adding routing policies (see next step), time ranges must be defined during which the policies will be active. In the sample network, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges** from the left panel menu and then click New on the right. Fill in the following fields.

**Name** An informative name (e.g. “Anytime”)  
**Mo through Su** Check the box under each day of the week for inclusion  
**Start Time** Enter start time (e.g. “00:00” for start of day)  
**End Time** Enter end time (e.g. “23:59” for end of day)

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The left sidebar contains a menu with 'Time Ranges' highlighted. The main content area is titled 'Time Ranges' and shows a table with one entry. The table has columns for 'State', 'Name', 'Mo', 'Tu', 'We', 'Th', 'Fr', 'Sa', 'Su', 'Start Time', 'End Time', and 'Notes'. The entry is 'Sync' with the name 'Anytime' and has checkboxes checked for all days of the week. The start time is '00:00' and the end time is '23:59'. There are buttons for 'Edit', 'New', 'Duplicate', 'Delete', 'More Actions', and 'Commit' at the top of the table area.

State	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
Sync	Anytime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

- Create routing policies to direct how calls will be routed to a system. Two routing policies must be added; one for Avaya Aura™ Communication Manager and one for Cisco UCM. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown) on the right.

**Under General**

Enter an informative name

**Under SIP Entity as Destination**

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

**Under Time of Day**

Click **Add**, and then select the time range configured in the previous step.

The following is screen shows the Routing Policy for Avaya Aura™ Communication Manager.



Home / Network Routing Policy / Routing Policies / Routing Policy Details

- ▶ Asset Management
  - ▶ User Management
  - ▶ Monitoring
  - ▼ Network Routing Policy
    - Adaptations
    - Dial Patterns
    - Entity Links
    - Locations
    - Regular Expressions
    - Routing Policies**
    - SIP Domains
    - SIP Entities
    - Time Ranges
    - Personal Settings
  - ▶ Security
  - ▶ Applications
  - ▶ Settings
  - ▶ Session Manager
- 
- Shortcuts**
- Change Password
  - Routing Policy Details field descriptions
  - SIP Entity List field descriptions
  - Time Range List field descriptions
  - Pattern List field descriptions
  - Regular Expressions List field descriptions
  - Saving Committing Synchronizing configuration changes

## Routing Policy Details

### General

Name	Disabled	Notes
• To Interop G430 (143xx)	<input type="checkbox"/>	

### SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Avaya-G430	172.28.43.5	CM	To Interop G430

### Time of Day

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time
<input type="checkbox"/>	0	Anytime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59

Select: All, None ( 0 of 1 Selected )

### Dial Patterns

0 Item | Refresh Filter: Enable

<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	-----------	-----	-----	----------------	------------	----------------------	-------

### Regular Expressions

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

The following is screen shows the Routing Policy for Cisco UCM.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Apr. 23, 2009 16:31 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Routing Policies / Routing Policy Details

**Routing Policy Details** Commit Cancel

**General**

Name	Disabled	Notes
To Interop CUCM (60xxx)	<input type="checkbox"/>	

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CiscoUCM-7	172.29.5.20	Other	To Interop CUCM

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time
<input type="checkbox"/>	0	Anytime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59

Select: All, None ( 0 of 1 Selected )

**Dial Patterns**

Add Remove

0 Item Refresh Filter: Enable

<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	-----------	-----	-----	----------------	------------	----------------------	-------

**Regular Expressions**

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

**Shortcuts**

- Change Password
- Routing Policy Details field descriptions
- SIP Entity List field descriptions
- Time Range List field descriptions
- Pattern List field descriptions
- Regular Expressions List field descriptions
- Saving Committing Synchronizing configuration changes

9. A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, 5-digit extension beginning with “143” reside on Avaya Aura™ Communication Manager, and 5-digit extension beginning with “60” reside on Cisco UCM. To add a dial pattern, select Dial Patterns on the left panel menu, and then click on the **New** button on the right (not shown).

Under General

<b>Pattern</b>	Dialed number or prefix
<b>Min</b>	Minimum length of dialed number
<b>Max</b>	Maximum length of dialed number
<b>Notes</b>	Comment on purpose of dial pattern

The following screen shows the dial pattern to Avaya Aura™ Communication Manager.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0 Welcome, admin Last Logged on at Apr. 23, 2009 16:31 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / Dial Pattern Details

**Dial Pattern Details** Commit Cancel

**General**

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
* 143	* 5	* 5	<input type="checkbox"/>	avaya.com	To interop G430

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To Interop G430 (143xx)	<input type="checkbox"/>	Avaya-G430	

Select: All, None ( 0 of 1 Selected )

**Denied Originating Locations**

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

\* Input Required Commit Cancel

The following screen shows the dial pattern to Cisco UCM.

