



Avaya Solution Interoperability Test Lab

Configuring Avaya 10x0 Series SIP Video Endpoints with Avaya Aura[®] Session Manager Release 6.1 and Avaya Aura[®] Communication Manager Evolution Server Release 6.0.1 – Issue 1.0

Abstract

These Application Notes describe the configuration of the Avaya 10x0 Series 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
2.1.2. AAR/ARS Routing Check.....	6
2.2. Add Node Name of Avaya Aura® Session Manager.....	7
2.3. Configure Codec Type.....	8
2.4. Configure IP Network Region.....	8
2.5. Add SIP Signaling Group.....	9
2.6. Add SIP Trunk Group.....	10
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.....	14
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 Entities 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.....	23
4. Configure Avaya 10x0 Video Endpoint.....	27
5. Verification Steps.....	34
5.1. Verify Avaya Aura® Session Manager Configuration.....	34

5.1.1. Verify Avaya Aura® Session Manager is Operational	34
5.1.2. Verify SIP Link Status.....	36
5.1.3. Verify Registrations of SIP Endpoints.....	37
5.2. Verify Avaya Aura® Communication Manager Evolution Server Configuration.....	39
5.3. Call Scenarios Verified	42
6. Acronyms.....	43
7. Conclusion.....	43
8. Additional References.....	43

1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura® Session Manager to support registration of Avaya 10x0 (1010, 1020, 1030, 1040, and 1050) SIP Video endpoints and enables connectivity to Avaya Aura® Communication Manager Evolution Server 6.0.1 using SIP trunks.

As shown in **Figure 1**, Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. Avaya 10x0 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 S8510 Server. Avaya Aura® Communication Manager 6.0.1 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 6.0.1.

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**).

