



Avaya Solution & Interoperability Test Lab

Sample Configuration for a SIP Trunk between Avaya SIP Enablement Services Server and Cisco Unified CM 7.0 – Issue 1.0

Abstract

These Application Notes describe the steps for configuring a SIP trunk between Avaya SIP Enablement Services (SES) Server and Cisco Unified Communications Manager (CUCM).

1. Introduction

Session Initiation Protocol (SIP) is a standards-based communication protocol capable of supporting voice, video, instant messaging and other multi-media communication. These Application Notes will outline a solution for using SIP as a trunking protocol to support calling between an Avaya Communication Manager and a Cisco IP PBX.

2. Overview

The sample network shown in **Figure 1** consists of two IP PBX systems each belonging to a different domain with its own dialing plan. The Avaya system consists of Avaya Communication Manager and Avaya SIP Enablement Services (SES) Server supporting a variety of Avaya 4600 and 9600 Series IP Telephones with either H.323 or SIP protocol along with digital and analog fax stations. The Cisco IP PBX system consists of Cisco Unified Communications Manager (CUCM) supporting the Cisco SIP and SCCP stations along with analog fax stations through the use of a Cisco 1751 router/gateway. A SIP trunk is configured between Avaya SES and CUCM to support calling for telephones between the Avaya and Cisco IP PBX systems. With the use of the SIP trunk transcoding, media and protocol conversion, calls between any 2 telephones are supported regardless in this sample network whether they are between SIP, H.323, DCP, SCCP or analog stations.

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 Communication Manager or Avaya SES and use extension 11xxx. All IP telephones in the 172.29.5.0/24 IP network are registered with CUCM and use extension 60xxx. A single SIP trunk between Avaya SES and CUCM manages call control between the Avaya and Cisco IP PBX systems.