The screenshot displays the Avaya Integrated Management System Manager 1.0 interface. The main content area is titled "Dial Pattern Details" and includes a "General" section with a table of dial patterns. A red box highlights the first row of this table, which contains the following data:

Pattern	Min	Max	Emergency Call	SIP Domain	Notes
60	5	5	<input type="checkbox"/>	avaya.com	To interop CUCM7

Below the "General" section is the "Originating Locations and Routing Policies" section, which contains a table with one item. A red box highlights this table:

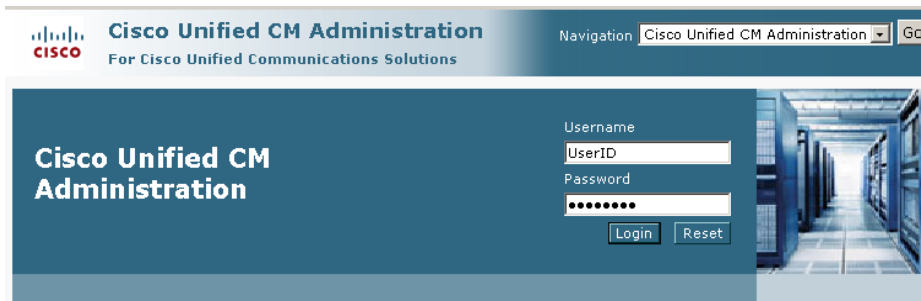
<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To Interop CUCM (60xxx)	<input type="checkbox"/>	CiscoUCM-7	

At the bottom right of the configuration page, there is a red box around the "Commit" button. A message "\* Input Required" is displayed above the buttons.

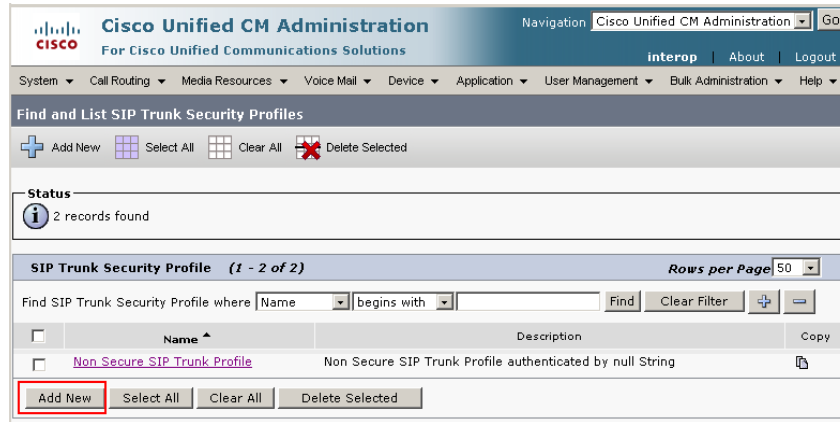
## 7. Configure Cisco UCM

This section provides the procedures for configuring Cisco UCM. The procedures include configuration of the following items. These Application Notes assumed that the basic configuration needed to support Cisco IP telephones has been completed. For further information on Cisco UCM, please consult references [6] and [7].