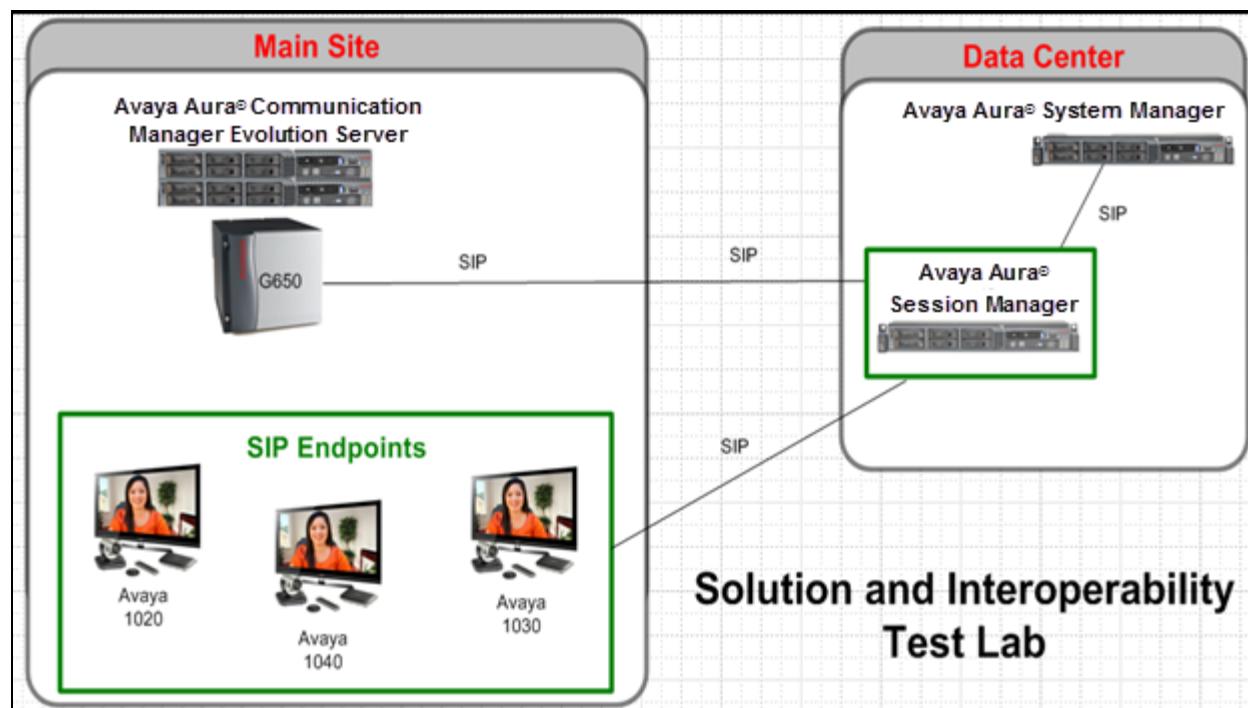


Figure 1 – Sample Configuration

1.1. Equipment and Software Validated

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

Equipment	Software
Avaya Aura [®] Session Manager	Release 6.1.0.0.610023
Avaya Aura [®] System Manager	Release 6.1 Load: 6.0.2.0.5
Avaya Aura [®] Communication Manager • Avaya S8800 Server Evolution Server	Release R016x.00.1.510.1-18599
Avaya IP Telephones10x0 Video Endpoints (SIP): • 1020 • 1030 • 1040	FW: AV_PP1_4.7.3(14) FW: AV_XX2_4.7.3(14) FW: AV_XX2_4.7.3(14)

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 instructions assume the G450 Media Gateway is already configured on Communication Manager Evolution Server. 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 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	328
Maximum Concurrently Registered IP Stations:		18000	17
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:		18000	12
Maximum Video Capable IP Softphones:		18000	109
Maximum Administered SIP Trunks:		24000	15493
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	80
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	15
Maximum Number of Expanded Meet-me Conference Ports:		300	0
(NOTE: You must logoff & login to effect the permission changes.)			

2.1.2. AAR/ARS Routing Check

Verify that **ARS** is enabled (on **Page 3** of **system-parameters customer options** form

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
A/D Grp/Sys List Dialing Start at 01? y		CAS Main? y	
Answer Supervision by Call Classifier? y		Change COR by FAC? y	
ARS? y		Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y		Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? y		DCS (Basic)? y	
ASAI Link Core Capabilities? y		DCS Call Coverage?	

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	135.9.88.13	
procr6	::	
silasm4	135.9.88.62	

2.3. Configure Codec Type

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

- Enter “**G.711MU**” and “**G.729**” as supported types of **Audio Codecs**
- **Silence Suppression:** Retain the default value “**n**”.
- **Frames Per Pkt:** Enter “**2**”.
- **Packet Size (ms):** Enter “**20**”.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size(ms)
1: G.711MU	n	2	20
2: G.729	n	2	20
3:			

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		Intra-region IP-IP Direct Audio: yes		
Codec Set: 1		Inter-region IP-IP Direct Audio: yes		
UDP Port Min: 2048		IP Audio Hairpinning? n		
UDP Port Max: 16585				

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 “1” 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                                SIP Enabled LSP? n
    IP Video? y                      Priority Video? n      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM

    Near-end Node Name: procr                      Far-end Node Name: silasm4
  Near-end Listen Port: 5060                      Far-end Listen Port: 5060
                                                Far-end Network Region: 2
Far-end Domain: dr.avaya.com

                                                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		
Dial Access? n	Night Service:		
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			

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 Avaya 1000 series video endpoints with the exception of the 1040 and 1050's. The only difference is that the 1040 can be administered to have up to 3 call appearances and the 1050 can have up to 7 call appearances for conferencing via their internal MCU's. The 1010, 1020, and 1030 have to be administered with only one call-appearance since they are a single-line endpoint with no conferencing or transferring capabilities.

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 50095 is an Avaya 1020 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 50095		Page 1 of 6	
STATION			
Extension: 50095	Lock Messages? n	BCC: 0	
Type: 9630SIP	Security Code: 123456	TN: 1	
Port: S00006	Coverage Path 1: 1	COR: 1	
Name: SIL Video Lab - 1030	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 19		Time of Day Lock Table:	
Display Language: english	Message Lamp Ext: 50095		
Survivable COR: internal	Button Modules: 0		
Survivable Trunk Dest? y	IP SoftPhone? n		
IP Video? y			

Note: It is important to assign only one call-appearance for the 1010, 1020, and 1030's.

add station 50095		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:	6:	
3:	7:	
4:	8:	

On **Page 6**, set:

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

change station 50095		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 50095							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
50095	OPS	-		50095	10	1	
		-					
		-					

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

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

change off-pbx-telephone station-mapping 50095							Page 2 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Appl Name	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	
50095	OPS	1	both	all	none		
			-				

2.10. Save Translations

Configuration of Communication Manager Evolution Server is complete. Use the **save translations** 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 and SIP phones must be re-registered. 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

- For each SIP entity in the sample configuration:
 - Define SIP Entity
 - Define Entity Links, which define the SIP trunk parameters used by Avaya Aura[®] Session Manager when routing calls to/from SIP Entities
 - Define Routing Policies, which control call routing between the SIP Entities
 - Define Dial Patterns, which govern to which SIP Entity a call is routed
- 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.

