



Avaya Solution & Interoperability Test Lab

Configuring Polycom HDX SIP Video Endpoints with Avaya Aura® Release 6.2 FP2, Avaya Aura® Session Manager Release 6.3 and Avaya Aura® Communication Manager Evolution Server Release 6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration of the Polycom HDX SIP Video Endpoints with Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server.

- Avaya Aura® Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura® Communication Manager operates as an Evolution Server for the SIP endpoints which communicate with Avaya Aura® Session Manager over SIP trunks.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

Table of Contents:

1.	Introduction.....	4
1.1.	Equipment and Software Validated.....	5
2.	Configuring Avaya Aura® Communication Manager Evolution Server.....	5
2.1.	Verify System Capabilities and Licensing.....	5
2.1.1.	SIP Trunk Capacity Check.....	6
2.2.	Add Node Name of Avaya Aura® Session Manager.....	6
2.3.	Configure Codec Type.....	6
2.4.	Configure IP Network Region.....	7
2.5.	Add SIP Signaling Group.....	8
2.6.	Add SIP Trunk Group.....	9
2.7.	Administering Numbering Plan.....	11
2.8.	Configure Stations.....	12
2.9.	Configure Off-PBX-Telephone Station-Mapping.....	14
2.10.	Save Translations.....	14
3.	Configure Avaya Aura® Session Manager.....	15
3.1.	Administer SIP Domains.....	15
3.2.	Define Locations.....	16
3.3.	Add Avaya Aura® Communication Manager Evolution Server.....	17
3.3.1.	Define SIP Entity for Avaya Aura® Communication Manager Evolution Server.....	17
3.3.2.	Define Entity Links for Avaya Aura® Communication Manager Evolution Server.....	18
3.3.3.	Define Routing Policy for Avaya Aura® Communication Manager Evolution Server.....	18
3.3.4.	Define Applications for Avaya Aura® Communication Manager Evolution Server.....	19
3.3.5.	Define Application Sequences for Avaya Aura® Communication Manager Evolution Server.....	20
3.3.6.	Define Avaya Aura® Communication Manager Evolution as an Administrable Entity.....	21
3.3.7.	Add SIP Users.....	22
4.	Configure Polycom HDX SIP Endpoint.....	26
5.	Verification Steps.....	28
5.1.	Verify Avaya Aura® Session Manager Configuration.....	28
5.1.1.	Verify Avaya Aura® Session Manager is Operational.....	28
5.1.2.	Verify SIP Link Status.....	30

5.1.3. Verify Registrations of SIP Endpoints.....	31
5.2. Verify Avaya Aura® Communication Manager Evolution Server Configuration.....	32
5.3. Call Scenarios Verified	36
6. Acronyms.....	37
7. Conclusion.....	37
8. Additional References.....	37

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura® Session Manager to support registration of Polycom HDX (4002, 8006, 9004) SIP Video endpoints and enables connectivity to Avaya Aura® Communication Manager Evolution Server R6.3 using SIP trunks.

As shown in **Figure 1**, Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. Polycom HDX Video Endpoints configured as SIP endpoints utilize the Avaya Aura® Session Manager User Registration feature and Avaya Aura® Communication Manager operating as an Evolution Server. Communication Manager Evolution Server is connected to Session Manager via a SIP signaling group and associated SIP trunk group.

For the sample configuration, Avaya Aura® Session Manager runs on an Avaya S8800 Server. Avaya Aura® Communication Manager 6.3 Evolution Server runs on a S8800 server with an Avaya 450 Gateway. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura® Communication Manager 6.3.

These Application Notes will focus on the configuration of Communication Manager Evolution Server and Session Manager. Detailed administration of Communication Manager Feature Server will not be described (see the appropriate documentation listed in **Section 8**).

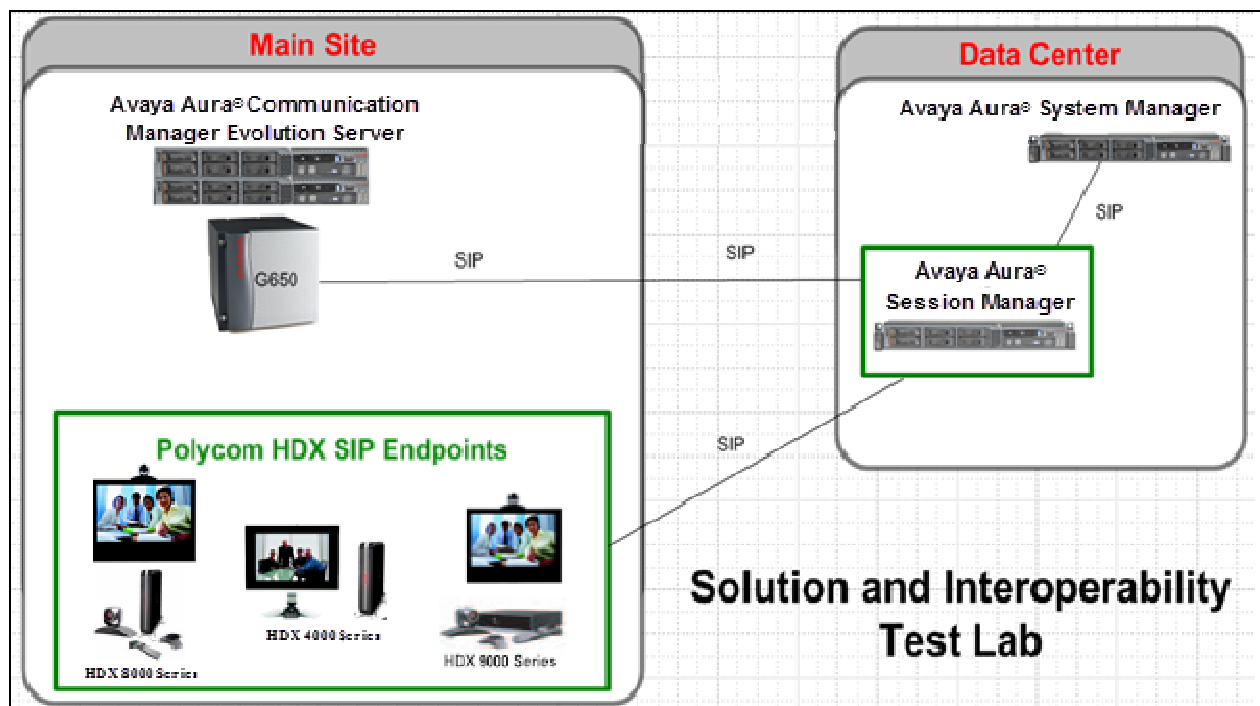


Figure 1 – Sample Configuration

1.1. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Equipment	Software
Avaya Aura [®] Session Manager	Release 6.3 - 6.3.2.0.84005
Avaya Aura [®] System Manager	Release 6.2 FP2 - 6.3.2.3.1275 System Platform – 6.3.0.0.17001
Avaya Aura [®] Communication Manager • Avaya S8800 Server Evolution Server	Release R016x.03.0.121.0 System Platform – 6.3.0.0.16001
Polycom HDX Video Endpoints (SIP): • 4002 • 8006 • 9004	3.0.4-20259 3.0.4-20259 3.0.4-20259

2. Configuring Avaya Aura[®] Communication Manager Evolution Server

This section describes the administration of Communication Manager Evolution Server using a System Access Terminal (SAT). Alternatively, some of the station administration could be performed using the Communication System Management application on System Manager. These Application Notes assume that basic Communication Manager administration, including PROCR, CLAN, Media Processor, Dial Plan, ARS/AAR, and Route Patterns, etc., have already been performed. Some administration screens have been abbreviated for clarity.