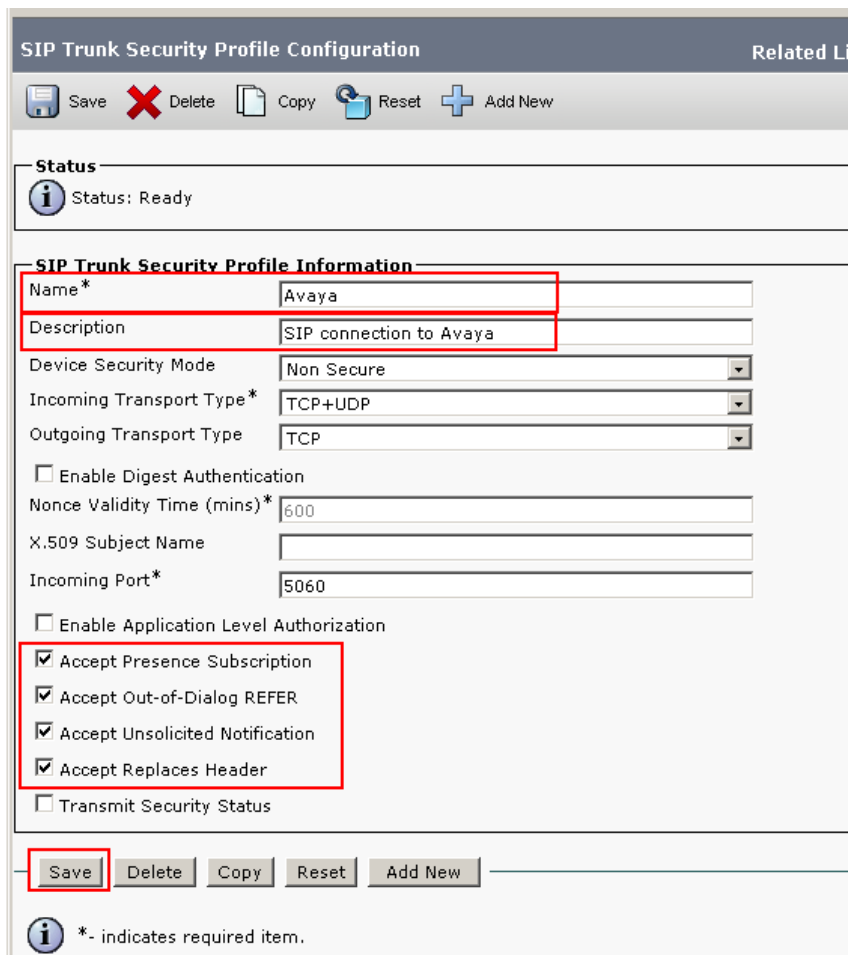
1. Open Cisco Unified CM Administration by entering the IP address of the CUCM into the Web Browser address field, and log in using an appropriate Username and Password.



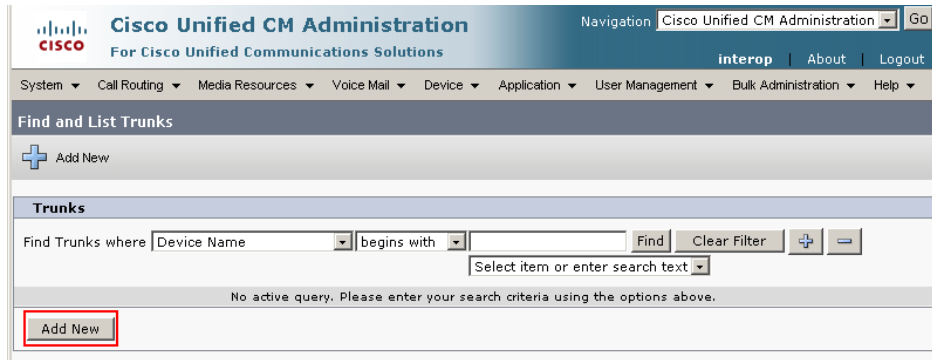
2. Select **System** → **Security Profile** → **SIP Trunk Security Profile** from the top menu then click **Add New** to add a new SIP Trunk Security Profile.



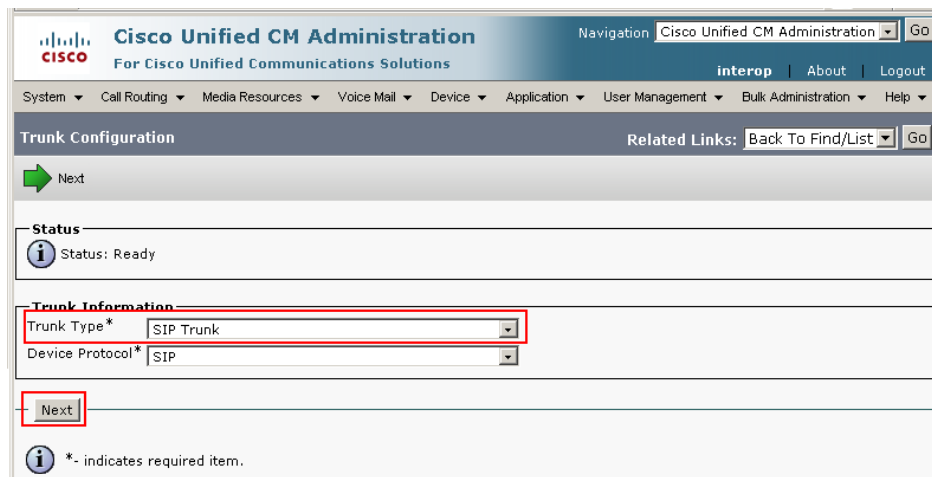
The following is a screen capture of the SIP Trunk Security Profile used in the sample network. Configure the highlighted areas and click **Save** to commit the changes.



