



Configuring SIP Trunks among Cisco Unified Communications Manager, Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager 5.2 as a Feature Server – 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 as a Feature Server and Cisco Unified Communications Manager using SIP trunks.

The results in these Application Notes should be applicable to other Avaya Servers and Media Gateways that support Avaya Aura™ Communication Manager. Testing was conducted via the 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 Aura™ Session Manager to connect Avaya Aura™ Communication Manager as a Feature Server and Cisco Unified Communications Manager (Cisco UCM) using SIP trunks.

2. Overview

The sample network is shown in **Figure 1**. Communication Manager supports the Avaya 9620 IP Telephone (SIP). The Cisco UCM supports the Cisco 7911G IP Telephone (SIP) and the Cisco 7911G IP Telephone (SCCP). SIP trunks are used to connect these two systems to Session Manager. All inter-system calls are carried over these SIP trunks. 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 Session Manager is managed by a separate Avaya Aura™ System Manager, which can manage multiple Session Managers.

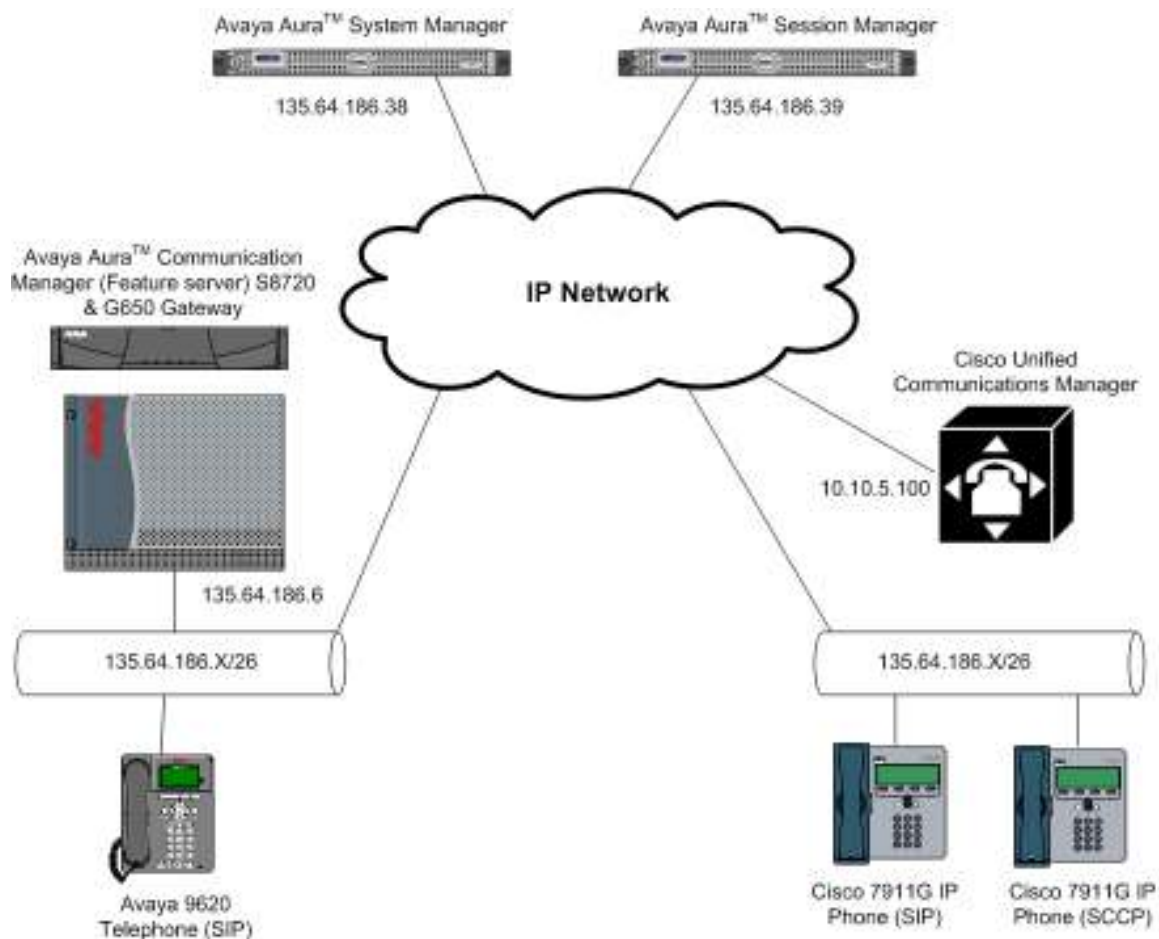


Figure 1: Connection of CM and CUCM via Session Manager using SIP Trunks

All telephones in the 135.64.186.x/26 IP network are either registered with Communication Manager or Cisco UCM. Avaya phones are registered to Avaya Aura™ Communication Manager and Cisco phones to Cisco UCM. Avaya SIP stations use extensions 320xx. Cisco UCM registered stations use extensions 3500x. Two separate SIP trunks are provisioned to the Session Manager to manage call control for calls between the two systems. One from Communication Manager and one from Cisco UCM.

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8720 Media Server	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya G650 Media Gateway <ul style="list-style-type: none"> • TN799DP C-LAN Circuit Pack • TN2312BP IP Server Interface • TN2602AP IP Media Pro • TN2224CP Digital Line 	HW01 FW034 HW15 FW047 HW08 FW049 HW08 FW015
Avaya S8510 Server with SM100 Card	Avaya Aura™ Session Manager 5.2
Avaya S8510 Server	Avaya Aura™ System Manager 5.2
Avaya 9620 IP Telephone (SIP)	2.5.5.19
Cisco Unified Communications Manager	7.0.2.10000-18
Cisco 7911G SIP Telephone	SIP11.8-4-3S
Cisco 7911G SCCP Telephone	SCCP11.8-4-3S

4. Configure Avaya Aura™ Communication Manager

This section shows the configuration of 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 Communication Manager, please consult with references [4] and [5]. The procedures include the following areas:

- Verify Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec set
- Administer SIP Signaling Group and Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan and AAR analysis
- Save Changes

4.1. Verify Communication Manager License

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 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		30	0
Maximum Concurrently Registered IP Stations:		18000	9
Maximum Administered Remote Office Trunks:		0	0
Maximum Concurrently Registered Remote Office Stations:		0	0
Maximum Concurrently Registered IP eCons:		0	0
Max Concur Registered Unauthenticated H.323 Stations:		0	0
Maximum Video Capable Stations:		10	1
Maximum Video Capable IP Softphones:		10	4
Maximum Administered SIP Trunks:		100	55

4.2. Administer System Parameters Features

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?		y	
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:		none	
Music (or Silence) on Transferred Trunk Calls?		no	
DID/Tie/ISDN/SIP Intercept Treatment:		attd	
Internal Auto-Answer of Attd-Extended/Transferred Calls:		transferred	
Automatic Circuit Assurance (ACA) Enabled?		n	