- Verify System Capabilities and Communication Manager Licensing
- Administer IP node names
- Administer codec type
- Administer IP network region
- Administer SIP signaling group
- Administer SIP trunk group
- Administer numbering plan
- Administer station endpoints
- Administer off-pbx-telephone station-mapping
- Save translations

After completing these steps, the **save translation** command should be performed.

2.1. Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities and licensing have been configured. If there is insufficient capacity or a required feature is not available, contact an authorized Avaya sales representative to make the appropriate changes.

2.1.1. SIP Trunk Capacity Check

Issue the **display system-parameters customer-options** command to verify that an adequate number of video capable stations, IP Softphones, and SIP trunk members are licensed for the system as shown below:

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	398	
Maximum Concurrently Registered IP Stations:		18000	8	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		414	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		41000	31	
Maximum Video Capable IP Softphones:		18000	118	
Maximum Administered SIP Trunks:		24000	2646	
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	130	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	
Maximum TN2501 VAL Boards:		128	1	
Maximum Media Gateway VAL Sources:		250	0	
Maximum TN2602 Boards with 80 VoIP Channels:		128	0	
Maximum TN2602 Boards with 320 VoIP Channels:		128	9	
Maximum Number of Expanded Meet-me Conference Ports:		300	0	
(NOTE: You must logoff & login to effect the permission changes.)				

2.2. Add Node Name of Avaya Aura® Session Manager

Using the **change node-names ip** command, add the node-name and IP for the Session Manager's software asset, if not previously added.

change node-names ip		Page	1 of	2
IP NODE NAMES				
Name	IP Address			
default	0.0.0.0			
procr	192.168.1.1			
procr6	::			
silasm4	192.168.1.2			

2.3. Configure Codec Type

Issue the **change ip-codec-set n** command where “n” is the next available number. Enter the following values:

- **Audio Codec:** Enter “**SIREN14-32k**”, “**G.722-64k**”, and “**G.711MU**” as supported types of **Audio Codecs**
- **Silence Suppression:** Retain the default value “n”.
- **Frames Per Pkt:** Enter “**1**” or “**2**” (contact system administration for details)
- **Packet Size (ms):** Enter “**20**”.

```
change ip-codec-set 1                                     Page 1 of 2
                                     IP Codec Set
```

```
Codec Set: 1
```

	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1:	SIREN14-32K		1	20
2:	G.722-64K		2	20
3:	G.711MU	n	2	20

On page 2 enter “y” for **Allow Direct-IP Multimedia**. Set the **Maximum Call Rate for Direct-IP Multimedia** and **Maximum Call Rate for Priority Direct-IP Multimedia** values to values that meet your criteria.

```
change ip-codec-set 1                                     Page 2 of 2
                                     IP Codec Set
```

```

                                     Allow Direct-IP Multimedia? y
                                     Maximum Call Rate for Direct-IP Multimedia: 1920:Kbits
                                     Maximum Call Rate for Priority Direct-IP Multimedia: 1920:Kbits
```

	Mode	Redundancy
FAX	relay	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

2.4. Configure IP Network Region

Using the **change ip-network-region 1** command set the **Authoritative Domain**. For the sample configuration “dr.avaya.com” was used. Verify the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields are set to **yes**.

```
change ip-network-region 1                               Page 1 of 20
                                     IP NETWORK REGION
```

```

Region: 1
Location: 1      Authoritative Domain: dr.avaya.com
Name: CMES-Video
MEDIA PARAMETERS
  Codec Set: 1
  UDP Port Min: 2048
  UDP Port Max: 16585
                                     Intra-region IP-IP Direct Audio: yes
                                     Inter-region IP-IP Direct Audio: yes
                                     IP Audio Hairpinning? n
```

2.5. Add SIP Signaling Group

Issue the **add signaling-group n** command, where “n” is an available signaling group number, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. In the sample configuration, trunk group “10” and signaling group “1” were used to connect to Avaya Aura® Session Manager.