3. Add a new SIP trunk by selecting **Device** → **Trunk** from the top menu then click **Add New** to begin adding a new SIP trunk.



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



Enter the appropriate information for the SIP Trunk. The following screen shows the configuration used in the sample network. Click **Save** to complete.

<b>Device Name</b>	An informative name
<b>Description</b>	Any note for this trunk
<b>Remote-Party-Id</b>	checked to send
<b>Asserted-Identity</b>	Checked to send caller information
<b>Asserted-Type</b>	Select “ <b>PAI</b> ” for P-Asserted-Identity
<b>Destination Address</b>	IP address of Avaya Aura™ Session Manager
<b>Destination Port</b>	Destination port number use for SIP communication
<b>SIP Trunk Sec. Profile</b>	Profile configured at <b>Step 2</b>
<b>DTMF Signaling Method</b>	Select “ <b>RFC 2833</b> ”

The screenshot displays the Cisco Unified CM Administration interface for configuring a SIP Trunk. The page title is "Cisco Unified CM Administration" and the navigation menu includes "Cisco Unified CM Administration". The main menu includes "System", "Call Routing", "Media Resources", "Voice Mail", "Device", "Application", "User Management", and "Bulk Admin". The current page is "Trunk Configuration" with a "Related Links" section containing "Back To Find/List".

The configuration form includes the following sections:

- Status:** Status: Ready
- Device Information:**
  - Product: SIP Trunk
  - Device Protocol: SIP
  - Device Name\*: ASM-interop
  - Description: To Avaya ASM
  - Device Pool\*: Default
  - Common Device Configuration: < None >
  - Call Classification\*: Use System Default
  - Media Resource Group List: < None >
  - Location\*: Hub\_None
  - AAR Group: < None >
  - Packet Capture Mode\*: None
  - Packet Capture Duration: 0
  - Media Termination Point Required
  - Retry Video Call as Audio
  - Transmit UTF-8 for Calling Party Name
  - Unattended Port
  - SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
  - Use Trusted Relay Point\*: Default
- Incoming Calling Party Settings:**
  - If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.
  - Buttons: Clear Prefix Settings, Default Prefix Settings
  - Incoming Calling Party Unknown Number Prefix: Default

**Multilevel Precedence and Preemption (MLPP) Information**  
 MLPP Domain

---

**Call Routing Information**

Remote-Party-Id  
 Asserted-Identity  
 Asserted-Type\*   
 SIP Privacy\*

**Inbound Calls**

Significant Digits\*   
 Connected Line ID Presentation\*   
 Connected Name Presentation\*   
 Calling Search Space   
 AAR Calling Search Space   
 Prefix DN   
 Redirecting Diversion Header Delivery - Inbound

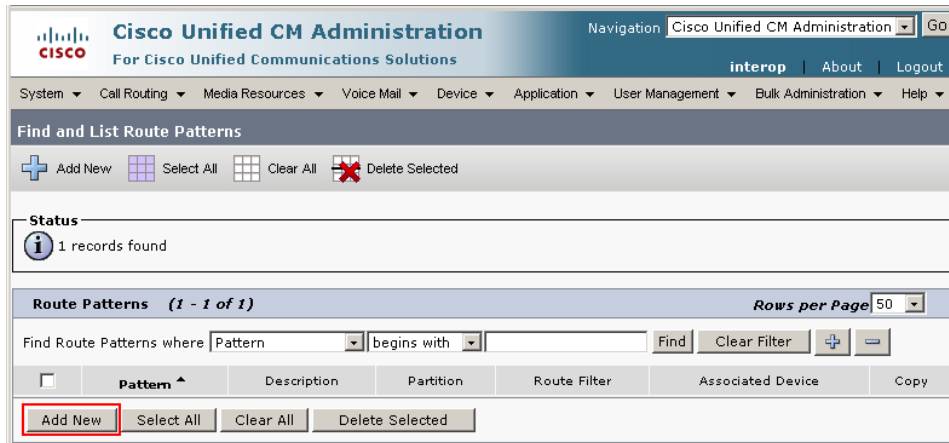
**Outbound Calls**

Called Party Transformation CSS   
 Use Device Pool Called Party Transformation CSS  
 Calling Party Transformation CSS   
 Use Device Pool Calling Party Transformation CSS  
 Calling Party Selection\*   
 Calling Line ID Presentation\*   
 Calling Name Presentation\*   
 Caller ID DN   
 Caller Name   
 Redirecting Diversion Header Delivery - Outbound

**SIP Information**

Destination Address   
 Destination Address is an SRV  
 Destination Port\*   
 MTP Preferred Originating Codec\*   
 Presence Group\*   
 SIP Trunk Security Profile\*   
 Rerouting Calling Search Space   
 Out-Of-Dialog Refer Calling Search Space   
 SUBSCRIBE Calling Search Space   
 SIP Profile\*   
 DTMF Signaling Method\*

4. Select **Call Routing** → **Route/Hunt** → **Route Pattern** then click **Add New** to add a new route pattern for extension 143xx which are for telephones registered with Avaya Aura™ Communication Manager.