4.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for the Communication Manager and Session Manager that will be used for connectivity. In the sample network, **clan1a3** and **135.64.186.6** are entered as **name** and **IP Address** for the CLAN card in Communication Manager running on the Avaya S8720 Server. In addition, **SM100** and **135.64.186.40** are entered for Session Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
Gateway001	135.64.186.1	
MBTCM	135.64.186.68	
MX6200	135.64.186.15	
SM100	135.64.186.40	
clan1a3	135.64.186.6	
clan1b3	135.64.186.7	
default	0.0.0.0	
mpro1a2	135.64.186.8	
mpro1b2	135.64.186.9	
onexmobile	135.64.186.30	
procr	135.64.186.10	
silstackaes	135.64.186.28	

4.4. Administer IP Network Region and Codec Set

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 3 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 **3** to use ip-codec-set 3.

change ip-network-region 3		Page 1 of 19
IP NETWORK REGION		
Region: 3		
Location:	Authoritative Domain: silstack.com	
Name: To ASM		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 3	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 3

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

4.5. Administer SIP Signaling Group and Trunk Group

4.5.1. SIP Signaling Group

In the test configuration, Communication Manager acts as a Feature Server. An IMS enabled SIP trunk is required. Use signal group 150 along with trunk group 155 to reach the Session Manager. Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system. Use the values defined in **Section 4.3** and **4.4** for **Near-end Node Name**, **Far-End Node-Name** and **Far-End Network Region**. The **Far-end Domain** is left blank so that the signaling group accepts any authoritative domain.

Set **IMS Enabled** to **y**.

add signaling-group 150

Page 1 of 2

SIGNALING GROUP

Group Number: 150

Group Type: sip

Transport Method: tcp

IMS Enabled? y

IP Video? n

Near-end Node Name: clan1a3

Far-end Node Name: SM100

Near-end Listen Port: 5063

Far-end Listen Port: 5063

Far-end Network Region: 3

Far-end Domain:

Incoming Dialog Loopbacks: eliminate

Bypass If IP Threshold Exceeded? n

DTMF over IP: rtp-payload

RFC 3389 Comfort Noise? n

Session Establishment Timer(min): 3

Direct IP-IP Audio Connections? y

Enable Layer 3 Test? n

IP Audio Hairpinning? n

H.323 Station Outgoing Direct Media? y

Direct IP-IP Early Media? n

Alternate Route Timer(sec): 6

4.5.2. SIP Trunk Group

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 155.

```
add trunk-group 155                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 155          Group Type: sip          CDR Reports: y
  Group Name: Avaya SIP phones      COR: 1      TN: 1      TAC: 155
  Direction: two-way      Outgoing Display? y
  Dial Access? n          Night Service:
  Queue Length: 0
Service Type: tie          Auth Code? n
                                     Signaling Group: 150
                                     Number of Members: 10
```

Navigate to **page 3** and enter **private** for **Numbering Format**.

```
add trunk-group 155                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n          Measured: none
                                     Maintenance Tests? y
                                     Numbering Format: private
                                     UI Treatment: service-provider
                                     Replace Restricted Numbers? y
                                     Replace Unavailable Numbers? y
Show ANSWERED BY on Display? Y
```

Navigate to **page 4** and enter **120** for **Telephone Event Payload Type**.

```
add trunk-group 155                                     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: 120
```


4.6. Administer Route Pattern

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 **Section 4.8**. Configure this route pattern to route calls to trunk group number **155** configured in **Section 4.5.2**. Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern.

change route-pattern 150													Page		1 of 3	
Pattern Number: 140 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			
													Intw			
1:	155	0											n	user		
2:												n	user			
3:												n	user			
4:												n	user			
		BCC VALUE		TSC	CA-TSC		ITC BCIE Service/Feature			PARM	No.	Numbering	LAR			
		0	1	2	M	4	W	Request			Dgts	Format				
													Subaddress			
1:	y	y	y	y	y	n	n	rest							none	
2:	y	y	y	y	y	n	n	rest							none	
3:	y	y	y	y	y	n	n	rest							none	
4:	y	y	y	y	y	n	n	rest							none	

4.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration below, all calls originating from a 5-digit extension beginning with 320 will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
5	2			5	Total Administered: 4	
5	4			5	Maximum Entries: 540	
5	8			5		
5	320			5		

4.8. Administer Dial Plan and AAR Analysis

Configure the dial plan for dialing 5-digit extensions beginning with **350** to stations registered with Cisco UCM. Use the **change dialplan analysis** command to define **Dialed String 350** 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						
3		5	ext						
300		5	ext						
350		5	aar						
8		1	fac						
9		1	fac						
*		3	fac						
#		3	fac						

Use the **change aar analysis n** command where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 350** to use **Route Pattern 150**

change aar analysis 350						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all				Percent Full: 2			
	Dialed String	Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
350		5	5	150	aar		n
7		7	7	254	aar		n
8		7	7	254	aar		n
9		7	7	254	aar		n

4.9. Save Changes

Use the **save translation** command to save all changes.

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

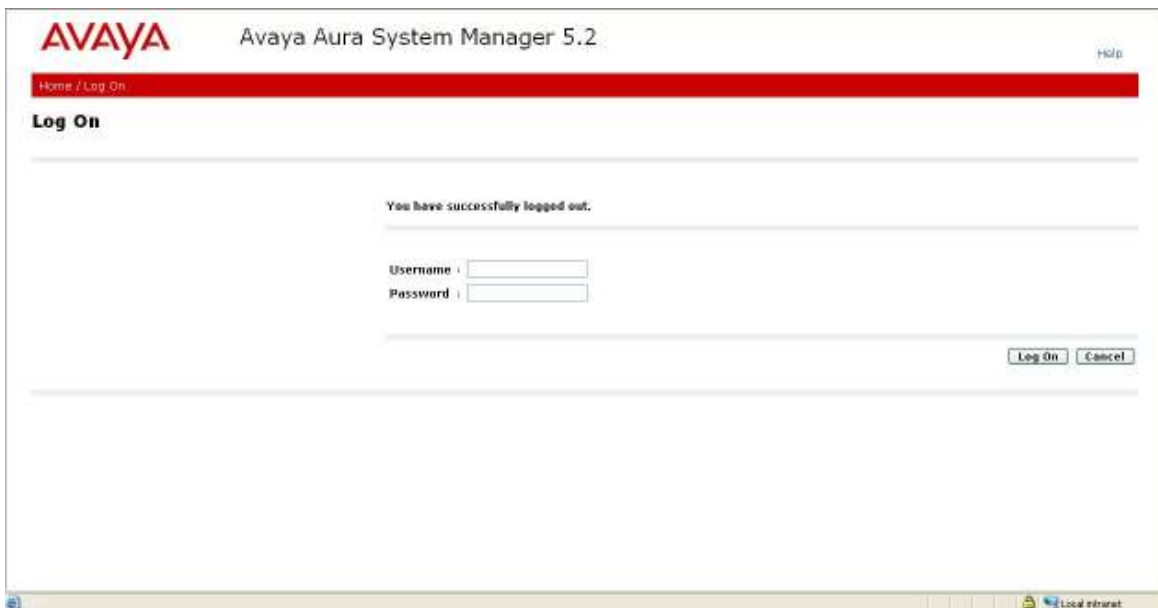
5. Configuring Session Manager

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

- Login to Session Manager
- Administer SIP domain
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Session Manager
- Add Communication Manager as a Feature Server
- Add Users for SIP Phones

5.1. Login to Session Manager

Access the Avaya Aura™ System Manager using a Web Browser and entering *<http://<ip-address>/SMGR>*, where <ip-address> is the IP address of System Manager. Log in using appropriate credentials and accept the subsequent Copyright Legal Notice.