Avaya Aura[™] System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Home

Home / Elements / Routing / Domains - Domain Management

Domain Management

1 Item Refresh Filter: Enable

Name	Type	Default	Notes
* dr.avaya.com	sip	<input type="checkbox"/>	SIL Lab domain

* Input Required

Commit Cancel

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 Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for Help, About, Change Password, and Log off admin. The main content area is titled "Home / Elements / Routing / Locations - Location Details". On the left, a sidebar menu lists various configuration options under the "Routing" category, with "Locations" currently selected. The main panel shows the "Location Details" form. It includes a "General" section with fields for "Name" (set to "135.9.88") and "Notes" (set to "CMFS and CMES 6.0"). Below this is the "Overall Managed Bandwidth" section, which includes a dropdown for "Managed Bandwidth Units" (set to "Kbit/sec") and a "Total Bandwidth" field. The "Per-Call Bandwidth Parameters" section has a "Default Audio Bandwidth" field (set to "80 Kbit/sec"). The "Location Pattern" section features an "Add" button and a table with one entry: "IP Address Pattern" with the value "135.9.88.*" and "Notes" with the value "88 Subnet". At the bottom, there is a "Commit" button and a "Cancel" button. A red asterisk indicates that input is required for the "Name" field.

AVAYA Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Locations - Location Details

Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: 135.9.88

Notes: CMFS and CMES 6.0

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

IP Address Pattern	Notes
* 135.9.88.*	88 Subnet

Select : All, None

* Input Required

Commit Cancel

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 Entities 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 Avaya Aura System Manager 6.1 web interface. The left sidebar shows a navigation menu with options like Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a breadcrumb trail: 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. The 'General' tab is active, showing fields for Name (s8800_cmes), FQDN or IP Address (135.9.88.13), Type (CM), Notes (CMES 6.0), Adaptation, Location (135.9.88), Time Zone (America/Denver), and checkboxes for 'Override Port & Transport with DNS SRV' and 'SIP Timer B/F (in seconds): 4'. There are also fields for 'Credential name' and 'Call Detail Recording: none'. The 'SIP Link Monitoring' section has a dropdown for 'SIP Link Monitoring: Link Monitoring Enabled' and input fields for 'Proactive Monitoring Interval (in seconds): 900', 'Reactive Monitoring Interval (in seconds): 120', and 'Number of Retries: 1'. The 'Entity Links' section includes 'Add' and 'Remove' buttons and a table with one item. The table has columns for SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. The entry shows 'silasm4' as SIP Entity 1, 'TCP' as Protocol, '5060' as Port, 's8800_cmes' as SIP Entity 2, '5060' as Port, and 'Trusted' checked. At the bottom, there is a 'Commit' button and a 'Cancel' button.

AVAYA Avaya Aura™ System Manager 6.1 Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details

General

* Name: s8800_cmes

* FQDN or IP Address: 135.9.88.13

Type: CM

Notes: CMES 6.0

Adaptation:

Location: 135.9.88

Time Zone: America/Denver

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: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links

Add Remove

1 Item Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	silasm4	TCP	* 5060	s8800_cmes	* 5060	<input checked="" type="checkbox"/>

Select : All, None

* Input Required

Commit Cancel

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 shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes a breadcrumb trail: Home / Elements / Routing / Entity Links- Entity Links. There are 'Commit' and 'Cancel' buttons at the top right. Below the title, there is a table with the following data:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* silasm4-to-cmes	* silasm4	TCP	* 5060	* s8800_cmes	* 5060	<input checked="" type="checkbox"/>	

At the bottom of the table, there is a message: '* Input Required'. There are also 'Commit' and 'Cancel' buttons at the bottom right.

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.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help | About | Change Password | Log off admin". Below this is a breadcrumb trail: "Home / Elements / Session Manager / Application Configuration / Applications- Applications". The left sidebar contains a tree view with categories like "Session Manager", "Network Configuration", "Device and Location Configuration", "Application Configuration", "Implicit Users", "NRS Proxy Users", "System Status", and "System Tools". The "Application Configuration" category is expanded, showing "Applications" as the selected option. The main content area is titled "Application Editor" and contains the following fields:

- Name:** A text input field containing "cmes_cm4".
- SIP Entity:** A dropdown menu showing "s8800_cmes".
- CM System for SIP Entity:** A dropdown menu showing "Select CM System", with a "Refresh" button and a link "View/Add CM Systems".
- Description:** A text input field containing "CM4 CMES".