- **Group Type:** “sip”
- **Transport Method:** ”tcp”
- **IP Video?:** “y”
- **Peer Detection Enabled?:** “y”
- **Peer Server:** Use default value. **Note:** default value is replaced with “SM” after SIP trunk to Session Manager is established
- **Near-end Node Name:** procr from **Section 2.2**
- **Far-end Node Name:** Session Manager node name from **Section 2.2**
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”
- **Far-end Domain:** Authoritative Domain from **Section 2.4**
- **Enable Layer 3 Test:** “y”
- **Initial IP-IP Direct Media?:** “y”

```
display signaling-group 10                                     Page 1 of 1
SIGNALING GROUP
Group Number: 10          Group Type: sip
IMS Enabled? n           Transport Method: tcp
Q-SIP? n
IP Video? y              Priority Video? y          Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers?y
Remove '+'from Incoming Called/Calling/Alerting/Diverting/Connected Numbers?n
Near-end Node Name: procr          Far-end Node Name: silasm4
Near-end Listen Port: 5060         Far-end Listen Port: 5060
Far-end Domain: dr.avaya.com       Far-end Network Region:
Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload         Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3 IP Audio Hairpinning? n
Enable Layer 3 Test? y           Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```


2.6. Add SIP Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where “n” is an available trunk group number and fill in the indicated fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Signaling Group:** The number of the signaling group added in **Section 2.5**
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in **Section 2.1.1**).

add trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: SIP Video TG to silasm4	COR: 1	TN: 1	TAC: #010
Direction: two-way	Outgoing Display? y	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 10	
		Number of Members: 64	

Once the add command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

On **Page 2**, set the **Preferred Minimum Session Refresh Interval** to 1200. **Note:** to avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of 1200.

add trunk-group 10		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 1200			

On **Page 3**, set the **Numbering Format** to **private**.

add trunk-group 10		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
 Numbering Format: private		
	UUI Treatment: service-provider	
	Replace Restricted Numbers? n	
	Replace Unavailable Numbers? n	
 Modify Tandem Calling Number: no		
 Show ANSWERED BY on Display? y		
DSN Term? n	SIP ANAT Supported? n	

2.7. Administering Numbering Plan

SIP Users registered to Session Manager needs to be added to either the private or public numbering table on Communication Manager Evolution Server. For the sample configuration, public numbering was used and all extension numbers were unique within the public network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in References [3] and [8] in **Section 8**.

To enable SIP endpoints to dial extensions defined in Communication Manager Evolution Server, use the **change public-unknown-numbering x** command, where “x” is the number used to identify the private number plan. For the sample configuration, extension numbers starting with 5-XXXX are used on Communication Manager Evolution Server.

- **Ext Len:** Enter the extension length allowed by the dial plan
- **Ext Code:** Enter leading digit (s) from extension number
- **Trunk Grp(s):** Enter the SIP Trunk Group number for the SIP trunk between the Evolution Server and Session Manager
- **CPN Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.
- **Total CPN Len:** Enter the total CPN length.

change public-unknown-numbering 5					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
5	5	10		5	Total Administered: 1
					Maximum Entries: 9999

2.8. Configure Stations

The method is the same for administering all of the Polycom HDX video endpoints.

For each SIP user to be defined in Session Manager, add a corresponding station on Communication Manager Evolution Server. **Note:** instead of manually defining each station using the Communication Manager SAT interface, the preferred option is to automatically generate the SIP station when adding a new SIP user. See **Section 3.3.7** for more information on adding SIP users.

The phone number defined for the station will be the number the SIP user enters to register to Session Manager. Use the **add station x** command where “x” is a valid extension number defined in the system. In this example extension 50091 is a Polycom HDX 8006 video endpoint. On **Page 1** of the **add station** form:

- **Phone Type:** Set to 9630SIP
- **Name:** Display name for user
- **Security Code:** Number used when user logs into station. **Note:** this code should match the “**Shared Communication Profile Password**” field defined when adding this user in Session Manager. See **Section 3.3.7**.
- **IP Video?** Enable endpoint for video

add station 50091		Page 1 of 6	
STATION			
Extension: 50091	Lock Messages? n	BCC: 0	
Type: 9630SIP	Security Code: 123456	TN: 1	
Port: IP	Coverage Path 1: 1	COR: 10	
Name: HDX8006-SIP x50091	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 1		Time of Day Lock Table:	
Display Language: english		Message Lamp Ext: 50091	
		Button Modules: 0	
Survivable COR: internal			
Survivable Trunk Dest? y		IP SoftPhone? n	
		IP Video? Y	

add station 50091	Page 4 of 6
STATION	
SITE DATA	
Room:	Headset? n
Jack:	Speaker? n
Cable:	Mounting: d
Floor:	Cord Length: 0
Building:	Set Color:
ABBREVIATED DIALING	
List1:	List2: List3:
BUTTON ASSIGNMENTS	
1: call-appr	5:
2: call-appr	6:
3: call-appr	7:
4:	8:

On **Page 6**, set:

- **SIP Trunk option:** Enter SIP Trunk Group defined in **Section 2.6** or use AAR

change station 50091	Page 6 of 6
STATION	
SIP FEATURE OPTIONS	
Type of 3PCC Enabled: None	
SIP Trunk: 10	

2.9. Configure Off-PBX-Telephone Station-Mapping

Use the **change off-pbx-telephone station-mapping** command for each extension associated with SIP users defined in Session Manager. On **Page 1**, enter the SIP Trunk Group defined in **Section 2.6** and use default values for other fields.

change off-pbx-telephone station-mapping 50091							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
50091	OPS	-		50091	10	1	
		-					
		-					

On **Page 2**, enter the following values:

- **Mapping Mode:** “both”
- **Calls Allowed:** “all”

change off-pbx-telephone station-mapping 50091							Page 2 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Appl Name	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	
50091	OPS	3	both	all	none		
			-				

2.10. Save Translations

Configuration of Communication Manager Evolution Server is complete. Use the **save translation** command to save these changes

Note: After a change on Communication Manager Evolution Server which alters the dial plan, synchronization between Communication Manager Evolution Server and Session Manager needs to be completed. To request an on demand synchronization, log into the System Manager console and use the **Synchronize CM Data** feature under the Communication System Management menu.

3. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring the Session Manager and includes the following items:

- Administer SIP domain
- Define Logical/Physical Locations that can be occupied by SIP Entities
- Define SIP entity
- Define Communication Manager Evolution Server as an Managed Element
- Adding SIP Endpoints/SIP URE users

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL “http://<fqdn>/SMGR” or “http://<ip-address>/SMGR”, where “<fqdn>” is the fully qualified domain name of Avaya Aura® System Manager or the “<ip-address>” is the IP address of Avaya Aura® System Manager.

Log in with the appropriate credentials.

Once logged in select the **Routing** Link under the **Elements** column. Select a specific item such as **Domains**.

3.1. Administer SIP Domains

Select **Domains**.

- Click **New** (Not shown)
- Under *Name* add the same name given in **Section 2.4** for the **Authoritative Domain**
- Under *Notes* add a brief description.
- Click **Commit** to save.

The screen below shows the information for the sample configuration.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and user information: 'Last Logged on at March 11, 2013 12:56 PM' and 'Help | About | Change Password | Log off admin'. The main navigation menu on the left lists various configuration areas: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The 'Routing' menu is expanded, showing 'Domains' as the selected option. The breadcrumb trail at the top of the content area reads 'Home / Elements / Routing / Domains'. The 'Domain Management' section includes buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below this is a table with 6 items, showing a list of domains. The table has columns for 'Name', 'Type', and 'Notes'. The domains listed are: dr.avaya.com (SIP, SIL Lab domain), mtinet.net (SIP, cs2100 Domain in Richardson, TX), mx.dr.avaya.com (SIP, mx.dr.avaya.com), silasm4.dr.avaya.com (SIP), silfst.dr.avaya.com (SIP), and sqa.dr.avaya.com (SIP). A 'Filter: Enable' link is present to the right of the table. At the bottom of the table, it says 'Select : All, None'.