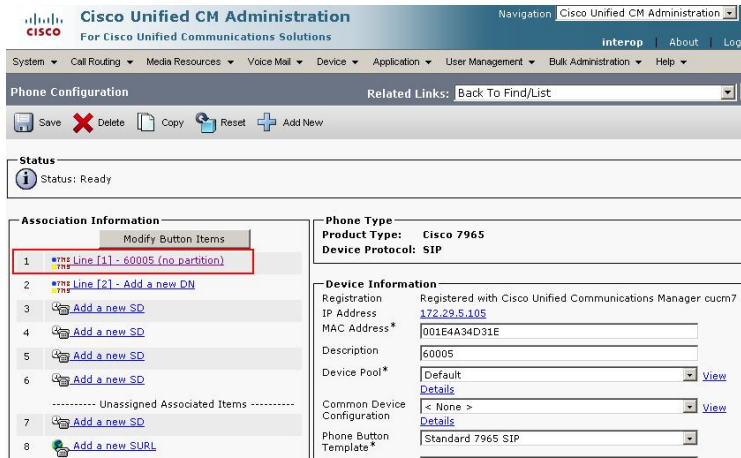
The following screen shows the route pattern used in the sample network. The route pattern “143xx” will cause all 5 digit calls beginning with “143” to be routed through the “ASM-Interop” SIP Trunk defined in **Step 3**. Click **Save** to complete.

The screenshot displays the Cisco Unified CM Administration interface for configuring a route pattern. The page title is "Route Pattern Configuration" and it includes a navigation menu at the top with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, and Bulk Administration. Below the navigation is a toolbar with icons for Save, Delete, Copy, and Add New. The main configuration area is divided into several sections:

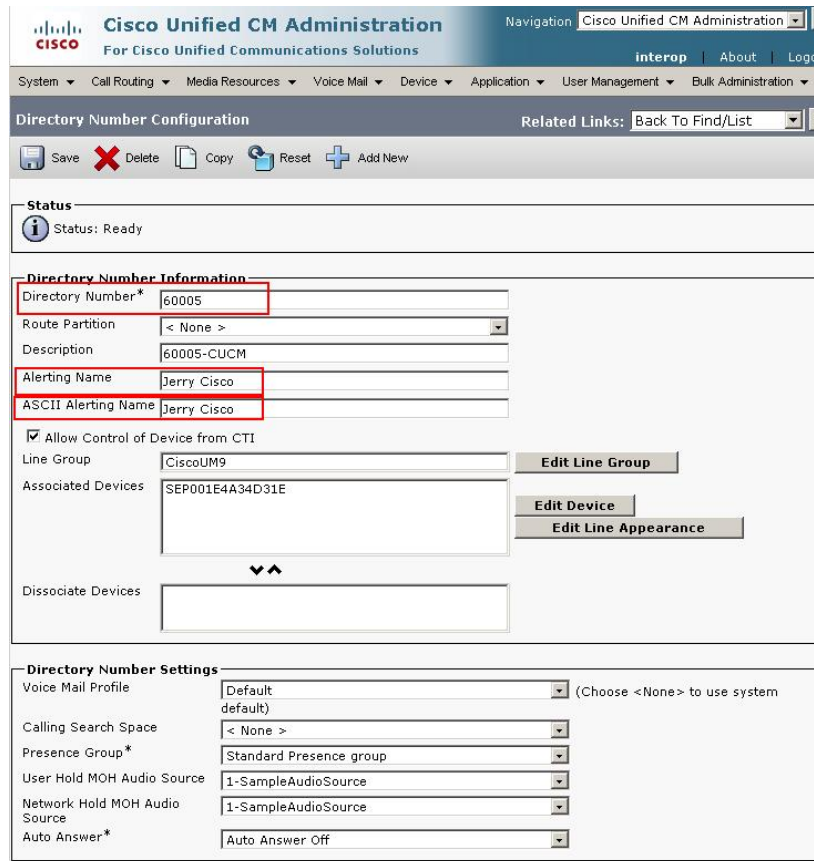
- Status:** Shows "Status: Ready".
- Pattern Definition:** This section contains the primary configuration fields:
  - Route Pattern\*: 143XX
  - Route Partition: < None >
  - Description: To Avaya G430
  - Numbering Plan: -- Not Selected --
  - Route Filter: < None >
  - MLPP Precedence\*: Default
  - Resource Priority Namespace Network Domain: < None >
  - Gateway/Route List\*: ASM-Interop (with an Edit link)
  - Route Option:  Route this pattern,  Block this pattern (with a No Error dropdown)
  - Call Classification\*: OffNet
  - Checkboxes: Allow Device Override, Provide Outside Dial Tone, Allow Overlap Sending, Urgent Priority, Require Forced Authorization Code, Require Client Matter Code.
  - Authorization Level\*: 0
- Calling Party Transformations:**
  - Use Calling Party's External Phone Number Mask
  - Calling Party Transform Mask: [Empty]
  - Prefix Digits (Outgoing Calls): [Empty]
  - Calling Line ID Presentation\*: Default
  - Calling Name Presentation\*: Default
  - Calling Party Number Type\*: Cisco CallManager
  - Calling Party Numbering Plan\*: Cisco CallManager
- Connected Party Transformations:**
  - Connected Line ID Presentation\*: Default
  - Connected Name Presentation\*: Default
- Called Party Transformations:**
  - Discard Digits: < None >
  - Called Party Transform Mask: [Empty]
  - Prefix Digits (Outgoing Calls): [Empty]
  - Called Party Number Type\*: Cisco CallManager
  - Called Party Numbering Plan\*: Cisco CallManager
- ISDN Network-Specific Facilities Information Element:**
  - Network Service Protocol: -- Not Selected --
  - Carrier Identification Code: [Empty]
  - Network Service: -- Not Selected --
  - Service Parameter Name: < Not Exist >
  - Service Parameter Value: [Empty]