By selecting **Network Routing Policy** from the left panel menu, a short procedure for configuring Network Routing Policy is shown on the right panel.

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura System Manager 5.2', and a user status bar indicating 'Welcome, admin' and 'Last Logged on at Nov. 04, 2009 9:42 PM'. A navigation menu on the left lists various system management functions, with 'Network Routing Policy' highlighted. The main content area, titled 'Introduction to Network Routing Policy (NRP)', provides a step-by-step guide for configuring the NRP. It explains that NRP consists of several applications like 'Domains', 'Locations', 'SIP Entities', etc., and lists a recommended 9-step workflow. The steps include creating domains, locations, adaptations, SIP entities, entity links, time ranges, routing policies, dial patterns, and regular expressions. Each step includes specific instructions and sub-tasks. For example, Step 4 involves creating SIP entities that act as outbound proxies and assigning them to locations and adaptations. Step 7 involves creating routing policies and assigning them to destinations and time of day. Step 8 involves creating dial patterns and assigning them to locations and routing policies. Step 9 involves creating regular expressions and assigning them to routing policies. The page concludes with an important note about the dial pattern driven approach to define routing policies, stating that dial patterns are defined and assigned afterwards with the help of the NRP application 'Dial pattern'.

AVAYA Avaya Aura System Manager 5.2 Welcome, admin Last Logged on at Nov. 04, 2009 9:42 PM Help | Log off

Home / Network Routing Policy

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
Help for Import All Data
Help for Export All Data
Help for Committing configuration changes

Introduction to Network Routing Policy (NRP)

Network Routing Policy consists of several NRP applications like "Domains", "Locations", "SIP Entities", etc.
The recommended order to use the NRP applications (that means the overall NRP workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other NRP applications are referring domains of type SIP).
- 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 "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
 - Align with the tariff information received 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 patterns 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 Policies" 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)

5.2. Administer SIP Domain

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.

Complete the following options:

Name The authoritative domain name (e.g., **silstack.com**)

Notes Description for the domain (optional)

Click **Commit** to save changes.

Verify the domain is created as in screenshot below.



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

5.3. Administer Adaptations

Create an adaptation entry for an incoming call from Cisco UCM. For the Cisco UCM adaptation, enter the following information:

Name CiscoUCM-7, an informative name for the adaptation
Adaptation Module Enter **CiscoAdapter 10.10.5.100**, where 10.10.5.100 is the Cisco UCM IP address.
Digit Conversion for incoming Calls to SM Matching Pattern **350** with a minimum and maximum of **5** digits long, which is the dial pattern for a station registered with Cisco UCM. Delete Digits has value **0** to indicate no digits are to be deleted.

AVAYA Avaya Aura System Manager 5.2

Welcome, admin Last Logged on at Nov 04, 2009 3:42 PM Help | Log off

Home / Network / Routing Policy / Adaptations / Adaptation Details

Asset Management
Communication System 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: Cisco

Adaptation Module: CiscoAdapter 10.10.5.100

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item: Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*350	5	5	0		both	

Select: All, None (0 of 1 Selected)

Digit Conversion for Outgoing Calls from SM

5.4. Administer SIP Entities

A SIP Entity must be added for 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). Enter the following for each SIP Entity:

Under **General**:

Name	An informative name (e.g., SessionManager)
FQDN or IP Address	IP address of the signaling interface on the Session Manager
Type	”Session Manager” for Session Manager, “CM” for Communication Manager, or “Other” for Cisco UCM
Time Zone	Time zone for this location

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a user status bar indicating 'Welcome, admin' and 'Last Logged on at Nov. 11, 2009 8:32 AM'. The left-hand navigation menu is expanded to show 'SIP Entities' under the 'Network Routing Policy' section. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows: 'Name' is 'SessionManager', 'FQDN or IP Address' is '135.64.186.40', 'Type' is 'Session Manager' (selected from a dropdown), 'Notes' is empty, 'Location' is empty, 'Outbound Proxy' is empty, 'Time Zone' is 'Europe/Dublin' (selected from a dropdown), and 'Credential name' is empty. At the bottom, there is a 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located in the top right corner of the form area.

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 Port definitions for the Session Manager SIP Entity.

The screenshot shows a web interface for managing ports. On the left, there is a sidebar with links: "Shortcuts", "Change Password", "Help for SIP Entity Details fields", and "Help for Committing configuration changes". The main area is titled "Port" and has "Add" and "Remove" buttons. Below this is a table with 5 items, showing a list of ports. The table has columns for "Port", "Protocol", "Default Domain", and "Notes". The data rows are:

Port	Protocol	Default Domain	Notes
5060	TCP	sipstack.com	
5061	TLS	sipstack.com	
5062	TLS	sipstack.com	
5063	TCP	sipstack.com	
5064	TLS	sipstack.com	

Below the table, it says "Select: All, None (0 of 5 Selected)". At the bottom right, there are "Commit" and "Cancel" buttons. A note at the bottom left says "* Input Required".

The following screen shows the SIP Entity for Communication Manager.

The screenshot shows the "Avaya Aura™ System Manager 5.2" interface. The top navigation bar includes the Avaya logo, the product name, and a welcome message for user "admin" logged in at 11:20 AM on 11/11/2009. The breadcrumb trail is "Home / Network Routing Policy / SIP Entities / SIP Entity Details". The left sidebar shows a tree view with categories: "Asset Management", "Communication System Management", "User Management", "Monitoring", "Network Routing Policy", "SIP Domains", "SIP Entities" (highlighted), "Time Ranges", "Personal Settings", "Security", "Applications", "Settings", and "Session Manager". The main content area is titled "SIP Entity Details" and has "Commit" and "Cancel" buttons. It is divided into two tabs: "General" and "SIP Link Monitoring". The "General" tab is active, showing fields for: "Name" (AvayaCMcom), "FQDN or IP Address" (135.64.180.6), "Type" (CM), "Notes", "Adaptation", "Location", "Time Zone" (Europe/Dublin), "Override Port & Transport with DNS SRV" (unchecked), "SIP Timer B/F (in seconds)" (4), "Credential name", "Call Detail Recording" (none), and "SIP Link Monitoring" (Use Session Manager Configuration).

The following screen shows the SIP Entity for Cisco UCM.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name, and a user status bar showing 'Welcome, admin' and 'Last Logged on at Nov. 11, 2009 8:32 AM'. A red breadcrumb trail indicates the path: Home / Network Routing Policy / SIP Entities / SIP Entity Details. On the left, a sidebar menu lists various management categories, with 'SIP Entities' highlighted under the 'Network Routing Policy' section. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The configuration form includes fields for 'Name' (CiscoCM), 'FQDN or IP Address' (10.10.5.100), 'Type' (Other), and 'Notes'. Below these are dropdown menus for 'Adaptation' (Cisco), 'Location', and 'Time Zone' (Europe/Dublin). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV', a 'SIP Timer B/F (in seconds)' field set to 4, a 'Credential name' field, and a 'Call Detail Recording' dropdown set to 'none'. At the bottom, the 'SIP Link Monitoring' section has a dropdown set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are located in the top right corner of the form area.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Nov. 11, 2009 8:32 AM Help | Log off

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

SIP Entity Details

Commit Cancel

General

* Name: CiscoCM

* FQDN or IP Address: 10.10.5.100

Type: Other

Notes:

Adaptation: Cisco

Location:

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

5.5. Administer Entity Links

A SIP trunk between a 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). Fill in the following fields in the new row that is displayed.