Name	Type	Notes
dr.avaya.com	sip	SIL Lab domain
mtinet.net	sip	cs2100 Domain in Richardson, TX
mx.dr.avaya.com	sip	mx.dr.avaya.com
silasm4.dr.avaya.com	sip	
silst.dr.avaya.com	sip	
sqa.dr.avaya.com	sip	

3.2. Define Locations

Select **Locations**. Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

- Click **New** (Not shown)
- In the *General* Section, under *Name* add a descriptive name.
- Under *Notes* add a brief description.
- In the *Location Pattern* Section, click **Add**. Under IP Address Pattern section, enter pattern used to logically identify the location. Under *Notes* add a brief description.
- Click **Commit** to save.

The screen below shows the information for Communication Manager Evolution Server in the sample configuration.

The screenshot displays the 'Locations' configuration page within the Avaya Communication Manager Evolution Server interface. The breadcrumb trail at the top reads 'Home / Elements / Routing / Locations'. The left-hand navigation menu includes 'Routing', 'Domains', 'Locations' (highlighted), 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. It is divided into several sections: 'General' with fields for 'Name' (192.168.1) and 'Notes'; 'Dial Plan Transparency in Survivable Mode' with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'; 'Overall Managed Bandwidth' with fields for 'Managed Bandwidth Units' (Kbit/sec), 'Total Bandwidth', and 'Multimedia Bandwidth', along with a checked 'Audio Calls Can Take Multimedia Bandwidth' checkbox; 'Per-Call Bandwidth Parameters' with fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth' (64 Kbit/Sec), and 'Default Audio Bandwidth' (80 Kbit/sec); 'Alarm Threshold' with fields for 'Overall Alarm Threshold' (80 %), 'Multimedia Alarm Threshold' (80 %), and latency triggers; and 'Location Pattern' with an 'Add' button and a table showing one item with the IP address pattern '192.168.1.*' and a 'Notes' column. A 'Filter: Enable' button is located at the bottom right of the table.

IP Address Pattern	Notes
* 192.168.1.*	

3.3. Add Avaya Aura[®] Communication Manager Evolution Server

The following section captures relevant screens for defining Avaya Aura[®] Communication Manager Evolution Server applicable for the sample configuration.

3.3.1. Define SIP Entity for Avaya Aura[®] Communication Manager Evolution Server

The following screen shows addition of Communication Manager Evolution Server. The IP address used is that of the Processor Ethernet (procr) of Avaya Communication Manager Evolution Server.

The screenshot displays the 'SIP Entity Details' configuration page in the Avaya Aura Configuration Manager. The left sidebar shows a navigation tree with 'SIP Entities' selected. The main area contains the following sections:

- General:** Fields for Name (CM4_PROCR), FQDN or IP Address (192.168.1.1), Type (CM), Notes (CMES 6.3), Adaptation (Presence Buddy List adapter), Location (SIL Lab), and Time Zone (America/Denver). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV'.
- SIP Timer B/F (in seconds):** Set to 4.
- Credential name:** Empty field.
- Call Detail Recording:** Set to none.
- Loop Detection:** Loop Detection Mode is set to Off.
- SIP Link Monitoring:** Set to Use Session Manager Configuration.
- Supports Call Admission Control:** Unchecked.
- Shared Bandwidth Manager:** Unchecked.
- Primary Session Manager Bandwidth Association:** Empty dropdown.
- Backup Session Manager Bandwidth Association:** Empty dropdown.
- Entity Links:** Includes 'Add' and 'Remove' buttons. Below is a table with 1 item:

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
silasm4	TLS	* 5061	CM4_PROCR	* 5061	trusted	<input type="checkbox"/>

Below the table are fields for 'TCP Failover port' and 'TLS Failover port', both empty.

- SIP Responses to an OPTIONS Request:** Includes 'Add' and 'Remove' buttons. Below is a table with 0 items.

Response Code & Reason Phrase	Mark Entity Up/Down	Notes
-------------------------------	---------------------	-------

At the bottom right are 'Commit' and 'Cancel' buttons.

3.3.2. Define Entity Links for Avaya Aura® Communication Manager Evolution Server

The following screen shows the Entity Link defined for Avaya Aura® Communication Manager Evolution Server.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and user information: 'Last Logged on at March 11, 2013 2:22 PM' and links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar shows a tree view with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links' (highlighted), 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Entity Links' and contains a table with the following columns: 'Name', 'SIP Entity 1', 'Protocol', 'Port', 'SIP Entity 2', 'Port', 'Connection Policy', 'Deny New Service', and 'Notes'. A single row is visible in the table with the following values: 'silasm4_CM4_PROCR', 'silasm4', 'TCP', '5060', 'CM4_PROCR', '5060', 'trusted', and an unchecked checkbox for 'Deny New Service'. The 'Notes' column is empty. Below the table, there is a 'Select: All, None' option. At the bottom of the main area are 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* silasm4_CM4_PROCR	* silasm4	TCP	* 5060	* CM4_PROCR	* 5060	trusted	<input type="checkbox"/>	

3.3.3. Define Routing Policy for Avaya Aura® Communication Manager Evolution Server

Since the SIP users are registered on Session Manager, a routing policy does not need to be defined for Communication Manager Evolution Server.

3.3.4. Define Applications for Avaya Aura® Communication Manager Evolution Server

To define Avaya Aura® Communication Manager Evolution Server Applications,

- **Elements -> Session Manager->Application Configuration -> Applications**
 - Click **New** (Not shown)
 - Under *Name*, enter a name for the Application entry
 - Under *SIP Entity* drop-down menu, select the appropriate SIP Entity.
 - Under *CM System for SIP Entity*, this field can be left as the default of Select CM System.
 - Under *Description*, enter a description if desired.
 - Click **Commit** to save.

Avaya Aura® System Manager 6.3

Home / Elements / Session Manager / Application Configuration / Applications

Application Editor [Commit] [Cancel]

Application

*Name

*SIP Entity

*CM System for SIP Entity [View/Add CM Systems](#) [Refresh]

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

Application Media Attributes

Enable Media Filtering ☐

Audio	Video	Text	Match Type	If SDP Missing
<input type="text" value="YES"/>	<input type="text" value="YES"/>	<input type="text" value="YES"/>	<input type="text" value="NOT_EXACT"/>	<input type="text" value="ALLOW"/>

*Required [Commit] [Cancel]

3.3.5. Define Application Sequences for Avaya Aura® Communication Manager Evolution Server

To define Avaya Aura® Communication Manager Evolution Server Application Sequences,

- **Elements -> Session Manager->Application Configuration -> Application Sequences**
 - Click **New** (Not shown)
 - Under *Name*, enter a name of the Application Sequence.
 - Under *Description*, enter a description if desired.
 - Under *Available Applications*, select the Application that was created in **Section 3.3.4**. The way to select the Application of choice is to click on the “+” symbol next to the Application desired. This will be added to the **Applications in this Sequence** list.
 - Click **Commit** to save.

Second, define an Application Sequence for call application sequencing in Avaya Aura® Communication Manager Evolution Server as shown below:

The screenshot shows the Avaya Aura System Manager 6.3 web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, Applications, Application Sequences, Conference Factories, Implicit Users, NRS Proxy Users, System Status, System Tools, and Performance. The main content area is titled 'Application Sequence Editor' and includes a breadcrumb trail: Home / Elements / Session Manager / Application Configuration / Application Sequences. The interface has a 'Commit' and 'Cancel' button at the top right. Below the title, there's a section for 'Application Sequence' with fields for 'Name' (CMES App Seq 1) and 'Description' (CMES SIP endpoints (CM4)). Below this is a section titled 'Applications in this Sequence' with buttons for 'Move First', 'Move Last', and 'Remove'. A table lists the applications in the sequence, showing 1 item: 'cmes_cm4' with SIP Entity 'CM4_PROCR' and Description 'CM4 CMES'. Below this is a section titled 'Available Applications' with a 'Refresh' button and a 'Filter: Enable' option. A table lists 6 available applications: 'CM7', 'CM8', 'cmes_cm4', 's8800-G450-APP', 'silcm2', and 'sv-mako_CLAN_app'. Each application has a '+' icon to its left, indicating it can be added to the sequence. The bottom of the interface has a '* Required' label and 'Commit' and 'Cancel' buttons.

Avaya Aura® System Manager 6.3

Home / Elements / Session Manager / Application Configuration / Application Sequences

Application Sequence Editor [Commit] [Cancel]

Application Sequence

*Name: CMES App Seq 1
Description: CMES SIP endpoints (CM4)

Applications in this Sequence

[Move First] [Move Last] [Remove]