At the bottom of the configuration area, there is a toolbar with buttons for Save, Delete, Copy, and Add New. The "Save" button is highlighted with a red box.

- Select **Device** → **Phone** then click on the Device that needs to be administered. 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 following screen shows the display after the line has been selected. Note: The **Display (Internal Caller ID)** and **ASCII Display (Internal Caller ID)** will be display on called party phone on all outgoing calls. Click **Save** to complete.



AAR Settings			
Voice Mail	AAR Destination Mask	AAR Group	
AAR <input type="checkbox"/> or	<input type="text"/>	< None >	
<input checked="" type="checkbox"/> Retain this destination in the call forwarding history			

Call Forward and Call Pickup Settings			
Voice Mail	Destination	Calling Search Space	
Calling Search Space Activation Policy		Use System Default	
Forward All <input type="checkbox"/> or	<input type="text"/>	< None >	
Secondary Calling Search Space for Forward All		< None >	
Forward Busy Internal <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward Busy External <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward No Answer Internal <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward No Answer External <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward No Coverage Internal <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward No Coverage External <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward on CTI Failure <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward Unregistered Internal <input type="checkbox"/> or	<input type="text"/>	< None >	
Forward Unregistered External <input type="checkbox"/> or	<input type="text"/>	< None >	
No Answer Ring Duration (seconds)	<input type="text"/>		
Call Pickup Group	<input type="text" value="interop-group"/>		

MLPP Alternate Party Settings	
Target (Destination)	<input type="text"/>
MLPP Calling Search Space	< None >
MLPP No Answer Ring Duration (seconds)	<input type="text"/>

Line Settings for All Devices		
Hold Reversion Ring Duration (seconds)	<input type="text"/>	Setting the Hold Reversion Ring Duration to zero will disable the feature
Hold Reversion Notification Interval (seconds)	<input type="text"/>	Setting the Hold Reversion Notification Interval to zero will disable the feature

**Line 1 on Device SEP001E4A34D31E**

Display (Internal Caller ID)  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)

Line Text Label

ASCII Line Text Label

External Phone Number Mask

Visual Message Waiting Indicator Policy\*

Audible Message Waiting Indicator Policy\*

Ring Setting (Phone Idle)\*

Ring Setting (Phone Active)  Applies to this line when any line on the phone has a call in progress.

Call Pickup Group Audio Alert Setting (Phone Idle)

Call Pickup Group Audio Alert Setting (Phone Active)

Recording Option\*

Recording Profile

Monitoring Calling Search Space

---

**Multiple Call/Call Waiting Settings on Device SEP001E4A34D31E**

Note: The range to select the Max. Number of calls is: 1-50

Maximum Number of Calls\*

Busy Trigger\*  (Less than or equal to Max. Calls)

---

**Forwarded Call Information Display on Device SEP001E4A34D31E**

Caller Name

Caller Number

Redirected Number

Dialed Number

---

**Users Associated with Line**

## 8. Verification

This section provides the tests that can be performed on Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, and Cisco UCM to verify proper their proper configuration.