- Name** An informative name
- SIP Entity 1** Select SessionManager
- Port** Port number to which the other system sends its SIP requests
- SIP Entity 2** The other SIP Entity for this link, created in **Section 5.4**
- Port** Port number to which the other system expects to receive SIP requests
- Trusted** Whether to trust the other system
- Protocol** 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.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar contains a navigation menu with options like Asset Management, Communication System Management, User Management, Monitoring, and Network Routing Policy. The main area is titled 'Entity Links' and contains a table with 8 items. The table columns are Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The rows are: Avaya (SessionManager, TLS, 5002, AvayaCM, 5002, checked), AvayaTdm (SessionManager, TCP, 5063, AvayaCMTdm, 5063, checked), Branch Office (SessionManager, TLS, 5001, Branch CM, 5001, checked), Cisco (SessionManager, TCP, 5060, CiscoCM, 5060, checked), Feature Server (SessionManager, TLS, 5004, feature, 5004, checked), MX-S6200 (SessionManager, UDP, 5065, MX-S6200, 5065, checked, with a link to MX6200), To OCS Mediation (SessionManager, TCP, 5000, Stack OCS Mediation Server, 5000, checked), and VoiceMailMM (SessionManager, TCP, 5060, VoiceMail, 5060, checked). At the bottom, it says 'Select: All, None (0 of 8 Selected)'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
Avaya	SessionManager	TLS	5002	AvayaCM	5002	<input checked="" type="checkbox"/>	
AvayaTdm	SessionManager	TCP	5063	AvayaCMTdm	5063	<input checked="" type="checkbox"/>	
Branch Office	SessionManager	TLS	5001	Branch CM	5001	<input checked="" type="checkbox"/>	
Cisco	SessionManager	TCP	5060	CiscoCM	5060	<input checked="" type="checkbox"/>	
Feature Server	SessionManager	TLS	5004	feature	5004	<input checked="" type="checkbox"/>	
MX-S6200	SessionManager	UDP	5065	MX-S6200	5065	<input checked="" type="checkbox"/>	Link to MX6200
To OCS Mediation	SessionManager	TCP	5000	Stack OCS Mediation Server	5000	<input checked="" type="checkbox"/>	
VoiceMailMM	SessionManager	TCP	5060	VoiceMail	5060	<input checked="" type="checkbox"/>	

5.6. Administer Time Ranges

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. Always)
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 Aura System Manager 5.2 interface. The left sidebar contains a menu with the following items: Asset Management, Communication System Management, User Management, Monitoring, and Network Routing Policy. Under Network Routing Policy, the following items are listed: Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities, Time Ranges (highlighted with a red box), and Personal Settings. The main area is titled 'Time Ranges' and contains a table with the following columns: Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. The table contains two rows: '24/7' and 'always'. The 'always' row is highlighted with a red box. The 'always' row has checkboxes checked for all days of the week (Mo, Tu, We, Th, Fr, Sa, Su) and a Start Time of 00:00 and End Time of 23:59. The Notes column for the 'always' row contains the text 'Time Range 24/7'.

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
24/7	<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	Time Range 24/7
always	<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	

5.7. Administer Routing Policies

Create routing policies to direct how calls will be routed to a system. Two routing policies must be added; one for 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).

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 screen shows the **Routing Policy Details** for Communication Manager.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The left sidebar contains a navigation menu with options like Asset Management, Communication System Management, User Management, Monitoring, and Network Routing Policy. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button. The 'General' tab is active, showing fields for Name (AvayaCMTom), Disabled (unchecked), and Notes. The 'SIP Entity as Destination' tab is also visible, with a 'Select' button. The 'Time of Day' tab shows a table with columns for Name, FQDN or IP Address, Type, and Notes. The table contains one entry: AvayaCMTom, 135.64.186.6, CM. Below the table, there is a 'Time of Day' section with 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. At the bottom, a table shows the policy configuration for '1 Item' with columns for Ranking, Name, and days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). The table shows a policy with Ranking 0, Name always, and active on all days from 00:00 to 23:55.

Name	FQDN or IP Address	Type	Notes
AvayaCMTom	135.64.186.6	CM	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	always								00:00	23:55	

The following screen shows the **Routing Policy Details** for Cisco UCM.

AVAYA Avaya Aura System Manager 5.2 Welcome, **admin** Last Logged on at Nov. 04, 2009 3:42 PM Help | Log off

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

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CiscoCM	10.10.5.100	Other	

Time of Day

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	always	00	00	00	00	00	00	00	00:00	23:59	

5.8. Administer Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, 5-digit extensions beginning with **320** reside on Communication Manager and 5-digit extension beginning with **350** reside on Cisco UCM. For Communication Manager Dial Pattern configuration perform the following. Select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**

Pattern	Dialed number or prefix
Min	Minimum length of dialed number
Max	Maximum length of dialed number
Notes	Comment on purpose of dial pattern
SIP Domain	Select ALL

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. At the top left is the Avaya logo. To its right, the text "Avaya Aura™ System Manager 5.2" is displayed. Further right, a welcome message reads: "Welcome, **admin** Last Logged on at Nov, 11, 2009 3:04 PM". Below this is a "Help | Log off" link. A red breadcrumb trail at the top of the main content area reads: "Home / Network Routing Policy / Dial Patterns / Dial Pattern Details". On the left side, there is a vertical navigation menu with the following items: "Asset Management", "Communication System Management", "User Management", "Monitoring", "Network Routing Policy" (expanded), "Adaptations", "Dial Patterns" (highlighted with a red box), "Entity Links", "Locations", "Regular Expressions", and "Routing Policies". The main content area is titled "Dial Pattern Details" and includes "Commit" and "Cancel" buttons. Under the "General" tab, the following fields are visible: "* Pattern:" with a text box containing "320" (highlighted with a red box); "* Min:" with a text box containing "5" (highlighted with a red box); "* Max:" with a text box containing "5" (highlighted with a red box); "Emergency Call:" with an unchecked checkbox; "SIP Domain:" with a dropdown menu showing "-ALL-" (highlighted with a red box); and "Notes:" with an empty text box.

Navigate to **Originating Locations and Routing Policies** and select **Add** (not shown). Under **Originating Location** select all locations by checking the box next to **ALL** and under **Routing Policies** select a Routing Policy by checking the box next to **AvayaCMtom**. Click **Select** button to confirm the chosen options. You will then be returned to the Dial Pattern screen (shown above), select **Commit** button to save.