Below these fields is a section titled "Application Attributes (optional)" which contains a table with two columns: "Name" and "Value". The table has two rows: "Application Handle" and "URI Parameters", each with an empty text input field.

At the bottom of the form, there is a "Required" label and two buttons: "Commit" and "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 6.1 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, Implicit Users, NRS Proxy Users, System Status, and System Tools. The main content area is titled 'Application Sequence Editor' and shows the configuration for an 'Application Sequence'. The 'Name' field is 'CMES App Seq 1' and the 'Description' is 'CMES SIP endpoints (CM4)'. Below this, the 'Applications in this Sequence' section shows a table with one item: 'cmes_cm4' with SIP Entity 's8800_cmes' and Description 'CM4 CMES'. The 'Available Applications' section shows a table with three items: 'cmes_cm4', 'ps1', and 's8800-G450-APP'. The 'Required' checkbox is checked. The interface includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

Avaya Aura[™] System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager * Home

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

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	1	cmes_cm4	s8800_cmes	<input checked="" type="checkbox"/>	CM4 CMES

Select : All, None

Available Applications

3 Items Refresh Filter: Enable

	Name	SIP Entity	Description
+	cmes_cm4	s8800_cmes	CM4 CMES
+	ps1	Presence-Element	IPS6.0
+	s8800-G450-APP	cm4	CM as FS only

*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, expand **Elements** -> **Inventory** -> **Manage Elements (Application tab)** and click **New** (Not shown).

- Under *Name*, enter an identifier for Communication Manager Evolution Server.
- Under *Type*, select CM from drop-down menu.
- Under *Node*, enter the IP address of the administration interface for the Evolution Server as shown below:

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. Below the navigation bar, there are tabs for 'Inventory' (selected) and 'Home'. The left sidebar shows a tree view with 'Inventory' expanded, containing 'Manage Elements' (selected), 'Discovered Inventory', 'Discovery Management', and 'Synchronization'. The main content area shows the breadcrumb 'Home / Elements / Inventory / Manage Elements- Edit CM' and the title 'Edit CM: silcm4'. There are 'Commit' and 'Cancel' buttons. The form has two tabs: 'Application' (selected) and 'Attributes'. Under the 'Application' tab, there are fields for 'Name' (silcm4), 'Type' (CM), 'Description' (CMES 6.0), and 'Node' (135.9.88.13). There are also sections for 'Access Point' and 'Port'. A legend at the bottom left indicates '* Required'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

Defining Avaya Aura[®] Communication Manager Evolution Server as an administrable entity (continued):

- **Manage Elements – Attributes** tab
 - Under *Login and Password*, enter the login and password used for administration access to the Evolution Server.
 - Select SSH access.
 - Under *Port*, enter the port number for the administration interface of 5022 as shown below:

The screenshot displays the Avaya Aura[™] System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura[™] System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. A breadcrumb trail shows 'Home / Elements / Inventory / Manage Elements - Edit CM'. The left sidebar contains a tree view with 'Inventory' expanded, showing 'Manage Elements', 'Discovered Inventory', 'Discovery Management', and 'Synchronization'. The main content area is titled 'Edit CM: silcm4' and features a 'Help ?' link. Below the title are 'Commit' and 'Cancel' buttons. The 'Attributes' tab is selected, showing a form for configuring the CM. The form includes fields for 'Login' (tjm), 'Password' (masked), 'Confirm Password' (masked), 'Is SSH Connection' (checked), 'Port' (5022), 'Alternate IP Address', 'RSA SSH Fingerprint (Primary IP)', 'RSA SSH Fingerprint (Alternate IP)', 'Is ASG Enabled' (unchecked), 'ASG Key', 'Confirm ASG Key', and 'Location'. A legend at the bottom left indicates '* Required'.

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 create station on Communication Manager when new user is added.

Under **Users** column, select **User Management** → **Manage Users** and 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 from **Section 3.1**
Note: This field is primary handle of user.
- **Authentication Type:** select **Basic**
- **Password:** enter password which will be used to log into System Manager application.
Note: This field is displayed when adding new user.
- **Confirm Password:** repeat value entered above.