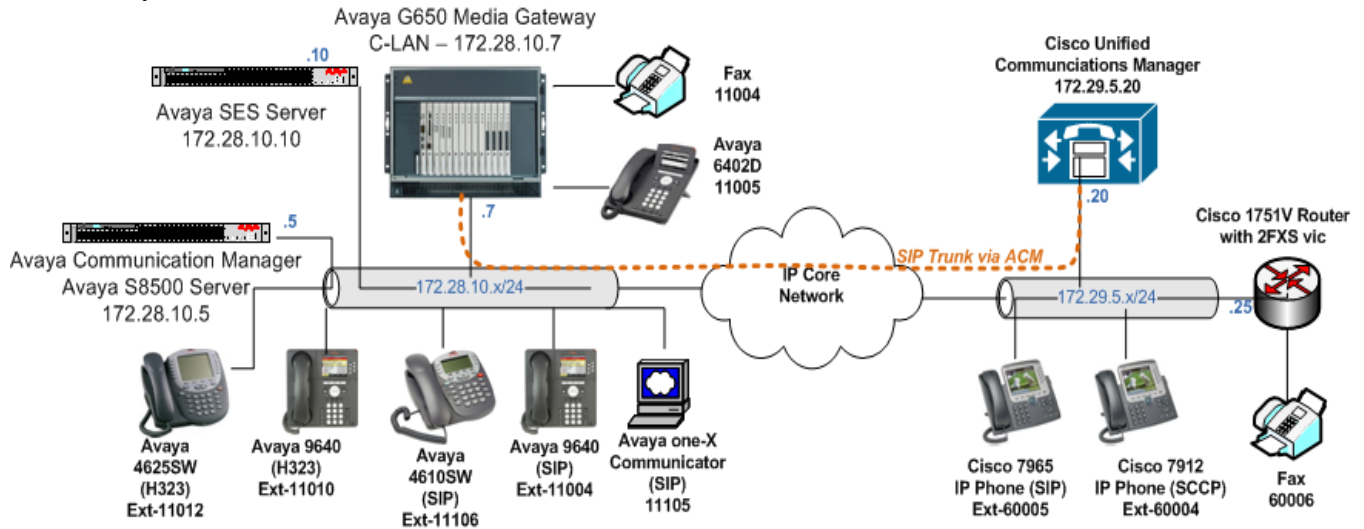


Figure 1: Sample Network Configuration

4. Equipment and Software Validated

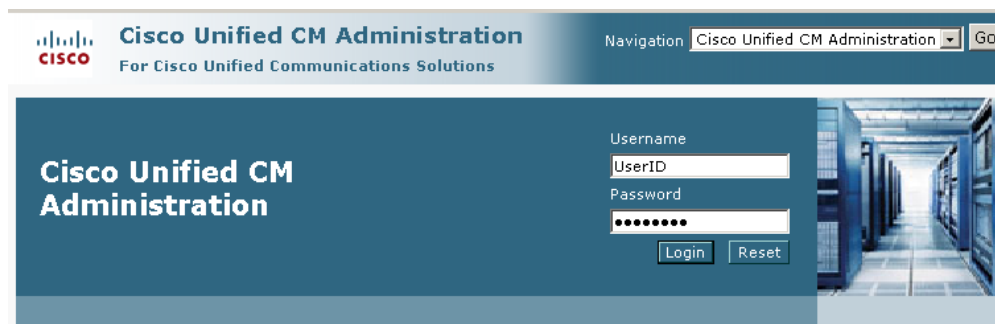
The following equipment and software/firmware were used for the sample configuration:

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8500 Server with G650 Media Gateway	5.1.2
Avaya SIP Enablement Services (SES) Server	5.1.2
Avaya 4625SW IP Telephone (H.323)	2.9
Avaya 9640 IP Telephone (H.323)	2.0
Avaya 4610SW IP Telephone (SIP)	2.2.2
Avaya 9640 IP Telephone (SIP)	2.2.0
Avaya 6402D Digital Telephone	-
Avaya One-X Communicator (SIP)	1.0
Cisco Unified Communications Manager	7.0.1.1.11000-2
Cisco 7965 Unified IP Phone (SIP)	SIP45.8-4-1S
Cisco 7912 Unified IP Phone (SCCP)	App Load ID CP7912080003SCCP070409A Boot Load ID LD0100BOOT021112A
Cisco 1751v router	IOS 12.4(10a)

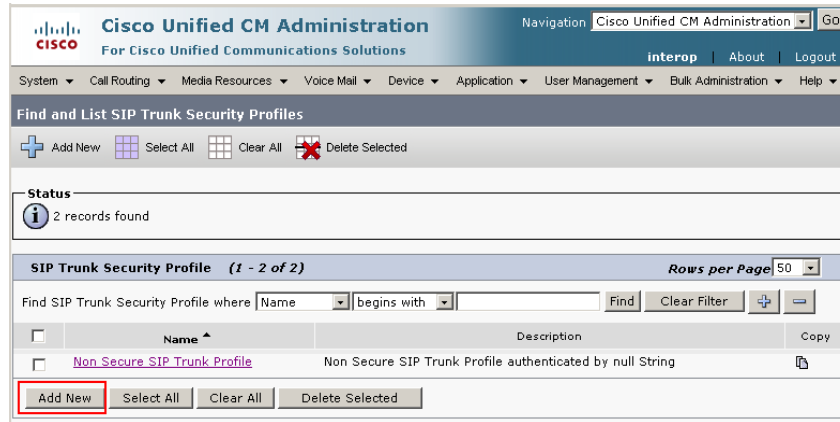
5. Configure Cisco Unified CM

This section describes the SIP Trunk configuration for CUCM as shown in **Figure 1**. It is assumed that the basic configuration needed to interoperate with the 1751 router/gateway and support for Cisco IP telephones has been completed. For further information on Cisco Unified CM, please consult references [8] and [9].