Originating Location and Routing Policy List Select Cancel

Originating Location

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	-ALL-	Any Locations
<input type="checkbox"/>	Avaya	
<input type="checkbox"/>	Cisco	
<input type="checkbox"/>	Stack Enterprise	Main Office for Stack Testing

Select : All, None (0 of 4 Selected)

Routing Policies

8 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	AvayaCM	<input type="checkbox"/>	AvayaCM	
<input checked="" type="checkbox"/>	AvayaCMtom	<input type="checkbox"/>	AvayaCMtom	
<input type="checkbox"/>	BranchCM	<input type="checkbox"/>	Branch CM	Branch CM
<input type="checkbox"/>	CiscoCM	<input type="checkbox"/>	CiscoCM	

To configure Cisco UCM Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**

Pattern	Dialed number or prefix
Min	Minimum length of dialed number
Max	Maximum length of dialed number
Notes	Comment on purpose of dial pattern
SIP Domain	Select ALL

The screenshot displays the Avaya Aura System Manager 5.2 web interface. At the top left is the Avaya logo. To its right, the text 'Avaya Aura™ System Manager 5.2' is displayed. In the top right corner, a welcome message reads: 'Welcome, admin Last Logged on at Nov, 11, 2009 3:04 PM' with links for 'Help' and 'Log off'. A red breadcrumb trail at the top of the main content area shows the path: 'Home / Network Routing Policy / Dial Patterns / Dial Pattern Details'. On the left side, there is a vertical navigation menu with several categories: 'Asset Management', 'Communication System Management', 'User Management', 'Monitoring', and 'Network Routing Policy'. The 'Network Routing Policy' category is expanded, showing sub-items: 'Adaptations', 'Dial Patterns' (which is highlighted with a red box), 'Entity Links', 'Locations', 'Regular Expressions', 'Routing Policies', and 'SIP Domains'. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible: '* Pattern:' with a text box containing '350' (highlighted with a red box), '* Min:' with a text box containing '5' (highlighted with a red box), '* Max:' with a text box containing '5' (highlighted with a red box), 'Emergency Call:' with an unchecked checkbox, 'SIP Domain:' with a dropdown menu showing '-ALL-' (highlighted with a red box), and 'Notes:' with an empty text box.

Navigate to **Originating Locations and Routing Policies** and select **Add** (not shown). Under **Originating Location** select **ALL** and under **Routing Policies** select **CiscoCM**. Click **Select** button to confirm the chosen options. You will then be returned to the Dial Pattern screen (shown above), select **Commit** button to save.

- Asset Management
- Communication System 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

Originating Location and Routing Policy List

Select

Cancel

Originating Location

4 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	-ALL-	Any Locations
<input type="checkbox"/>	Avaya	
<input type="checkbox"/>	Cisco	
<input type="checkbox"/>	Stack Enterprise	Main Office for Stack Testing

Select : All, None (0 of 4 Selected)

Routing Policies

8 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	AvayaCM	<input type="checkbox"/>	AvayaCM	
<input type="checkbox"/>	AvayaCMtom	<input type="checkbox"/>	AvayaCMtom	
<input type="checkbox"/>	BranchCM	<input type="checkbox"/>	Branch CM	Branch CM
<input type="checkbox"/>	CiscoCM	<input type="checkbox"/>	CiscoCM	

5.9. Administer Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the Session Manager menu on the left and select **Session Manager Administration**. Then click **Add** and fill in the fields as described below and shown in the following screen:

Under **General**:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP** Enter the IP address of the Session Manager management interface.

Under **Security Module**:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

5.10. Add Communication Manager as a Feature Server

In order for Communication Manager to provide configuration and Feature Server support to SIP phones when they register to Session Manager, Communication Manager must be added as an application.

5.10.1. Create an Application Entity

Select **Applications** → **Entities** on the left. Click on **New** (not shown). Enter the following fields and use defaults for the remaining fields:

Name	A descriptive name
Type	Select CM
Node	Select Other.. and enter the IP address for CM SAT access

The screenshot shows the Avaya Aura System Manager 5.2 web interface. The left sidebar contains a navigation menu with the following items: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, Security, Applications (expanded), and Settings. Under the 'Applications' section, the following items are listed: FRM, MSA, HMC, Session Manager 5.2, SMGR, SIP AS 8.0, and **Entities** (highlighted with a red box). The main content area is titled 'New CM Instance' and includes a 'Commit' button and a 'Cancel' button. Below the title, there are tabs for 'Application', 'Port', 'Access Point', and 'Attributes', with 'Application' selected. The 'Application' tab contains the following fields: 'Name' (set to 'EnterpriseCM'), 'Type' (set to 'CM' with a 'Reset' button), 'Description' (empty text area), and 'Node' (set to '135.64.186.10').

Navigate to the **Attributes** section and enter the following:

Login	Login used for SAT access
Password	Password used for SAT access
Confirm Password	Password used for SAT access

Click on **Commit** to save.

Attributes *

* Login

Password

Confirm Password

Is SSH Connection ☒

* Port 5022

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Alternate IP Address

Is ASG Enabled ☐

ASG Key

Confirm ASG Key

Location

* Required

Commit Cancel

5.10.2. Create a Feature Server Application

Select **Session Manger** → **Application Configuration** → **Applications** on the left. Click on **New** (not shown). Enter following fields and use defaults for the remaining fields:

Name A descriptive name

SIP Entity Select the CM SIP Entity defined in **Section 5.4**

Click on **Commit** to save.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar contains a navigation tree with 'Session Manager' expanded and 'Applications' selected. The main area is titled 'Application Editor'. It has a 'Name' field with 'Feature' entered, a 'SIP Entity' dropdown menu showing 'AvayaCMTom', and a 'Description' field. Below these is an 'Application Attributes (optional)' section with a table for 'Name' and 'Value'. At the bottom right are 'Commit' and 'Cancel' buttons.

5.10.3. Create a Feature Server Application Sequence

Select **Session Manager** → **Application Configuration** → **Application Sequences** on the left. Click on **New** (not shown). Enter a descriptive **Name**. Click on the + sign next to the appropriate **Available Applications** and they will move up to the **Applications in this Sequence** section. Click on **Commit** to save.

The screenshot shows the Avaya Aura System Manager 5.2 'Application Sequence Editor' interface. The left sidebar shows 'Application Sequences' selected. The main area has a 'Sequence Name' section with a 'Name' field containing 'App Sequence'. Below is a table titled 'Applications in this Sequence' with one item: 'Feature' (SIP Entity: feature, Mandatory: checked). At the bottom is an 'Available Applications' section with a table containing 'Feature' (SIP Entity: feature). A red box highlights the '+' icon next to 'Feature' in the 'Available Applications' table. 'Commit' and 'Cancel' buttons are at the top right.