1 Item

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
1	cmes_cm4	CM4_PROCR	<input checked="" type="checkbox"/>	CM4 CMES

Select: All, None

Available Applications

6 Items | Refresh | Filter: Enable

Name	SIP Entity	Description
+ CM7	cm7	CM Rel 6.2
+ CM8	cm8	CM Rel 6.2 - Business Collaboration Solution
+ cmes_cm4	CM4_PROCR	CM4 CMES
+ s8800-G450-APP	CMFS1	CM as FS only
+ silcm2	SILCM2	
+ sv-mako_CLAN_app	sv-mako_CLAN_64A05	CC Elite SV Lab D2-C20

* Required [Commit] [Cancel]

3.3.6. Define Avaya Aura® Communication Manager Evolution as an Administrable Entity

Before adding SIP users, Avaya Aura® Communication Manager Evolution Server must also be added to System Manager as an administrable entity. This action allows System Manager to access Communication Manager over its administration interface similar to how other administration tools such as Avaya Site Administrator access Communication Manager. Using this administration interface, System Manager will notify Communication Manager Evolution Server when new SIP users are added.

To define Avaya Aura® Communication Manager Evolution Server as an administrable entity,

- **Services -> Inventory -> Manage Elements**
 - Click **New** (Not shown)
 - Under **Type** drop-down menu, select **Communication Manager** (Not shown)
 - Under **Name**, enter an identifier for Communication Manager Evolution Server.
 - Under **Host Name or IP Address**, enter the IP address of the administration interface for the Evolution Server as shown below:
 - Under **Login and Password**, enter the login and password used for administration access to the Evolution Server.
 - Select SSH Connection.
 - Under **Port**, enter the port number for the administration interface of 5022 as shown below:

The screenshot shows the 'Edit Communication Manager silcm4' form in the Avaya System Manager. The form is divided into two tabs: 'General Attributes (G)' and 'SNMP Attributes (S)'. The 'General Attributes (G)' tab is selected. The form contains the following fields and values:

Field	Value
Name	silcm4
Hostname or IP Address	192.168.1.1
Login	tjm
Authentication Type	Password (selected)
Password	*****
Confirm Password	*****
SSH Connection	Checked
RSA SSH Fingerprint (Primary IP)	
RSA SSH Fingerprint (Alternate IP)	
Description	CMES 6.3
Alternate IP Address	
Enable Notifications	Unchecked
Port	5022
Location	

Buttons: Commit, Clear, Cancel (top right and bottom right)

3.3.7. Add SIP Users

Add SIP users corresponding to the 96XX SIP stations defined in **Section 2.8**. Alternatively, use the option to automatically generate the SIP stations on Communication Manager Evolution Server when adding a new SIP user.

- Under the **Users** column
 - Select **User Management → Manage Users**
 - Click **New** (Not shown)

Step 1 (Identity tab): Enter values for the following required attributes for a new SIP user in the **Identity** section of the new user form.

- **Last Name:** enter last name of user
- **First Name:** enter first name of user
- **Login Name:** enter extension no.@sip domain defined in **Section 3.1**. This field is primary handle of user.
- **Authentication Type:** select **Basic**
- **Password:** enter password which will be used to log into System Manager application (password). **NOTE:** This field is only displayed if adding a new user.
- **Confirm Password:** repeat value entered above. **NOTE:** This Filed is only displayed if adding a new user.

The screen below shows the Identity information when adding a new SIP user to the sample configuration.

AVAYA Avaya Aura® System Manager 6.3

Home / Users / User Management / Manage Users

User Profile Edit: 50091@dr.avaya.com

Commit & Continue Commit Cancel

Identity * Communication Profile * Membership Contacts

Identity *

* Last Name: x50091

* First Name: HDX8000-SIP

Middle Name:

Description: Password=password

Status: Offline

Update Time: April 26, 2011 8:38:39

* Login Name: 50091@dr.avaya.com

* Authentication Type: Basic

Change Password

Source: local

Localized Display Name: HDX8000-SIP x50091

Endpoint Display Name: HDX8000-SIP x50091

Title:

Language Preference: English (United States)

Time Zone:

Employee ID:

Department:

Company:

Address *

Localized Names *

* Required

Commit & Continue Commit Cancel

Step 2 (Communication Profile tab): Select the Communication Profile tab and Select **New** to define a **Communication Profile** for the new SIP user. Enter values for the following required attributes:

- **Communication Profile Password:** enter a numeric value which will be used to logon to SIP phone. **Note:** this field must match the Security Code field on the station form defined in **Section 2.8**.
- **Confirm Password:** repeat numeric password
- **Name:** enter name of communication profile
- **Default:** enter checkmark to indicate this profile is default profile

Select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required attributes:

- **Type:** select Avaya SIP
- **Fully Qualified Address:** enter extension number (**Note:** value is shown in **Handle** field after address is added)
- **Domain:** enter SIP domain defined in **Section 3.1**
- **@:** select SIP domain defined in **Section 3.1** (**Note:**

value is shown in **Domain** field)

Click **Add** to save the **Communication Address** for the new SIP user.

Step 3 (Communication Profile tab): Assign the **Application Sequence** defined in **Section 3.3.4** to the new SIP user as part of defining the **Communication Profile**. The **Application Sequence** can be used for both the originating and terminating sequence.

Select the **Session Manager Profile** box and enter the appropriate values for the following attributes:

- **Primary Session Manager:** select the appropriate Session Manager instance
- **Origination Application Sequence:** enter the appropriate sequence
- **Termination Application Sequence:** enter the appropriate sequence
- **Home Location:** select the appropriate location that was created in **Section 3.2**

Enter values for the following required attributes of the **Endpoint Profile** section:

- **System:** select the SIP Entity of the Communication Manager Evolution Server defined in **Section 3.3.6** from menu
- **Profile Type:** enter Endpoint
- **Use Existing Stations:** enter checkmark if station was already defined. Else, station will automatically be created.
- **Extension:** enter extension number
- **Template:** Select the template (system defined or user defined) you want to associate with the endpoint. Select the template based on the set type you want to add.
- **Set Type:** select “9630SIP” for this video endpoint
- **Security Code:** enter numeric value which will be used to logon to SIP phone.
Note: this field must match the value entered for the **Shared Communication Profile Password** field
- **Port:** select port number from the list for the selected template

Click **Commit** to save new user profile.

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at March 11, 2019 2:23
Help | About | Change Password | Log off

User Management

Home / Users / User Management / Manage Users

User Management

User Management

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

User Profile Edit: 50091@dr.avaya.com

Commit & Continue

Commit

Cancel

Identity

Communication Profile

Membership

Contacts

Communication Profile

Communication Profile Password: ***** Edit

New Delete Done Cancel

Name

Primary

Select : None

Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
<input checked="" type="checkbox"/> Avaya SIP	50091	dr.avaya.com
<input checked="" type="checkbox"/> Avaya XMPP	50091@ps.dr.avaya.com	

Select : All, None

Session Manager Profile

SIP Registration

Primary Session Manager

silasm4

Primary	Secondary	Maximum
83	7	90

Secondary Session Manager

silasm3

Primary	Secondary	Maximum
39	6	45

Survivability Server

silbsm1-sip

supports 43 Communication Profile(s).

Max. Simultaneous Devices

1

Block New Registration When Maximum Registrations Active?

Application Sequences

Origination Sequence

CMES App Seq 1

Termination Sequence

CMES App Seq 1

Call Routing Settings

Home Location

135.9.88

Conference Factory Set

(None)

CS 1000 Endpoint Profile

CallPilot Messaging Profile

CM Endpoint Profile

System

silom4

Profile Type

Endpoint

Use Existing Endpoints

Extension

50091

Endpoint Editor

Template

Select/Reset

Set Type

9630SIP

Security Code

Port

505106

Voice Mail Number

Preferred Handle

(None)

Enhanced Callr-Info display for 1-line phones

Delete Endpoint on Unassign of Endpoint from User or on Delete User.

Override Endpoint Name

Messaging Profile

IP Office Endpoint Profile

Presence Profile

Conferencing Profile

Required

Commit & Continue

Commit

Cancel

4. Configure Polycom HDX SIP Endpoint

To administer the HDX SIP video endpoints log in to the web interface using the IP address of the video endpoint. You will see a screen that looks similar to Figure 1 below. This is a sample configuration on how to administer an HDX SIP video endpoint. **NOTE:** The HDX endpoints can be dually registered as both SIP and H.323 but in this example it's configured as SIP only.