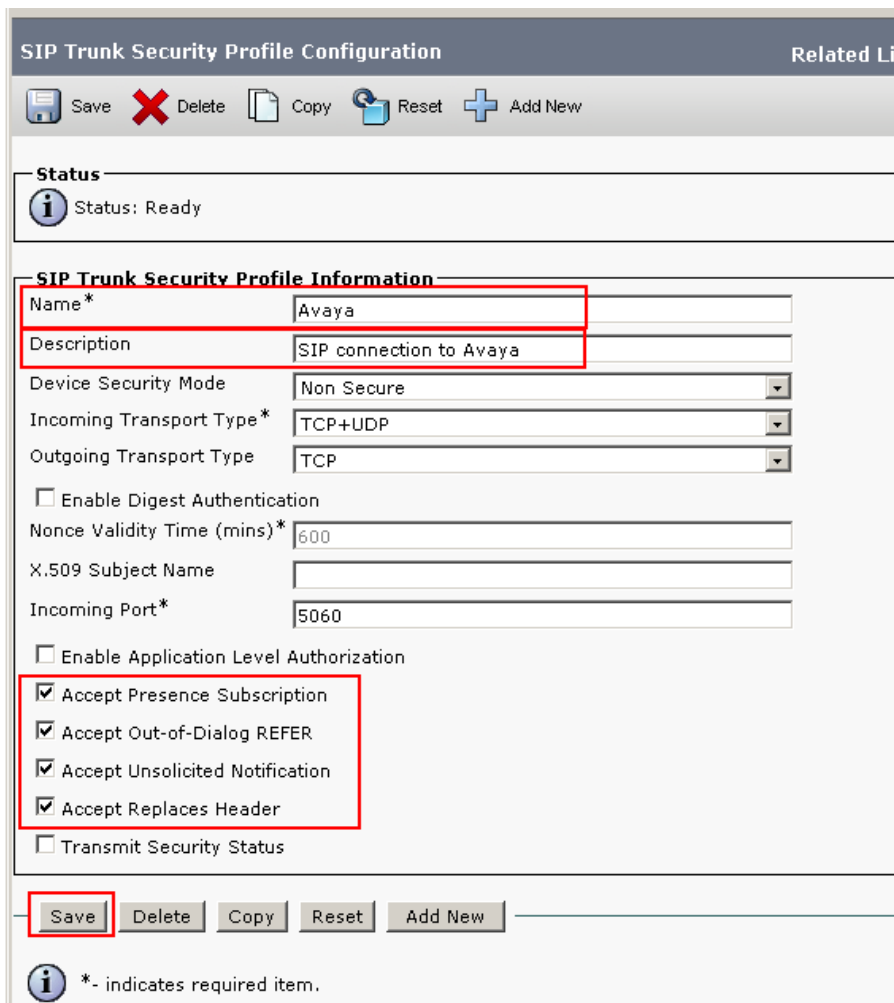
1. Open Cisco Unified CM Administration by entering the IP address of the CUCM into the Web Browser address field, and log in using an appropriate Username and Password.



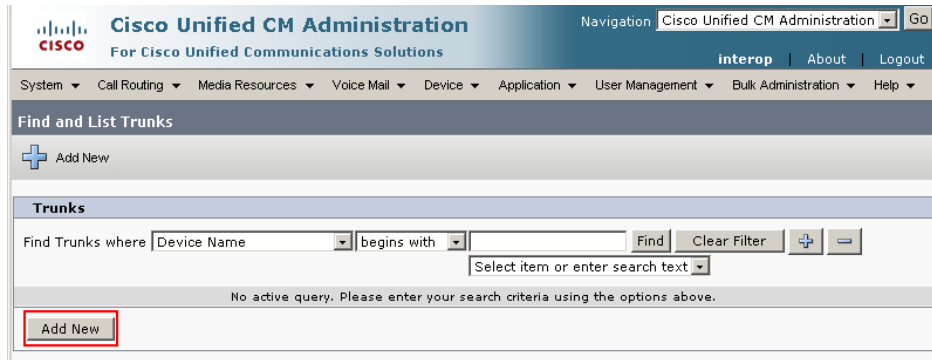
2. Select **System** → **Security Profile** → **SIP Trunk Security Profile** from the top menu then click **Add New** to add a new SIP Trunk Security Profile.