### 8.1. Verify Avaya Aura™ Communication Manager

1. Verify the status of the SIP trunk group by using the “status trunk n” command, where “n” is the trunk group number being investigated. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 25

                                TRUNK GROUP STATUS

Member   Port      Service State   Mtce Connected Ports
                                Busy

0025/001 T00007   in-service/idle no
0025/002 T00008   in-service/idle no
0025/003 T00009   in-service/idle no
0025/004 T00010   in-service/idle no
0025/005 T00011   in-service/idle no
0025/006 T00012   in-service/idle no
0025/007 T00013   in-service/idle no
0025/008 T00014   in-service/idle no
0025/009 T00015   in-service/idle no
0025/010 T00016   in-service/idle no
```

2. Verify the status of the SIP signaling-group by using the “status signaling-group n” command, where “n” is the signaling group number being investigated. Verify that the signaling group is in the “in-service” state as shown below.

```
status signaling-group 25

                                STATUS SIGNALING GROUP

Group ID: 25                               Active NCA-TSC Count: 0
Group Type: sip                             Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service
```

## 8.2. Verify Avaya Aura™ Session Manager

1. Expand the **Avaya Aura™ Session Manager** field on the left panel menu and click on **SIP Monitoring**. Verify as shown below that none of the links for SIP entities are down, indicating that they are all reachable for routing.

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The left navigation pane is expanded to 'Session Manager' > 'SIP Monitoring'. The main content area displays the 'SIP Entity Link Monitoring Status Summary' page. A table shows the status for the 'Avaya-asm' instance, with 'Entity Links Down/Total' highlighted as '0/4'. Below this, a list of 'All Monitored SIP Entities' includes 'Avaya-G430' and 'CiscoUCM7'.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at Apr. 15, 2009 10:27 AM [Help](#) | [Log off](#)

Home / Session Manager / SIP Monitoring

### SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

[Refresh](#)

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
<a href="#">Avaya-asm</a>	0/4	0	0	0

All Monitored SIP Entities

[Refresh](#)

4 Items | Filter: Enable

SIP Entity Name
<a href="#">Avaya-G430</a>
<a href="#">CiscoUCM7</a>

2. Select the SIP Entity Name entities, shown in the previous screen, and verify that the connection status is “Up”, as shown below for CiscoUCM7.

The screenshot shows the Avaya Integrated Management System Manager 1.0 interface. The left navigation pane is expanded to 'Session Manager' > 'SIP Monitoring'. The main content area displays the 'SIP Entity, Entity Link Connection Status' page for 'CiscoUCM7'. A table shows the connection status for the 'SM1' instance, with 'Conn. Status' highlighted as 'Up'.

**AVAYA** INTEGRATED MANAGEMENT SYSTEM MANAGER 1.0

Welcome, **admin** Last Logged on at May. 01, 2009 11:07 AM [Help](#) | [Log off](#)

Home / Session Manager / SIP Monitoring / SIP Entity Link Status

### SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: [CiscoUCM7](#)

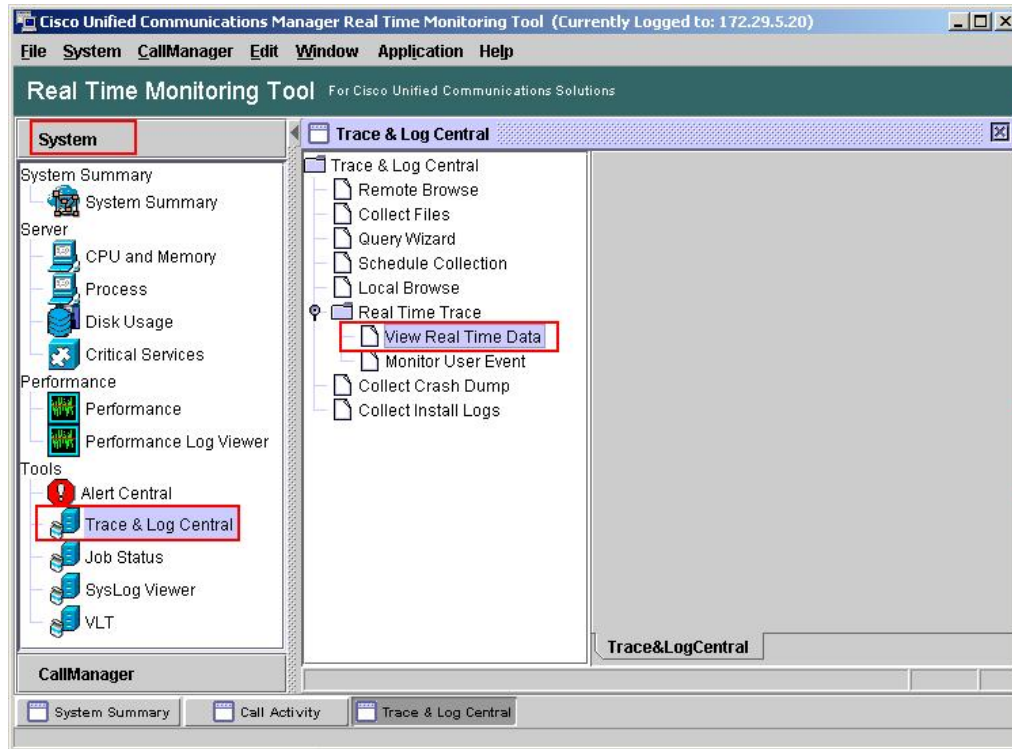
[Refresh](#) [Summary View](#)

1 Item | Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
<a href="#">Show</a>	<a href="#">SM1</a>	172.29.5.20	5060	TCP	Up	200 OK	Up

### 8.3. Verify Cisco Unified Communications Manager

1. The Real Time Monitoring Tool (RTMT) can be use to monitor events on Cisco Unified CM. This tool can be downloaded by selecting **Application** → **Plugins** from the top menu of the Cisco Unified CM Administration Web interface. For further information on this tool, please consult with reference [8]. The following screen shows where user can view and perform real time data capture.