The screen below shows results from **Step 1** when adding a new SIP user.

The screenshot shows the Avaya Aura™ System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help | About | Change Password | Log off admin". Below this is a breadcrumb trail: "Home /Users / User Management / Manage Users- User Profile Edit". The left sidebar contains a menu with "User Management" (selected), "Manage Users", "Public Contacts", "Shared Addresses", and "System Presence ACLs". The main content area is titled "User Profile Edit: 50095@dr.avaya.com" and has "Commit" and "Cancel" buttons. The "Identity" tab is active, showing fields for: Last Name (Michaels), First Name (Bret), Middle Name (), Description (), Status (Offline), Update Time (May 27, 2010 4:17:15), Login Name (50095@dr.avaya.com), Authentication Type (Basic), Source (local), Localized Display Name (Michaels, Bret), Endpoint Display Name (Michaels, Bret), Honorific (), Language Preference (English), and Time Zone (). A "Change Password" link is also present. At the bottom, there is an "Address" section and a legend for "*Required".

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 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.
- **@:** 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) associated with the type of endpoint to be added.
- **Set Type:** select “9630SIP” for this video endpoint
- **Security Code:** enter numeric value 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.

The screen shown on the next page displays the Communication Profile information when adding a new SIP user to the sample configuration.

User Profile Edit: 50095@dr.avaya.com

[Commit](#) [Cancel](#)

Identity * Communication Profile * Membership Contacts

Communication Profile

Communication Profile Password:

Confirm Password:

[New](#) [Delete](#) [Done](#) [Cancel](#)

Name

Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

[New](#) [Edit](#) [Delete](#)

<input type="checkbox"/>	Type	Handle	Domain
<input checked="" type="checkbox"/>	Avaya SIP	50095	dr.avaya.com

Select : All, None

Type: Avaya SIP

* Fully Qualified Address: 50095 @ dr.avaya.com

[Add](#) [Cancel](#)

Session Manager Profile

* Primary Session Manager silasm4

Primary	Secondary	Maximum
41	0	41

Secondary Session Manager (None)

Primary	Secondary	Maximum

Origination Application Sequence CMES App Seq 1

Termination Application Sequence CMES App Seq 1

Survivability Server (None)

* Home Location 135.9.88

Endpoint Profile

* System silcm4

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 50095

[Endpoint Editor](#)