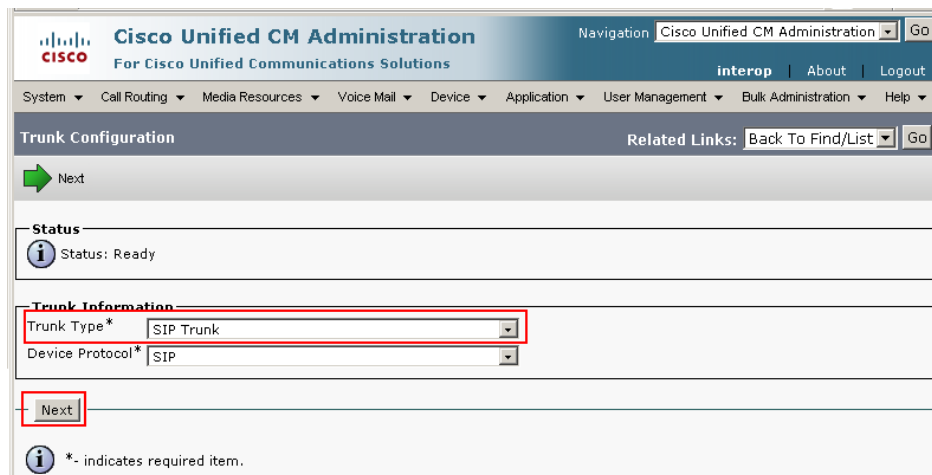
The following is a screen capture of the SIP Trunk Security Profile used in the sample network. Configure the highlighted areas and click **Save** to commit the changes.



3. Select **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 capture shows the configuration used in the sample network. Click **Save** to complete.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Trunk Configuration | Related Links: Back To Find/List

Save | Delete | Reset | Add New

Status
Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Device Name*	AvayaSES
Description	To Avaya SES
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.

Clear Prefix Settings | Default Prefix Settings

Incoming Calling Party Unknown Number Prefix | Default

Multilevel Precedence and Preemption (MLPP) Information
 MLPP Domain | < None >

Call Routing Information
 Remote-Party-Id
 Asserted-Identity
 Asserted-Type* | Default
 SIP Privacy* | None

Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	

Redirecting Diversion Header Delivery - Inbound

Outbound Calls

Called Party Transformation CSS < None >

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS < None >

Use Device Pool Calling Party Transformation CSS

Calling Party Selection* Originator

Calling Line ID Presentation* Default

Calling Name Presentation* Default

Caller ID DN

Caller Name

Redirecting Diversion Header Delivery - Outbound

SIP Information

Destination Address 172.28.10.10

Destination Address is an SRV

Destination Port* 5060

MTP Preferred Originating Codec* 711ulaw

Presence Group* Standard Presence group

SIP Trunk Security Profile* Avaya

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

*- indicates required item.

4. Select **Call Routing** → **Route/Hunt** → **Route Pattern** then click **Add New** to add a new route pattern for extension 11xxx which are for telephones registered with Avaya Communication Manager.

Cisco Unified CM Administration Navigation Cisco Unified CM Administration Go

interop About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Find and List Route Patterns

+ Add New Select All Clear All Delete Selected

Status

1 records found

Route Patterns (1 - 1 of 1) Rows per Page 50

Find Route Patterns where Pattern begins with Find Clear Filter + -

<input type="checkbox"/>	Pattern ^	Description	Partition	Route Filter	Associated Device	Copy
<p>Add New Select All Clear All Delete Selected</p>						

The following screen capture shows the route pattern used in the sample network. The route pattern “11xxx” will cause all 5 digit calls beginning with “11” to be routed through the “AvayaSES” SIP Trunk defined in **Step 3**. Click **Save** to complete.

Route Pattern Configuration Related Links: [Back To Find/List](#) [Go](#)

Save Delete Copy Add New

Status
i Status: Ready

Pattern Definition

Route Pattern*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence*

Resource Priority Namespace Network Domain

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

Route Option
 Route this pattern
 Block this pattern

Call Classification*

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

Require Forced Authorization Code

Authorization Level*

Require Client Matter Code

Calling Party Transformations

Use Calling Party's External Phone Number Mask

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Line ID Presentation*

Calling Name Presentation*

Calling Party Number Type*

Calling Party Numbering Plan*

Connected Party Transformations

Connected Line ID Presentation*

Connected Name Presentation*

Called Party Transformations

Discard Digits

Called Party Transform Mask

Prefix Digits (Outgoing Calls)

Called Party Number Type*

Called Party Numbering Plan*

ISDN Network-Specific Facilities Information Element

Network Service Protocol

Carrier Identification Code

Network Service	Service Parameter Name	Service Parameter Value
<input type="text" value=" -- Not Selected --"/>	<input type="text" value=" < Not Exist >"/>	<input type="text"/>

i *- indicates required item.