## 8.4. Verified Scenarios

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

- Basic calls between various telephones on Avaya Aura™ Communication Manager and Cisco Unified Communications Manager can be made in both directions using G.711MU, G.729, and G.729AB. For G.729 interoperability, the IP codec set on Avaya Aura™ Communication Manager must include a version of the G.729 that Cisco UCM supports.
- Proper display of the calling and called party name and number information was verified for all telephones with the basic call scenario.
- Supplementary calling features were verified. The feature scenarios involved additional endpoints on the respective systems, such as performing an unattended transfer of the SIP trunk call to a local endpoint on the same site, and then repeating the scenario to transfer the SIP trunk call to a remote endpoint on the other site. The supplementary calling features verified were shown below. Note that calling/called party name and number display may not be consistent in some cases.
  - Unattended transfer
  - Attended transfer
  - Hold/Unhold
  - Consultation hold
  - Call forwarding
  - Conference

## 9. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager can interoperate with Cisco Unified Communications Manager using SIP trunks via Avaya Aura™ Session Manager. The following is a list of interoperability items to note:

- For G.729 interoperability, make sure both G.729 and G729AB are part of the audio codec selection in Avaya Aura™ Communication Manager.
- For proper displaying of calling party information, Cisco UCM must be configured with the Internal Caller ID name as described in Section 7, Step 5.
- With direct media “shuffling” enabled, a “one-way” audio issue was observed when a call initiated by a Cisco SIP Telephone to an Avaya IP telephone was put on hold and then released on the Cisco SIP telephone side. When the Cisco SIP telephone released the hold, the Cisco SIP telephone sent media traffic to the Avaya G430 Media Gateway instead of directly to the Avaya IP telephone as instructed by Avaya Aura™ Communication Manager in the SDP portion of the final ACK message. The workaround is to disable direct media between the Cisco SIP telephones and Avaya IP telephones. This issue does not exist if the call is initiated from Avaya or if the Hold/Release is done from an Avaya IP Telephone. In addition, it is worth noting that this issue does not exist between Avaya IP telephones and Cisco IP telephones (SCCP).

## 10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>

- [1] *Avaya Aura™ Session Manager Overview*, Doc # 03-603323
- [2] *Installing and Administering Avaya Aura™ Session Manager*, Doc # 03-603324
- [3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc # 03-603325
- [4] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, May 2009
- [5] *Administering Avaya Aura™ Communication Manager*, Doc # 03-300509 May 2009

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

- [6] *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*, Release 7.0(1), Part Number: OL-15405-01
- [7] *Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communication Manager Business Edition*, Release 7.0(1), Part Number: OL-15409-01
- [8] *Cisco Unified Real-Time Monitoring Tool Administration Guide*, Release 7.0(1), Part Number: OL-14994-01

---

**©2009 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 Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)