5.10.4. Synchronize CM Data

Select **Communications System Management** → **Telephony** on the left. Select the appropriate **Element Name**. Select **Initialize data for selected devices**. Then click on **Now**. This may take some time. Use the menus on the left under **Monitoring** → **Scheduler** to determine when the task is complete.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Nov. 16, 2009 1:32 PM Help | Log off

Home / Communication System Management / Telephony / System

Synchronize CM Data and Configure Options

Synchronize CM Data/Launch Element Cut Through / Configuration Options | Expand All | Collapse All

Synchronize CM Data/Launch Element Cut Through *

1 Item Refresh	Filter: Enable						
<input checked="" type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
<input checked="" type="checkbox"/>	EnterpriseCM	135.64.186.10	Nov 16, 2009 02:00:26 AM +0000	Incremental	Failed		R015x.02.1.0t6.4

Select: All, None (1 of 1 Selected)

☒ Initialize data for selected devices
☐ Incremental Sync data for selected devices

Now Schedule Cancel Launch Element Cut Through

5.11. Add Users for SIP Phones

Users must be added via Session Manager and the details will be updated on the CM. Select **User Management** → **User Management** on the left. Then click on **New** (not shown). Enter a first **Name** and **Last** name.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Nov. 16, 2009 1:33 PM Help | Log off

Home / User Management / User Management / New User

New User Profile Commit Cancel

General | Identity | Communication Profile | Roles | Override Permissions | Group Membership | Attribute Sets | Default Contact List | Private Contacts | Expand All | Collapse All

General *

* Last Name: phelan
* First Name: tom
Middle Name:
Description:

User Type:
☐ administrator
☐ communication_user
☐ agent
☐ supervisor
☐ resident_expert
☐ service_technician
☐ lobby_phone

Navigate to the **Identity** section and enter the following and use defaults for other fields:

Login Name

The desired phone extension number
@domain.com where domain was defined
in **Section 5.2**

Password

Password for user to log into SMGR

Shared Communication Profile Password

Password to be entered by the user when
logging into the phone.

The screenshot shows a web form titled "Identity" with a dropdown arrow. The form contains the following fields:

- * Login Name:** A text input field containing "32007@csilstack.com".
- * Authentication Type:** A dropdown menu set to "Basic".
- SMGR Login Password:**
 - * Password:** A text input field containing "*****".
 - * Confirm Password:** A text input field containing "*****".
- Shared Communication Profile Password:**
 - * Password:** A text input field containing "*****".
 - Confirm Password:** A text input field containing "*****".
- Localized Display Name:** A text input field.
- Endpoint Display Name:** A text input field.
- Honorable:** A text input field.
- Language Preference:** A dropdown menu.
- Time Zone:** A dropdown menu.

Navigate to and click on **Communication Profile** section to expand. Then click on **Communication Address** to expand that section. Enter the following and defaults for the remaining fields:

Type Select **SIP**
SubType Select **Username**
Fully Qualified Address Enter the extension number

Click on **Add**.

The screenshot shows two configuration windows. The top window, titled "Communication Profile", has buttons for "New", "Delete", "Done", and "Cancel". It contains a table with one row labeled "Primary" and a "Select : None" dropdown. Below the table, the "Name" field is set to "Primary" and the "Default" checkbox is checked. The bottom window, titled "Communication Address", has buttons for "New", "Edit", and "Delete". It features a table with columns "Type", "SubType", "Handle", and "Domain", which currently shows "No Records found". Below the table, the "Type" dropdown is set to "sip", the "SubType" dropdown is set to "username", and the "Fully Qualified Address" field contains "32007" and "sistack.com". The "Add" button is highlighted with a red box.

Communication Profile

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default: ☒

Communication Address

New Edit Delete

Type	SubType	Handle	Domain
No Records found			

Type: sip

SubType: username

* Fully Qualified Address: 32007 sistack.com

Add Cancel

Navigate to and click on **Session Manager** section to expand. Select the appropriate Session Manager server for **Session Manager Instance**. For **Origination Application Sequence** and **Termination Application Sequence** select the application sequence created in **Section 5.10.3**. Click on **Station Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

System	Select the CM Entity
Extension	Enter a desired extension number
Template	Select a telephone type template
Port	Select IP

Click on **Commit** to save (not shown).

The screenshot displays a web-based configuration interface for Session Manager. The 'Session Manager' section is expanded, showing fields for 'Session Manager Instance' (set to 'SessionManager'), 'Origination Application Sequence' (set to 'App_sequence'), and 'Termination Application Sequence' (set to 'App_sequence'). Below this, the 'Messaging Profile' section is collapsed. The 'Station Profile' section is expanded, showing fields for 'System' (set to 'EnterpriseCM'), 'Use Existing Stations' (unchecked), 'Extension' (set to '32007'), 'Template' (set to 'DEFAULT_96505IP'), 'Set Type' (set to '96505IP'), 'Security Code' (empty), 'Port' (set to 'IP'), and 'Delete Station on Unassign of Station from User' (unchecked). Red boxes highlight the 'Session Manager', 'Station Profile', and the specific field values mentioned in the text.

6. Configure Cisco UCM

This section provides the procedures for configuring Cisco UCM. 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]. The procedures include configuration of the following items:

- Login to Cisco UCM
- Administer SIP Trunk Security Profile
- Administer SIP Trunk
- Administer Route Pattern
- Administer Phone

6.1. Login to Cisco UCM

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.



6.2. Administer SIP Trunk Security Profile

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 screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified CM Administration", and a navigation dropdown menu set to "Cisco Unified CM Administration". Below this is a secondary navigation bar with links for "interop", "About", and "Logout". A main navigation menu contains various system categories like "System", "Call Routing", "Media Resources", etc. The current page is titled "Find and List SIP Trunk Security Profiles". It features a toolbar with icons for "Add New", "Select All", "Clear All", and "Delete Selected". A status box indicates "2 records found". The main content area shows a table of SIP Trunk Security Profiles. The first row is "Non Secure SIP Trunk Profile" with a description "Non Secure SIP Trunk Profile authenticated by null String". At the bottom, there is a row of buttons: "Add New", "Select All", "Clear All", and "Delete Selected". The "Add New" button is highlighted with a red rectangle.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

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 SIP Trunk Security Profiles

+ Add New Select All Clear All Delete Selected

Status
2 records found

SIP Trunk Security Profile (1 - 2 of 2) Rows per Page: 50






Find SIP Trunk Security Profile where Name ▾ begins with ▾ Find Clear Filter + -


<input type="checkbox"/>	Name ^	Description	Copy
<input type="checkbox"/>	Non Secure SIP Trunk Profile	Non Secure SIP Trunk Profile authenticated by null String	

Add New Select All Clear All Delete Selected

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

SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Add New

 Status: Ready

SIP Trunk Security Profile Information

Name*

Avaya CM

Description

SIP connection to CM Silstack

Device Security Mode

Non Secure

▼

Incoming Transport Type*

TCP+UDP

▼

Outgoing Transport Type

TCP

▼

☐ Enable Digest Authentication

Nonce Validity Time (mins)*

600

X.509 Subject Name

Incoming Port*

5060

☐ Enable Application Level Authorization

☒ Accept Presence Subscription

☒ Accept Out-of-Dialog REFER

☒ Accept Unsolicited Notification

☒ Accept Replaces Header

☐ Transmit Security Status

Save

Delete

Copy

Reset

Add New

6.3. Administer SIP Trunk

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

The screenshot shows the 'Find and List Trunks' page in the Cisco Unified CM Administration interface. The top navigation bar includes 'Cisco Unified CM Administration' and 'For Cisco Unified Communications Solutions'. Below the navigation bar, there are tabs for 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'Device' tab is selected. The main content area is titled 'Find and List Trunks' and contains a search bar with the text 'Find Trunks where Device Name begins with'. Below the search bar, there is a message: 'No active query. Please enter your search criteria using the options above.' The 'Add New' button is highlighted with a red box.