6. Configure Avaya Communication Manager

This section shows the configuration of Avaya Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assume that the basic configuration between Avaya Communication Manager and Avaya SIP Enablement Services (SES) Server has already been completed and working. For further information on Avaya Communication Manager, please consult with references [1], [2] and [3].

1. Use the **add signaling-group** command to add a new signaling group into the system. The sample network uses signaling groups 29 and 80. Signaling group 29 is the signaling group configured for communication between Avaya Communication Manager and Avaya SES Server that should have been configured as part of the basic configuration. This signaling group has interop.com which is the same domain as Avaya Communication Manager configured as its Far-end Domain.

```
display signaling-group 29
SIGNALING GROUP
Group Number: 29          Group Type: sip
                          Transport Method: tls

Near-end Node Name: CLAN      Far-end Node Name: SES
Near-end Listen Port: 5061    Far-end Listen Port: 5061
                          Far-end Network Region: 9
Far-end Domain: interop.com

                          Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload    Direct IP-IP Audio Connections? y
                          IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 3    Alternate Route Timer(sec): 6
```

The following signaling-group 80 is added to Avaya Communication Manager for the SIP Trunk that is configured for traffic between Avaya SES and CUCM. The Far-end Domain is left blank to allow for incoming SIP calls from domains not matching interop.com. Alternatively, a specific domain that the CUCM system is in can also be entered.

```
display signaling-group 80
SIGNALING GROUP
Group Number: 80          Group Type: sip
                          Transport Method: tls

Near-end Node Name: CLAN      Far-end Node Name: SES
Near-end Listen Port: 5061    Far-end Listen Port: 5061
                          Far-end Network Region: 9
Far-end Domain:

                          Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload    Direct IP-IP Audio Connections? y
                          IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 3    Alternate Route Timer(sec): 6
```

2. Use the **add trunk-group** command to add a new trunk group into the system. The sample network uses trunk groups 29 and 80. Trunk group 29 is the trunk group configured for communication between Avaya Communication Manager and Avaya SES Server that should have been configured as part of the basic configuration. This trunk group is configured to use signaling group 29 shown in **Step 1**. The following is a screen capture for trunk group 29.

```
display trunk-group 29                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 29                Group Type: sip                CDR Reports: y
  Group Name: To-SES                COR: 1                TN: 1                TAC: 129
  Direction: two-way                Outgoing Display? n
Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n
                                     Signaling Group: 29
                                     Number of Members: 50
```

Trunk group 80 is added to Avaya Communication Manager for the SIP Trunk that is configured for traffic between Avaya SES and Cisco Unified CM. Trunk group 80 is configured to use signaling group 80 shown in **Step 1**. The following is a screen capture of trunk group 80. It is important to note that the trunk group used for domains other than interop.com has a higher trunk group number than the trunk group having the native domain, in this case trunk group 29 using interop.com. This helps match domain information on incoming SIP calls to the native domain when multiple SIP trunks are configured between Avaya Communication Manager and Avaya SES.

```
display trunk-group 80                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 80                Group Type: sip                CDR Reports: y
  Group Name: To-CUCM7                COR: 1                TN: 1                TAC: 180
  Direction: two-way                Outgoing Display? n
Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n
                                     Signaling Group: 80
                                     Number of Members: 10
```

- Use the **change ip-network-region** form to configure the ip-network-region and codec. The following screen capture shows ip-network-region 9 used in the sample network.

```

display ip-network-region 9                                     Page 1 of 19
                                     IP NETWORK REGION
Region: 9
Location: Authoritative Domain: interop.com
Name:
MEDIA PARAMETERS
  Codec Set: 1
  UDP Port Min: 2048
  UDP Port Max: 3329
  Intra-region IP-IP Direct Audio: yes
  Inter-region IP-IP Direct Audio: yes
  IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
  RTCP Reporting Enabled? y
RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? y
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
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
  RSVP Enabled? n