Perform the following steps to configure the Polycom HDX SIP Systems registered to Avaya Session Manager:

1. Install the Polycom system and connect it to your network.
2. Upgrade the Polycom system software (if necessary).
3. Using a web browser, access the Polycom home page for the unit, and select **Admin Settings>Network>IP Network**.
4. Select the **Enable SIP** check box.
5. Select the **Desired Transport Protocol** from the drop down box.
6. In the **User Name** box, enter an appropriate name.
7. In the **Domain User Name** box, enter an appropriate name.
8. In the **SIP Registrar Server** box enter the IP address of the Session Manager Software Asset.
9. In the **Proxy Server** box enter the IP address of the Session Manager Software Asset.
10. In the Type of Service box in the Quality of Service area, select the appropriate setting. Both **IP Precedence** and **DiffServ** are supported. Contact your Network Administrator for this information.
11. In the **Type of Service Value** boxes (**Video**, **Audio**, and **Control**), enter the QoS values necessary. Contact your Network Administrator for this information.
12. Select the **Enable PVEC** check box. PVEC (Polycom Video Error Concealment) is an algorithm for IP video Quality of Service (QoS). PVEC significantly improves video quality over congested IP networks that suffer from packet loss by compensating for the losses using packet information from before and after the actual occurrence. PVEC allows video frame rates to remain high during IP network hits and eliminates the poor images usually associated with heavy IP packet loss. This is done completely transparent to the user.
13. Select the **Enable RSVP** check box.
14. Select the **Dynamic Bandwidth** check box.
15. From the **Maximum Transmit Bandwidth** drop down box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Avaya Communication Manager system.
16. From the **Maximum Receive Bandwidth** drop down box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Avaya Communication Manager system.
17. Complete the Firewall and Streaming sections as necessary.
18. When finished, click the **Update** button at the top (see **Figure 1** below).

Repeat above Steps for each Polycom HDX SIP system.

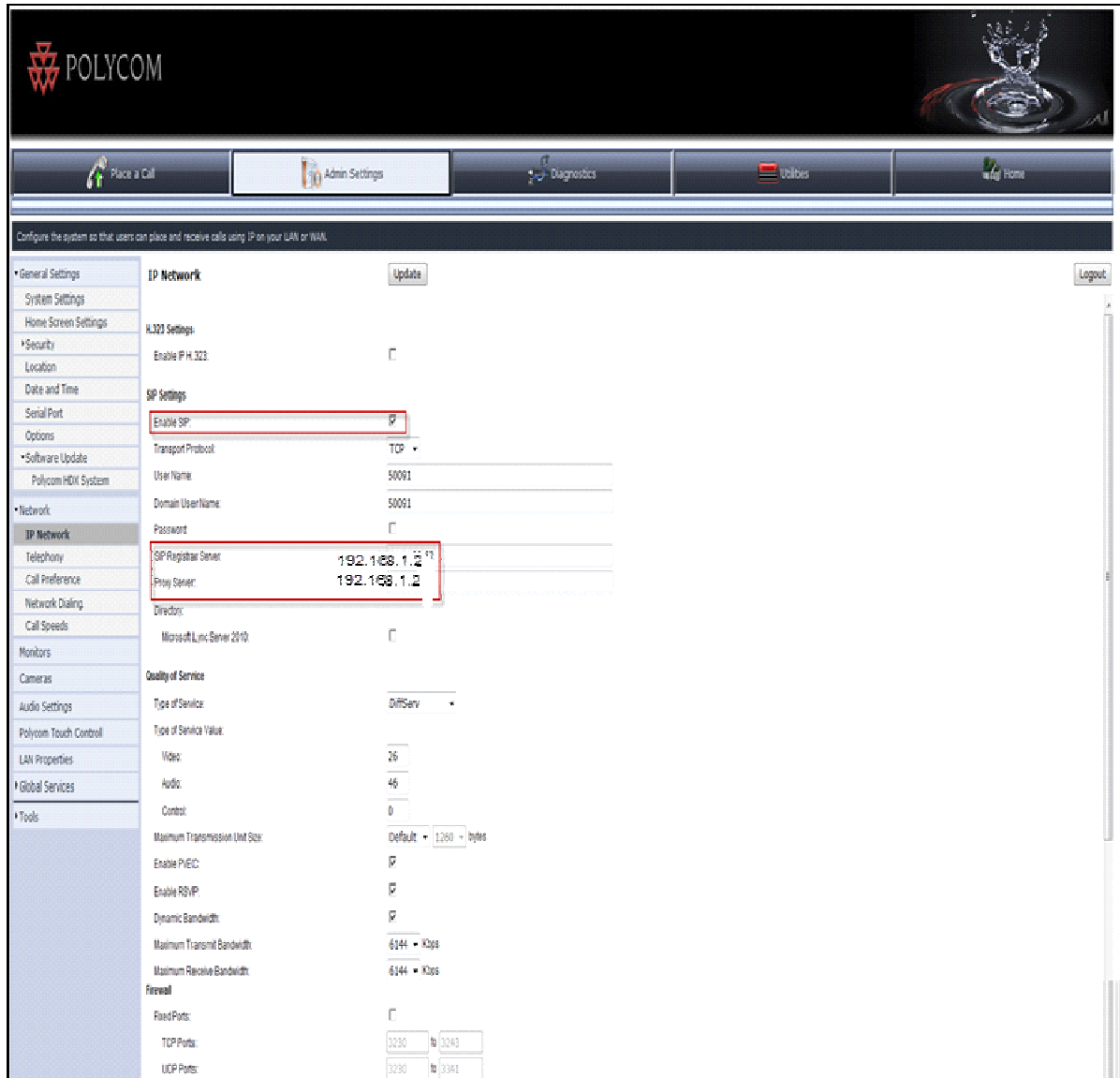


Figure 1. Example of a Polycom HDX8000 registered to Avaya Session Manager

5. Verification Steps

5.1. Verify Avaya Aura® Session Manager Configuration



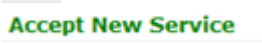

The following sections demonstrate some of the methods available to verify network connectivity and trace calls between PSTN users and SIP users registered to Session Manager.

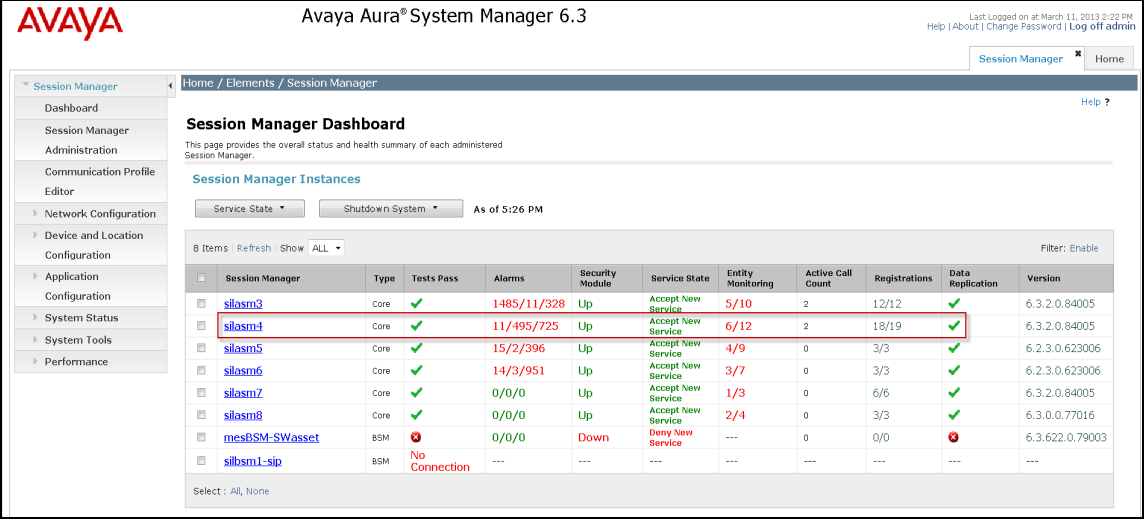
5.1.1. Verify Avaya Aura® Session Manager is Operational

Verify Avaya Aura® Session Manager is Operational

Navigate to **Elements** → **Session Manager** and select **Dashboard** to verify the overall system status of Session Manager.

Specifically, verify the status of the following fields as shown below:

- **Tests Pass** 
- **Security Module** 
- **Service State** 
- **Data Replication** 



Avaya Aura® System Manager 6.3

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: [Dropdown] Shutdown System: [Dropdown] As of 5:26 PM

8 Items | Refresh | Show ALL | Filter: Enable

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
silasm3	Core	✓	1485/11/328	Up	Accept New Service	5/10	2	12/12	✓	6.3.2.0.84005
silasm4	Core	✓	11/495/725	Up	Accept New Service	6/12	2	18/19	✓	6.3.2.0.84005
silasm5	Core	✓	15/2/396	Up	Accept New Service	4/9	0	3/3	✓	6.2.3.0.623006
silasm6	Core	✓	14/3/951	Up	Accept New Service	3/7	0	3/3	✓	6.2.3.0.623006
silasm7	Core	✓	0/0/0	Up	Accept New Service	1/3	0	6/6	✓	6.3.2.0.84005
silasm8	Core	✓	0/0/0	Up	Accept New Service	2/4	0	3/3	✓	6.3.0.0.77016
mesBSM-SWasset	BSM	✗	0/0/0	Down	Deny New Service	---	0	0/0	✗	6.3.622.0.79003
silbsml-sip	BSM	No Connection	---	---	---	---	---	---	---	---

Select: All, None

Navigate to **Elements** → **Session Manager** → **System Status** → **Security Module Status** to view more detailed status information on the status of Security Module for Session Manager. Verify the **Status** column displays “Up” as shown below.

Session Manager

Dashboard
Session Manager
Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
Registration Summary
User Registrations
Session Counts
System Tools
Performance

Home / Elements / Session Manager / System Status / Security Module Status

Session Manager x Home

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

The following errors have occurred:
Unable to access status information for Security Modules, silbsm1-sip - cannot connect to server, internal error.

Reset
Synchronize
Certificate Management
Connection Status

8 Items Refresh Show ALL Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
	Show	mesBSM-SWasset	BSM	Down	---	---	---	---	---	---	---
	Show	silasm3	SM	Up	51				Disabled	10/10	SIP CA
	Show	silasm4	SM	Up	46				Disabled	18/18	SIP CA
	Show	silasm5	SM	Up	16				Disabled	9/9	SIP CA
	Show	silasm6	SM	Up	13				Disabled	7/7	SIP CA
	Show	silasm7	SM	Up	32				Disabled	7/7	SIP CA
	Show	silasm8	SM	Up	13				Disabled	5/5	SIP CA
	Show	silbsm1-sip	BSM	---	---	---	---	---	---	---	---

Select : None

TJM Reviewed:
SPOC 11/5/2013

Solution Interoperability Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

29 of 39
HDX_SM62_ES62

5.1.2. Verify SIP Link Status

Expand the Session Manager menu on the left and click **SIP Entity Monitoring**. Verify all SIP Entity Links are operational as shown below:

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at March 11, 2013
Help | About | Change Password | Log Out

Session Manager

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Registration Summary

User Registrations

Session Counts

System Tools

Performance

SIP Entity Link Monitoring Status Summary

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

[SIP Entities Status for All Monitoring Session Manager Instances](#)

Run Monitor

8 Items Refresh Filter: Enable

Session Manager	Type	Monitored Entities						Total
		Down	Partially Up	Up	Not Monitored	Deny		
<input type="checkbox"/> silasm3	Core	5	0	5	0	0	10	
<input type="checkbox"/> silasm4	Core	6	0	5	1	2	14	
<input type="checkbox"/> silasm5	Core	4	2	3	0	N.A.	9	
<input type="checkbox"/> silasm6	Core	3	2	2	0	N.A.	7	
<input type="checkbox"/> silasm7	Core	1	0	2	0	4	7	
<input type="checkbox"/> silasm8	Core	2	0	2	0	1	5	

Select: All, None < Previous Page 1 of 2 Next >

All Monitored SIP Entities

Run Monitor

28 Items Refresh Filter: Enable

SIP Entity Name
<input type="checkbox"/> IBMSUIT
<input type="checkbox"/> m3kTPalohal
<input type="checkbox"/> StackMM
<input type="checkbox"/> CS1K_Ret7_5
<input type="checkbox"/> dauphin
<input type="checkbox"/> dennis-MPPs
<input type="checkbox"/> silfst RMX_1
<input type="checkbox"/> silaam61

Select: All, None < Previous Page 1 of 4 Next >

5.1.3. Verify Registrations of SIP Endpoints

Navigate to **Users → User Management → Manager Users** to verify SIP users have been created in the Session Manager. In the sample configuration, Extension 50091 SIP user was created as shown in the highlighted area below:

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at March 11, 2013 2:22 PM
Help | About | Change Password | Log off admin

User Management

Home

User Management

Home / Users / User Management / Manage Users

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

User Management

Criteria

Advanced Search

Login Name

Contains

50091

Clear

Search

Close

Users

View

Edit

New

Duplicate

Delete

More Actions

1 Item

Refresh

Reset

Show ALL

Filter: Enable

	Last Name	First Name	Display Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>	x50091	HDX8000-SIP	HDX8000-SIP x50091	50091@dr.avaya.com	50091	

Select : All, None

Navigate to **Elements** → **Session Manager** → **System Status** → **User Registrations** to verify the SIP endpoints have successfully registered with the Session Manager as shown below:

The screenshot displays the Avaya Aura System Manager 6.3 interface. The left sidebar contains navigation links for Session Manager, Dashboard, Session Manager, Administration, Communication Profile, Editor, Network Configuration, Device and Location, and System Status. The main content area is titled 'User Registrations' and shows a list of 42 items. A red box highlights the first row of the table, which contains the following information: First Name: Bret, Last Name: Michaels, Login Name: 50095@dr.avaya.com, Registration Address: 50095@dr.avaya.com, All Addresses: 50095@dr.avaya.com, Primary SM: sipasm4, Secondary SM: ---, Survivable SM: ---, Active Controller: sipasm4, Registration Time: Thu Dec 16 13:38:19 MST 2010, Event Subscriptions: ---, IP Address: 135.9.88.178-1060, MAC Address: 00-04-0d-ed-0c-4a, Device Vendor: Avaya, Device Type: one-X Deskphone, Device Model: 9620, Device Version: 2.6.0.

5.2. Verify Avaya Aura® Communication Manager Evolution Server Configuration

Verify the status of the SIP trunk group by using the **status trunk n** command, where “n” is the trunk group number administered in **Section 2.6**. Verify that all trunks are in the “in-service/idle” state as shown below:

```
status trunk 10
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports
			Busy
0010/001	T00001	in-service/idle	no
0010/002	T00002	in-service/idle	no
0010/003	T00003	in-service/idle	no
0010/004	T00004	in-service/idle	no
0010/005	T00005	in-service/idle	no
0010/006	T00006	in-service/idle	no
0010/007	T00007	in-service/idle	no
0010/008	T00008	in-service/idle	no
0010/009	T00009	in-service/idle	no
0010/010	T00010	in-service/idle	no

Verify the status of the SIP signaling groups by using the **status signaling-group n** command, where “**n**” is the signaling group number administered in **Section 2.5**. Verify the signaling group is “in-service” as indicated in the **Group State** field shown below:

```
status signaling-group 10
                        STATUS SIGNALING GROUP

      Group ID: 10
      Group Type: sip

      Group State: in-service
```

Use the Communication Manager SAT command, **list trace tac #**, where “**tac #**” is the trunk access code defined in **Section 2.6** to trace trunk group activity for the SIP trunk between the Session Manager and Communication Manager Evolution Server as shown below:

list trace tac #010		Page 1
		LIST TRACE
time	data	
18:32:04	TRACE STARTED 03/11/2013 CM Release String cold-02.0.823.0-20001	
18:32:41	SIP<INVITE sip:50091@dr.avaya.com;transport=tcp SIP/2.0	
18:32:41	dial 50091# route:UDP AAR	
18:32:41	term trunk-group 10 cid 0x13fe	
18:32:41	dial 50091# route:UDP AAR	
18:32:41	route-pattern 10 preference 1 cid 0x13fe	
18:32:41	seize trunk-group 10 member 19 cid 0x13fe	
18:32:41	Calling Number & Name NO-CPNumber NO-CPName	
18:32:41	Proceed trunk-group 10 member 19 cid 0x13fe	
18:32:42	SIP>SIP/2.0 180 Ringing	
18:32:42	Alert trunk-group 10 member 19 cid 0x13fe	
18:32:44	active trunk-group 10 member 19 cid 0x13fe	
18:32:44	G711MU ss:off ps:20	
	rgn:2 [f]:60304	
	rgn:2 [192.168.1.2]:60040	
18:32:44	G711MU ss:off ps:20	
	rgn:2 [192.168.1.2]:60040	
	rgn:2 [192.168.1.2]:60304	
18:32:44	SIP>SIP/2.0 200 OK	
18:32:44	Video: H264 [192.168.1.2]:60306	
18:32:44	Video: H264 [192.168.1.2]:60042	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:32:44	Video: H264 [192.168.1.2]:60042	
18:32:44	Video: H264 [192.168.1.2]:60306	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:32:44	SIP>INFO sip:50091@192.168.1.2;transport=tcp SIP/2.0	
18:32:44	SIP<ACK sip:50091@192.168.1.2;transport=tcp SIP/2.0	
18:32:44	SIP<SIP/2.0 200 OK	
18:32:51	SIP<BYE sip:50091@192.168.1.2;transport=tcp SIP/2.0	
18:32:51	SIP>SIP/2.0 200 OK	
18:32:51	idle station 50091 cid 0x13fe	