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 top navigation bar is the same as the previous screenshot. The main content area is titled 'Trunk Configuration' and contains a 'Next' button. Below the 'Next' button, there is a 'Status' section showing 'Status: Ready'. The 'Trunk Information' section contains two dropdown menus: 'Trunk Type*' set to 'SIP Trunk' and 'Device Protocol*' set to 'SIP'. The 'Next' button is highlighted with a red box. A legend at the bottom indicates that '*' indicates a required item.

Enter the appropriate information for the SIP Trunk. The following screen shows the configuration used in the sample network.

Device Name	An informative name
Description	Any note for this trunk
Remote-Party-Id	Checked to send
Asserted-Identity	Checked to send caller information
Asserted-Type	Select PAI for P-Asserted-Identity

Device Information

Product: SIP Trunk

Device Protocol: SIP

Device Name: ASM-Sistack

Description: To SM100

Device Pool: Default

Common Device Configuration: < None >

Call Classification: Use System Default

Media Resource Group List: DublinSIL-A

Location: Hub_None

AAR Group: < None >

Packet Capture Mode: None

Packet Capture Duration: 0

☐ Media Termination Point Required

☒ Retry Video Call as Audio

☐ Transmit UTP-6 for Calling Party Name

☐ Unattended Port

☐ SKTP 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: PAI

SIP Privacy: Default

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

Navigate to SIP Information section and enter following configuration:

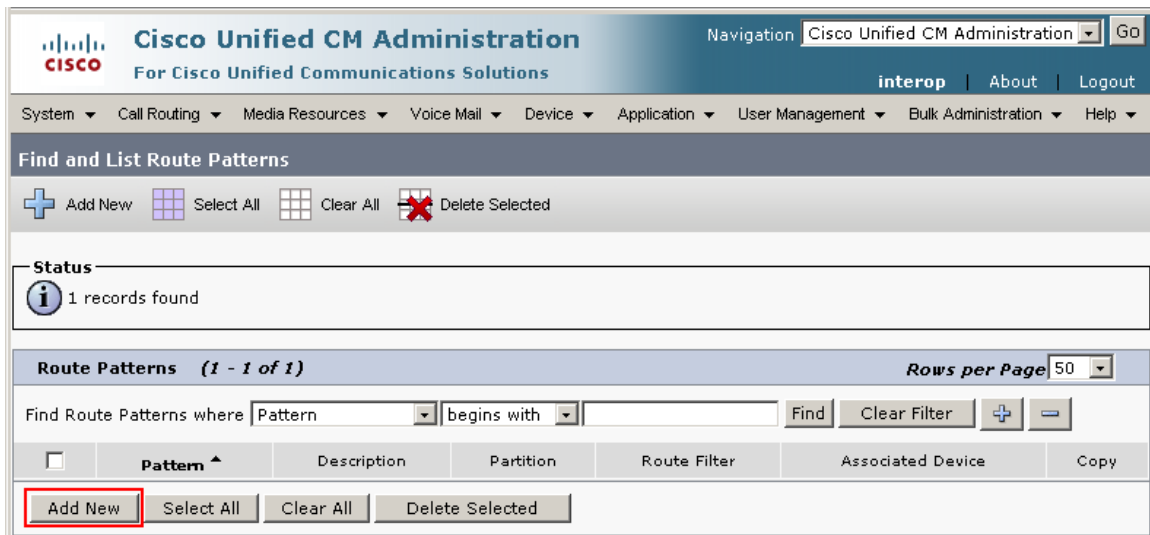
Destination Address	IP address of the Session Manager
Destination Port	Destination port number use for SIP communication
SIP Trunk Security Profile	Profile configured at Section 6.2
DTMF Signaling Method	Select RFC 2833



Click **Save** to complete.

6.4. Administer Route Pattern

Select **Call Routing** → **Route/Hunt** → **Route Pattern** then click **Add New** to add a new route pattern for extension 300xx which are for telephones registered with Communication Manager.



The following screen shows the route pattern used in the sample network. The route pattern **320xx** will cause all 5 digit calls beginning with 320 to be routed through the **ASM-Silstack** SIP Trunk defined in **Section 6.3**. 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

Route Pattern Configuration

Save X Delete Copy Add New

Related Links: Back To Find/Use

Status
Status: Ready

Pattern Definition

Route Pattern* 320xx
Route Partition < None >
Description To AvayaCM
Numbering Plan -- Not Selected --
Route Filter < None >
MPP Precedence* Default
Resource Priority Namespace Network Domain < None >
Gateway/Route List* ASM-Silstack (Edit)
Route Option
Route this pattern
Block this pattern No Error
Call Classification* OffNet
Allow Device Override ☐ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority
Require Forced Authentication Code ☐
Authorization Level* 0
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* 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
Prefix Digits (Outgoing Calls)
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
Network Service -- Not Selected -- Service Parameter Name -- Not Selected -- Service Parameter Value

Save Delete Copy Add New

6.5. Administer Phone

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 screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes links for System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled "Phone Configuration" and shows the status of a selected device as "Ready". Below this, there are two main sections: "Association Information" and "Phone Type". The "Association Information" section lists several lines, with the first line, "Line 1: 35000 (no partition)", highlighted. The "Phone Type" section shows the product type as "Cisco 7911" and the device protocol as "SIP".

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

The screenshot shows the Cisco Unified CM Administration interface for the "Directory Number Configuration" page. The top navigation bar is the same as the previous screenshot. The main content area is titled "Directory Number Configuration" and shows the status of the selected line as "Ready". Below this, there are several sections: "Directory Number Information", "Directory Number Settings", and "AAR Settings". The "Directory Number Information" section contains fields for "Directory Number", "Route Partition", "Description", "Alerting Name", and "ASCII Alerting Name". The "Alerting Name" and "ASCII Alerting Name" fields are highlighted. The "Directory Number Settings" section contains fields for "Voice Mail Profile", "Calling Search Space", "Presence Group", "User Hold MOH Audio Source", "Network Hold MOH Audio Source", and "Auto Answer". The "AAR Settings" section contains fields for "AAR", "Voice Mail", "AAR Destination Mask", and "AAR Group".

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 SEP0023049C0078

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 SEP0023049C0078

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 SEP0023049C0078



☒ Caller Name

☒ Caller Number

☒ Redirected Number

☒ Dialed Number

Users Associated with Line

	Full Name	User ID	Permission
	SIP_Cisco	CiscoSIP	

Associate End Users

7. Verification

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

7.1. Communication Manager

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 155

                                TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                Busy

0155/001 T00036    in-service/idle    no
0155/002 T00037    in-service/idle    no
0155/003 T00038    in-service/idle    no
0155/004 T00039    in-service/idle    no
0155/005 T00040    in-service/idle    no
0155/006 T00041    in-service/idle    no
0155/007 T00042    in-service/idle    no
0155/008 T00043    in-service/idle    no
0155/009 T00044    in-service/idle    no
0155/010 T00045    in-service/idle    no
```

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 150

                                STATUS SIGNALING GROUP

Group ID: 150                      Active NCA-TSC Count: 0
Group Type: sip                    Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service
```

7.2. Session Manager

Select **Session Manager** → **System Status** → **SIP Entity Monitoring**. Verify as shown below that none of the SIP entities for Avaya or Cisco links are down, indicating that they are all reachable for routing.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar contains a navigation menu with categories like Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, Security, Applications, Settings, and Session Manager. The Session Manager section is expanded, showing options like Session Manager Administration, Network Configuration, Device and Location Configuration, Application Configuration, and System Status. The System Status section is further expanded, showing System Status Administration, SIP Entity Monitoring (which is selected), Managed Bandwidth Usage, Security Module Status, Data Replication Status, Registration Summary, and User Registrations.