```

```

display ip-network-region 9                                     Page 3 of 19
                                     Inter Network Region Connection Management
src dst codec direct WAN-BW-limits Video Intervening Dyn
rgn rgn set WAN Units Total Norm Prio Shr Regions CAC IGAR AGL
9 1 1 y NoLimit
9 2
9 3
9 4
9 5
9 6
9 7
9 8
9 9 1 all

```

- Use the **change ip-codec-set** form to configure the audio codec. The following screen capture shows ip-codec-set 1 used in the sample network.

```

display 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:

```

- Use **change dialplan analysis** to define any 5 digit call beginning with 60 as an aar Call Type. The following screen capture shows the dialplan used in the sample network.

```
display dialplan analysis
```

DIAL PLAN ANALYSIS TABLE									
Location: all					Percent Full: 1				
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	3	dac							
11	5	ext							
60	5	aar							
8	1	fac							
9	1	fac							
*	3	fac							
#	3	fac							

- Use **change aar analysis** form to configure the appropriate route pattern for the 5 digit dial string that begins with 60. The following screen capture shows the calls to 60xxx are routed using Route Pattern 29 in the sample network.

```
display aar analysis 60
```

AAR DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 1			
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
60	5	5	29	aar		n	
7	7	7	999	aar		n	
8	7	7	999	aar		n	
9	7	7	999	aar		n	

- Use the **change route-pattern** form to configure the appropriate trunk group. The following screen capture shows that route pattern 29 directs calls to use trunk group 29 in the sample network.

```
change route-pattern 29
```

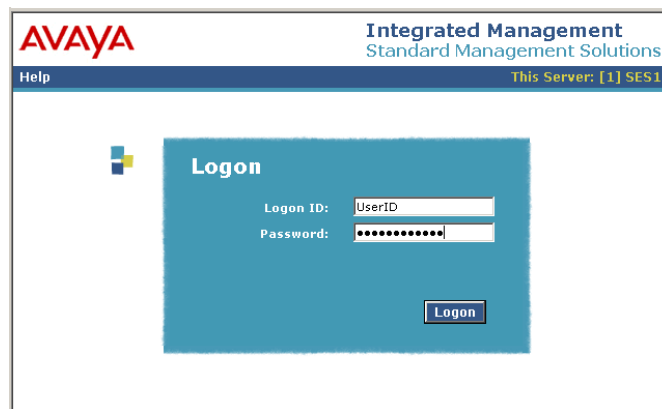
Pattern Number: 29 Pattern Name: To-CUCM-7										
SCCAN? n					Secure SIP? n					
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ IXC	IXC	
1:	29	0						n	user	
2:								n	user	
3:								n	user	
4:								n	user	
BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No. Dgts	Numbering Format	LAR
0	1 2 M 4 W		Request							
1:	y y y y y	n		rest						none
2:	y y y y y	n		rest						none
3:	y y y y y	n		rest						none
4:	y y y y y	n		rest						none

7. Configuring Avaya SES Server

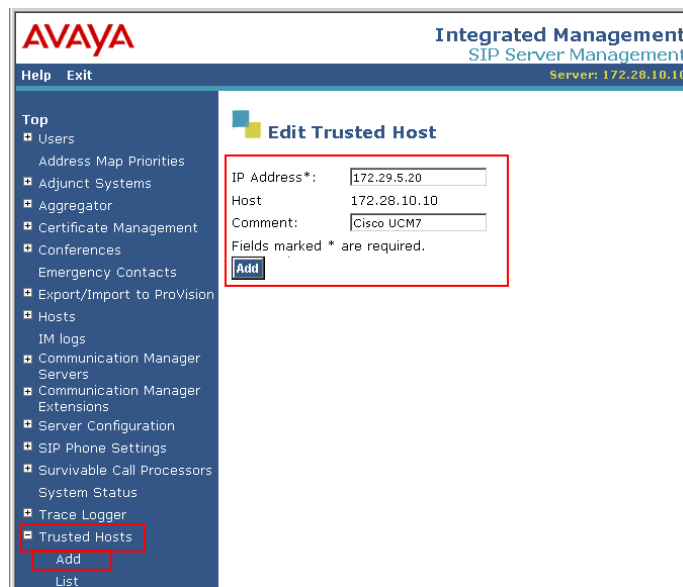
This section shows the configuration of Avaya SES Server. These Application Notes assume that the basic configuration between Avaya Communication Manager and Avaya SES Server has already been completed and working. For further information on Avaya SES, please consult references [4], [5] and [6].