Template Select/Reset

Set Type 9630SIP

Security Code

* Port 503852

Voice Mail Number

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

Messaging Profile

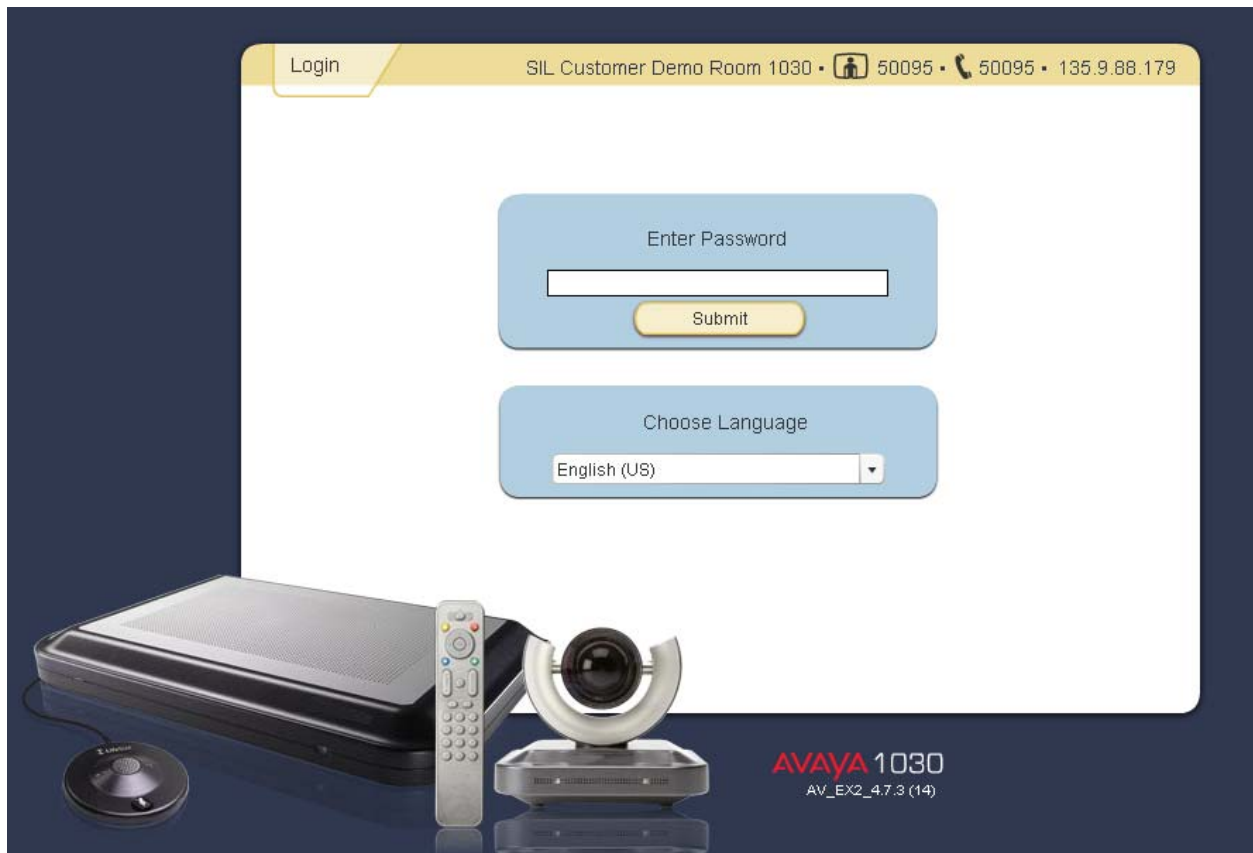
* Required

[Commit](#) [Cancel](#)

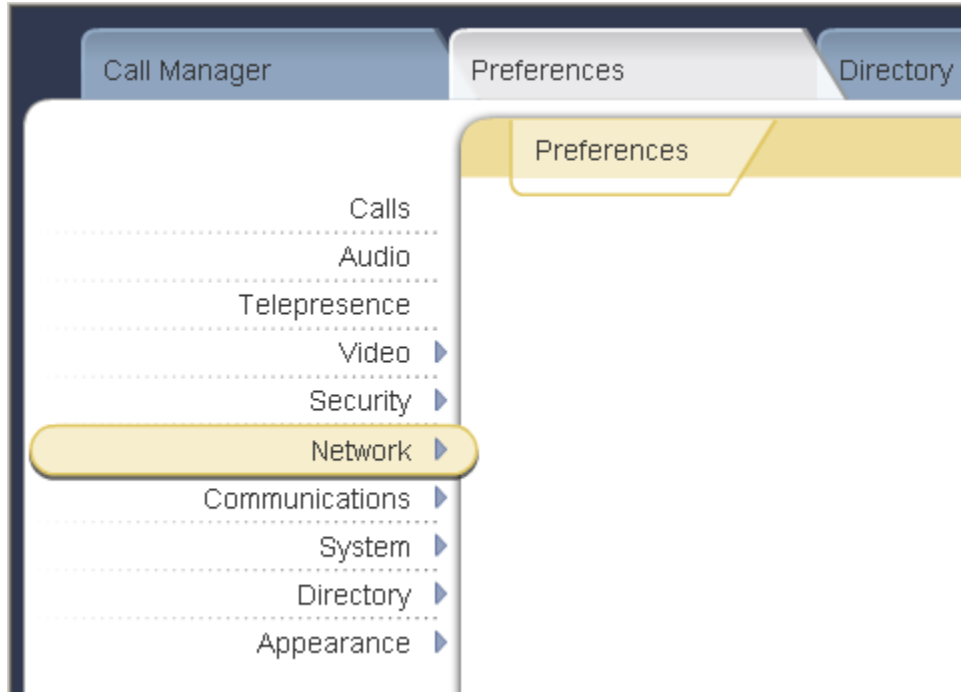
4. Configure Avaya 10x0 Video Endpoint

To administer the 10x0 video endpoints log in to the web interface using the IP address of the video endpoint. You will be redirected to a screen that looks similar to the one below. This is a sample configuration on how to administer a 10x0 video endpoint.

Step 1: Enter the proper login credentials and press **Submit**. Most of the Preferences can be customized to meet your needs. Mentioned below are the absolute necessary items that need to be administered to get the 10x0 up and running on the network.