Use the Communication Manager SAT command, **list trace station xxx**, where “xxx” is the extension number of the 96XX SIP telephone as shown below:

list trace station 50091		Page 1
LIST TRACE		
time	data	
18:35:36	TRACE STARTED 03/08/2013 CM Release String cold-02.0.823.0-20001	
18:36:13	active station 50091 cid 0x13ff	
18:36:13	SIP>INVITE sip:50091@dr.avaya.com SIP/2.0	
18:36:13	dial 50091# route:UDP AAR	
18:36:13	term trunk-group 10 cid 0x13ff	
18:36:13	dial 50091# route:UDP AAR	
18:36:13	route-pattern 10 preference 1 cid 0x13ff	
18:36:13	seize trunk-group 10 member 20 cid 0x13ff	
18:36:13	Setup digits 50091	
18:36:13	Calling Number & Name *50091 Michaels, Bre	
18:36:13	SIP<SIP/2.0 100 Trying	
18:36:13	Proceed trunk-group 10 member 20 cid 0x13ff	
18:36:13	SIP<SIP/2.0 422 Session Interval Too Small	
18:36:13	SIP>ACK sip:50091@dr.avaya.com SIP/2.0	
18:36:13	SIP>INVITE sip:50091@dr.avaya.com SIP/2.0	
18:36:13	SIP<SIP/2.0 100 Trying	
18:36:13	SIP<SIP/2.0 180 Ringing	
18:36:13	Alert trunk-group 10 member 20 cid 0x13ff	
18:36:15	SIP<SIP/2.0 200 OK	
18:36:15	active trunk-group 10 member 20 cid 0x13ff	
18:36:15	G711MU ss:off ps:20	
	rgn:2 [192.168.1.2]:60312	
	rgn:2 [192.168.1.2]:60048	
18:36:15	G711MU ss:off ps:20	
	rgn:2 [192.168.1.2]:60048	
	rgn:2 [192.168.1.2]:60312	
18:36:15	Video: H264 [192.168.1.2]:60314	
18:36:15	Video: H264 [192.168.1.2]:60050	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:36:15	Video: H264 [192.168.1.2]:60050	
18:36:15	Video: H264 [192.168.1.2]:60314	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:36:16	SIP<INFO sip:+50091@192.168.1.2;transport=tcp SIP/2.0	
18:36:16	SIP>SIP/2.0 200 OK	
18:36:16	SIP>ACK sip:50091@192.168.1.2;transport=tcp SIP/2.0	
18:36:22	SIP>BYE sip:50091@192.168.1.2;transport=tcp SIP/2.0	
18:36:22	idle station 50091 cid 0x13ff	

5.3. Call Scenarios Verified

Verification scenarios for the configuration described in these Application Notes included the following call scenarios:

Calls initiated from the GUI of the respective endpoint

- Place a point-to-point video call from a 4002/8006/9004 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way video and two-way talk path for all combinations of calls between HDX SIP video endpoints. Verify Call statistics on the endpoint GUI.
- Place a point-to-point video call from a 1040 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way video and talk path. Place a video conference call from 4002 to a 8006. Answer the call and verify three-way video and audio conference call. Add a fourth video endpoint to the call and verify video and audio. Verify Call statistics on the endpoint GUI.
- Place a point-to-point audio call from a 4002/8006/9004 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way talk path for all combinations of calls between HDX SIP video endpoints. Verify Call statistics on the endpoint GUI.
- Place a point-to-point audio call from a 9004 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way video and talk path. Place another video conference call from 9004 to a 4002/8006/9004. Answer the call and verify video and talk path on conference call. Add a fourth video endpoint to the call and verify video and talk path. Verify Call statistics on the endpoint GUI.

Calls initiated from the Web interface of the respective endpoint

- Place a point-to-point video call from a 4002/8006/9004 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way video and two-way talk path for all combinations of calls between HDX SIP video endpoints. Verify Call statistics on the endpoint GUI.
- Place a point-to-point video call from a 1040 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way video and talk path. Place a video conference call from 4002 to a 8006. Answer the call and verify three-way video and audio conference call. Add a fourth video endpoint to the call and verify video and audio. Verify Call statistics on the endpoint GUI.
- Place a point-to-point audio call from a 4002/8006/9004 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way talk path for all combinations of calls between HDX SIP video endpoints. Verify Call statistics on the endpoint GUI.
- Place a point-to-point audio call from a 9004 video endpoint registered to SM (CMES) to another 4002/8006/9004 video endpoint registered on SM (CMES). Answer the call and verify two-way video and talk path. Place another video conference call from 9004 to a 4002/8006/9004. Answer the call and verify video and talk path on conference call. Add a fourth video endpoint to the call and verify video and talk path. Verify Call statistics on the endpoint GUI.

6. Acronyms

AAR	Automatic Alternative Routing (Routing on Communication Manager)
ARS	Alternative Routing Service (Routing on Communication Manager)
CMES	Communication Manager Evolution Server
IMS	IP Multimedia Subsystem
IP	Internet Protocol
RTP	Real Time Protocol
SAT	System Access Terminal (Communication Administration Interface)
SIL	Solution Interoperability Lab
SIP	Session Initiation Protocol
SM	Avaya Aura [®] Session Manager
SMGR	System Manager (used to configure Session Manager)
TAC	Trunk Access Code (Communication Manager Trunk Access)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
URE	User Relation Element

7. Conclusion

These Application Notes describe how to configure Avaya Aura[®] Session Manager and Avaya Aura[®] Communication Manager operating as an Evolution Server to support the Polycom HDX SIP video endpoints. Interoperability testing included successfully making bi-directional calls between several different types of video endpoints and the use of the conferencing feature of the internal MCU of the HDX system. **NOTE:** Conferencing a.k.a. Embedded Multipoint, is an optional feature for the HDX system that must be purchased from Polycom. These successful calls were generated via the GUI of each respective video endpoint as well as each video endpoints respective Web interface.

8. Additional References

This section references the product documentation relevant to these Application Notes.

Session Manager

- 1) Avaya Aura[®] Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>.
- 2) Installing and Administering Avaya Aura[®] Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>.
- 3) Maintaining and Troubleshooting Avaya Aura[®] Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

Communication Manager

- 4) Hardware Description and Reference for Avaya Aura® Communication Manager (COMCODE 555-245-207)
http://support.avaya.com/elmodocs2/comm_mgr/r4_0/avayadoc/03_300151_6/245207_6/245207_6.pdf
- 5) SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206 available at <http://support.avaya.com>.
- 6) Administering Avaya Aura® Communication Manager, Doc ID 03-300509 available at <http://support.avaya.com>.
- 7) Administering Avaya Aura® Communication Manager as a Feature Server, Doc ID 03-603479 available at <http://support.avaya.com>

Polycom HDX Series Video Endpoints

- 8) Polycom references are available at <http://www.polycom.com/support/>

©2013 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