1. Open the Avaya SES administration interface by entering the IP address of Avaya SES Server into a Web Browser in the form of <http://IP address/admin>. Log in using appropriate credentials.

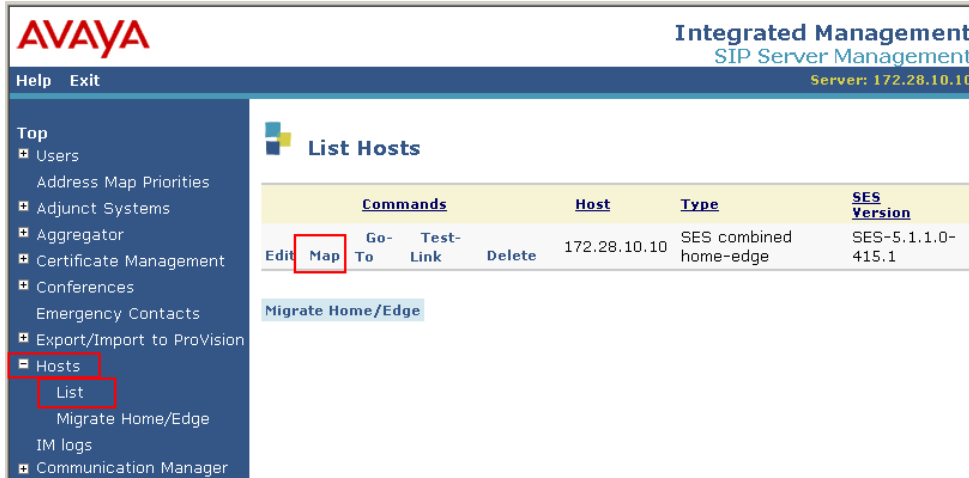
Upon successfully logging into Avaya SES, select Launch SES Administration Interface (not shown below).



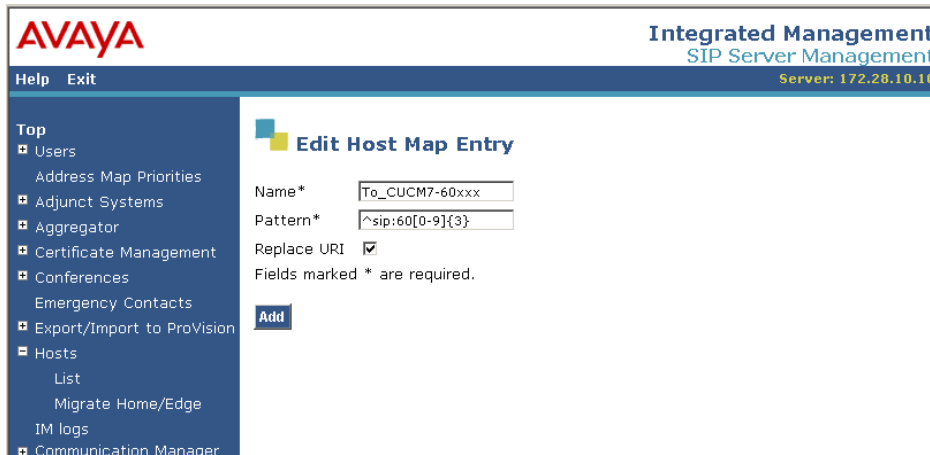
2. Select **Trusted Hosts** → **Add** to add the CUCM as a trusted host. The following is a screen capture of the Trusted Host information. Click **Add** to complete