The main content area displays the **SIP Entity Link Monitoring Status Summary**. It includes a sub-header **Entity Link Status for All Session Manager Instances** and a **Refresh** button. Below this is a table with the following data:

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
SessionManager	0/6	0	0	0

Below the table, there is a section titled **All Monitored SIP Entities** with a **Refresh** button. It shows a list of 8 items with a **Filter: Enable** button. The list includes the following SIP Entity Names:

- AvayaCM
- AvayaCMom
- Branch CM
- CiscoCM
- feature
- MX-R6200
- Stack OCS Mediation Server
- VoiceMail

Click on the SIP Entity Names AvayaCMtom and CiscoCM, shown in the previous screen, and verify that the connection status is **Up**, as shown in screenshots below.

The screenshot shows the Avaya Aura System Manager 5.2 web interface. The left sidebar contains a navigation menu with categories like Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, Security, Applications, and Settings. Under 'Session Manager', 'SIP Entity Monitoring' is highlighted. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a sub-header 'All Entity Links to SIP Entity: AvayaCMtom'. Below this, there are 'Refresh' and 'Summary View' buttons. A table displays the connection status for one item, 'SessionManager', with columns for Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The 'Conn. Status' and 'Link Status' are both 'Up'.

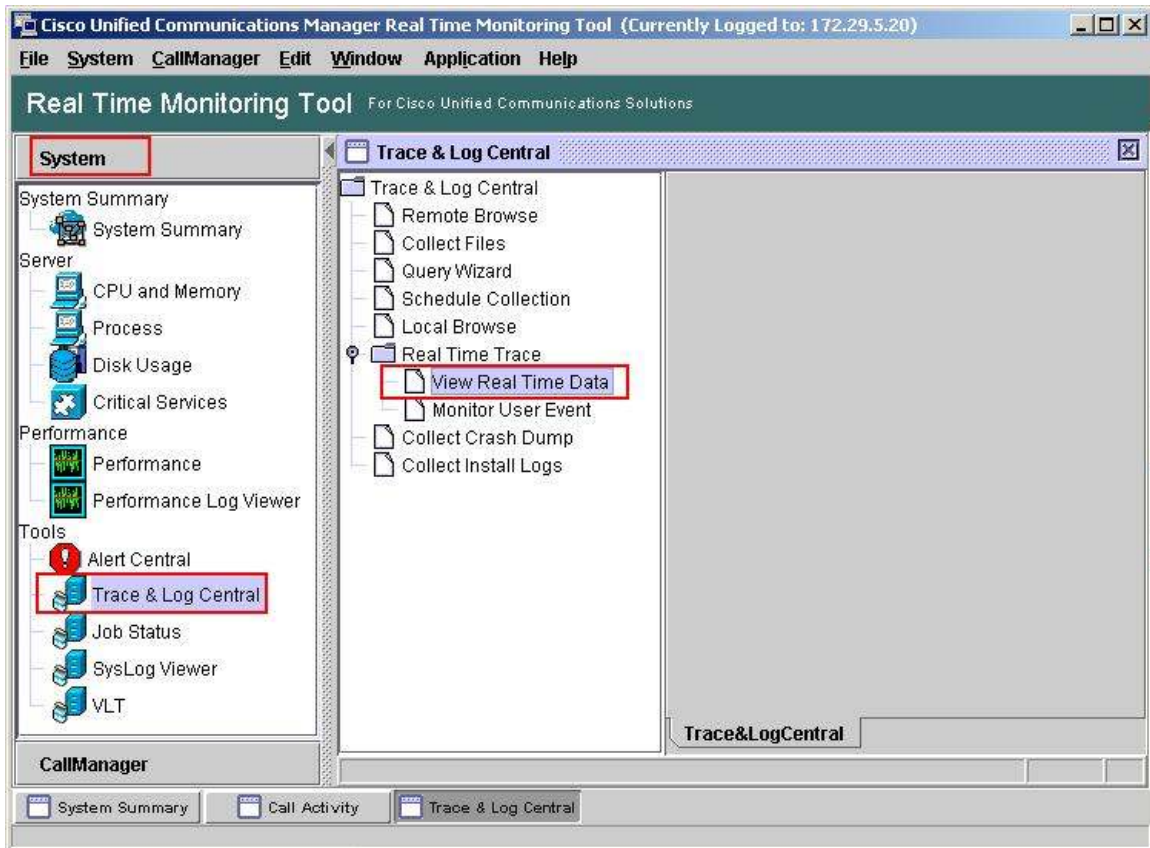
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SessionManager	135.64.186.6	5063	TCP	Up	200 OK	Up

This screenshot is similar to the one above, but it shows the status for 'CiscoCM'. The sub-header is 'All Entity Links to SIP Entity: CiscoCM'. The table shows the connection status for 'SessionManager' with a resolved IP of 10.10.5.100. The 'Conn. Status' and 'Link Status' are both 'Up'.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SessionManager	10.10.5.100	5060	TCP	Up	200 OK	Up

7.3. Cisco Unified Communications Manager

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 [8]. The following screen shows where users can view and perform real time data capture.



7.4. Verified Scenarios

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

- Basic calls between various telephones on Communication Manager and Cisco UCM can be made in both directions using G.711MU, G.729, and G.729AB. For G.729 interoperability, the IP codec set on 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 are shown below.
 - Unattended transfer
 - Attended transfer
 - Hold/Unhold
 - Consultation hold
 - Call forwarding
 - Conference

8. 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 observed:

- For G.729 interoperability, make sure both G.729 and G729AB are part of the audio codec selection in Communication Manager.
- For proper displaying of calling party information, Cisco UCM must be configured with the Internal Caller ID name as described in **Section 6.5**.
- With Music-On-Hold service enabled on Cisco UCM, an issue with call hold was observed. Pressing call hold button on SCCP phone caused the call to an Avaya phone to drop. A workaround is to disable Music-On-Hold service on Cisco for SCCP phones.

9. Additional References

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

- [1] *Avaya AuraTM Session Manager Overview*, Doc # 03-603323, Issue 2
- [2] *Administering Avaya AuraTM Session Manager*, Doc # 03-603324, Issue 2
- [3] *Maintaining and Troubleshooting Avaya AuraTM Session Manager*, Doc # 03-603325, Issue 2
- [4] *SIP Support in Avaya AuraTM Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 9
- [5] *Administering Avaya AuraTM Communication Manager*, Doc # 03-300509, Issue 5.0

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

©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 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