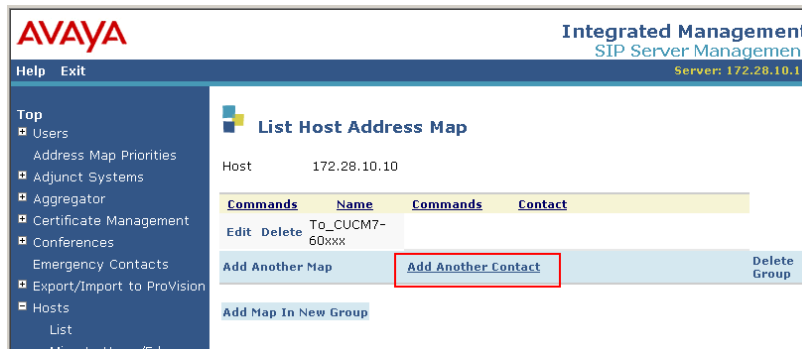
3. Select **Hosts** → **List** from the left menu panel to display a list of hosts then click on **Map** to begin adding a new address map.



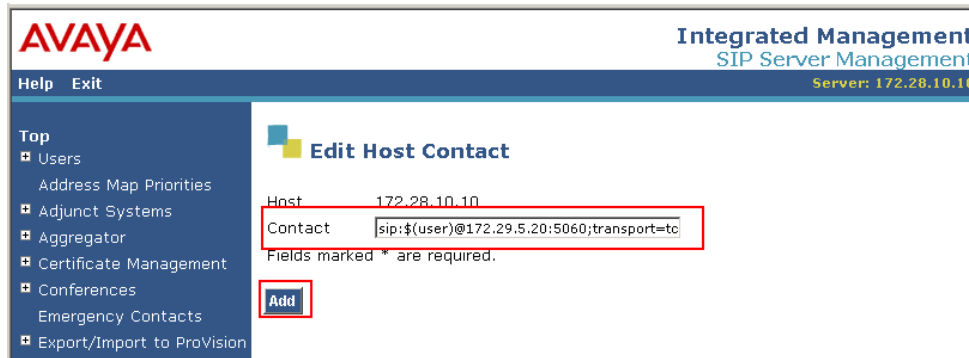
The following screen capture shows the host map to direct any 5 digit number beginning with “60” to Cisco Unified CM. Click **Add** to complete.



After adding the new host map, click **Add Another Contact** to configure the contact information.



The following screen capture shows the host contact used in the sample network. The Contact entry “sip:\$(user)@172.29.5.20:5060;transport=tcp” directs the SIP call to the CUCM IP address of 172.29.5.20 using TCP as the transport protocol. Click **Add** to complete.



8. Verification

The following steps may be used to verify the configuration:

1. “list trace station” may be used in Avaya Communication Manager via SAT to verify whether calls from Avaya H.323, digital, or analog telephones are being routed to the correct trunk group.
2. The Real Time Monitoring Tool (RTMT) can be used 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 [10].

9. Conclusion

These Application Notes describe the administrative steps required to configure a SIP trunk to support calls between an Avaya IP PBX and a Cisco IP PBX system. Basic calling including Hold, Transfer, Conference and Fax Pass-through as well as supplemental features such as Call Forward All, Call Park/Unpark are supported by this configuration.

Due to implementation differences between Cisco SIP and SCCP telephone, there is a certain limitation when using Music-on-Hold between an Avaya telephone and Cisco SCCP telephone. Music can not be heard on an Avaya telephone when a call is placed on Hold by the Cisco SCCP telephone. However, Music-on-Hold does work when the Hold is placed by an Avaya telephone. This limitation does not apply to the Cisco SIP telephone used in this configuration.

10. Additional References

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

- [1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4.0, Release 5.0, January 2008
- [2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 4, Release 5.0, January 2008
- [3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 13, January 2008
- [4] *Administering SIP Enablement Services on the Avaya S8300 Server*, Doc # 03-602508, Issue 1.0, January 2008
- [5] *SIP Support in Avaya Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 8, January 2008
- [6] *Configuring Avaya SIP Telephony Users on Avaya SIP Enablement Services and Avaya Communication Manager*, Issue 1.0
- [7] *one-X Communicator Administration Quick Setup*, Doc # 16-602603, Issue 3, December 2008

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

- [8] *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition*, Release 7.0(1), Part Number: OL-15405-01
- [9] *Cisco Unified Communications Manager Features and Services Guide for Cisco Unified Communication Manager Business Edition*, Release 7.0(1), Part Number: OL-15409-01
- [10] *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