Once logged in select the **Preferences** tab and then the **Network** option.



Select **General** option and enter values for the following required attributes.

- **DHCP:** select either Enabled/Disabled
- **IP Address:** enter IP Address if DHCP is **disabled**
- **Subnet Mask:** enter Subnet Mask if DHCP is **disabled**
- **Default Gateway:** enter Default Gateway if DHCP is **disabled**
- **Hostname:** enter the appropriate Hostname
- **DNS Servers:** enter the appropriate DNS Servers
- **NTP Server Hostname:** enter NTP Server Hostname

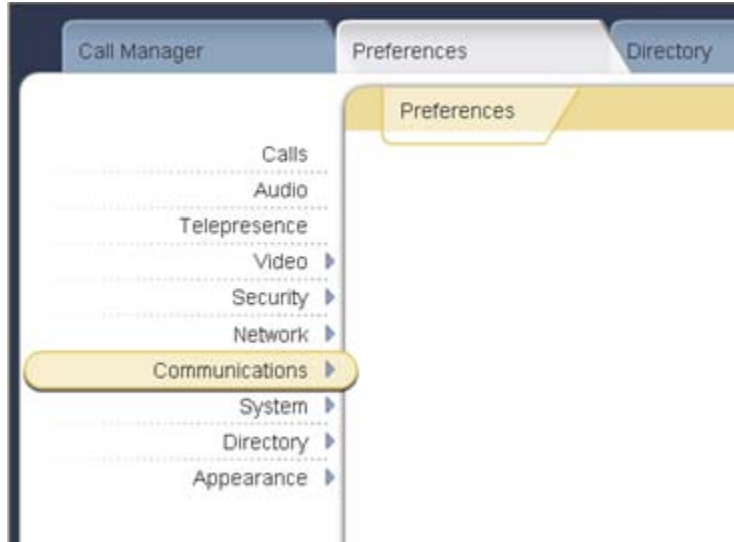
Select the **Save Changes** button to save the administration just added.

The screenshot shows the Avaya 1030 web interface for network configuration. The 'Preferences' tab is selected, and the 'General' sub-tab is active. The page title is 'Network • General' and the user is logged in as 'SIL Customer Demo Room 1030'. The configuration fields are as follows:

- DHCP: Enabled (dropdown)
- IP Address: (empty text field)
- Subnet Mask: 255.255.255.0 (text field)
- Default Gateway: 135.9.88.254 (text field)
- Hostname: SILVideo4 (text field)
- DNS Servers: 135.9.88.50 135.9.1.2 (text field)
- Name Search Domains: (empty text field)
- Network Speed: Auto (dropdown)
- VLAN Tag: (empty text field)
- NTP Server Hostname: (empty text field)
- 802.1x Authentication: Disabled (dropdown)

At the bottom, there are four buttons: 'Save Changes' (highlighted with a red box), 'Cancel Changes', 'Refresh', and 'Copy'. A footer note states: 'IP Address: Enter the static IP address of the device.' The bottom left corner shows 'AVAYA 1030 AV_EX2_4.7.3 (14)' and the bottom right corner has 'Remote Control' and 'Log out' buttons.

Select the **Preferences** option and select the **Communications** option.



Select the **SIP** option.

- **SIP:** select Enabled
- **SIP Username:** enter the SIP Username for the device. **NOTE:** The SIP Username should be unique and meaningful to the endpoint.
- **Authorization Name:** enter the SIP Server authorization username. **NOTE:** The Authorization Name should be the extension number that is used to register the SIP endpoint defined in **Section 3.3.7**
- **Authorization Password:** enter the SIP Server authorization password which should match the Shared Communication Profile Password defined in **Section 3.3.7**
- **SIP Registration:** select the communication path to use when registering with a SIP Registrar
- **SIP Proxy:** choose 'Enabled' to use the SIP proxy
- **Proxy Hostname:** enter the hostname or IP address of the SIP proxy server. **NOTE:** This is the Session Manager software asset card IP address
- **Proxy IP Port:** enter the IP port number of SIP proxy server
- **SIP Registrar:** choose 'Enabled' to use the SIP registrar
- **Registrar Hostname:** enter the hostname or IP address of the SIP registrar server

The screenshot shows the Avaya 1030 web interface with the 'SIP' configuration page selected. The page title is 'Communications • SIP' and the status bar shows 'SIL Customer Demo Room 1030 • 50095 • 50095 • 135.9.88.179'. The left sidebar has 'SIP' highlighted under 'Preferences'. The main content area contains the following fields:

- Registrar Status: Registered
- SIP: Enabled (dropdown)
- SIP Username: 50095
- Authorization Name: 50095
- Authorization Password: *****
- SIP Registration: Through Proxy (dropdown)
- SIP Proxy: Enabled (dropdown)
- Proxy Hostname: 135.9.88.62
- Proxy IP Port: 5060
- SIP Registrar: Enabled (dropdown)
- Registrar Hostname: 135.9.88.62
- Registrar IP Port: 5060

At the bottom, there are buttons for 'Save Changes', 'Cancel Changes', 'Refresh', and 'Copy'. A tooltip for 'Registrar Hostname' is visible, stating: 'Enter the hostname or IP address of the SIP registrar server.' The bottom left corner shows 'AVAYA 1030 AV_EX2_4.7.3 (14)' and the bottom right corner has 'Remote Control' and 'X Log out' buttons.

- **Registrar IP Port:** enter the IP port number of the SIP registrar server
- **UDP Signaling Port:** enter the UDP port number of the SIP configuration
- **TCP Signaling:** choose 'Enable' to use TCP for placing SIP call
- **TCP signaling Port:** enter the TCP port number of the SIP configuration

Select the **Save Changes** button to save the administration just added.

Registrar IP Port: 5060

UDP Signaling Port: 5060

TCP Signaling: Enabled

TCP Signaling Port: 5060

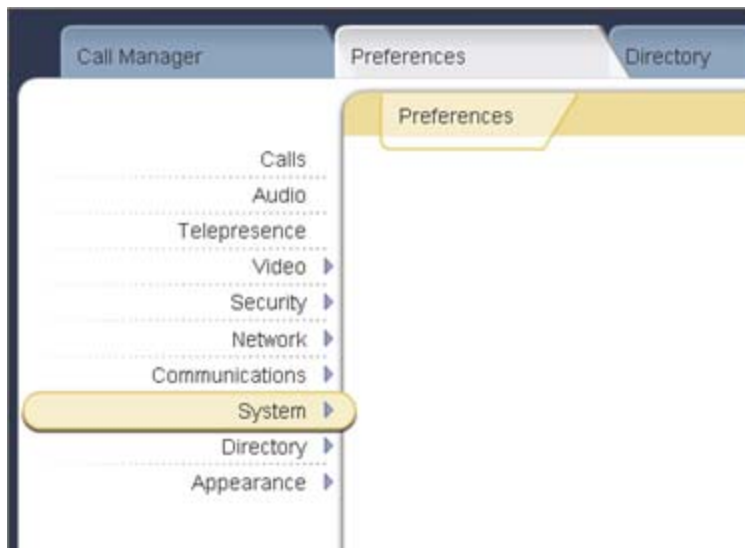
Save Changes Cancel Changes Refresh Copy

? Proxy Hostname:
Enter the hostname or IP address of the SIP proxy server.

AVAYA 1030
AV_EX2_4.7.3 (14)

Remote Control X Log out

Select the **Preferences** option again and select **System**.



Select the **Identification** option. This option will allow the user to display the name and video/voice numbers on the menu bar.

- **System Name:** enter a descriptive name for the system
- **Video Number:** enter the video number of the endpoint
- **Voice Number:** enter the voice number of the endpoint

Select the **Save Changes** button to save the administration just added.

The screenshot displays the Avaya 1030 web interface. The top navigation bar includes tabs for Call Manager, Preferences, Directory, Diagnostics, and Maintenance. The left sidebar shows a tree view with 'Identification' selected. The main content area is titled 'System • Identification' and shows the configuration for 'SIL Customer Demo Room 1030'. The configuration fields are:

- System Name: SIL Customer Demo Room 1030
- Video Number: 50095
- Voice Number: 50095
- Location: United States

Red boxes and arrows highlight the 'Save Changes' button and the fields being edited. The bottom of the page shows the 'AVAYA 1030' logo and version 'AV_EX2_4.7.3 (14)'. The bottom right corner has buttons for 'Remote Control' and 'Log out'.


5. Verification Steps

5.1. Verify Avaya Aura[®] Session Manager Configuration

5.1.1. Verify Avaya Aura[®] Session Manager is Operational

Navigate to **Elements** → **Session Manager** → **Dashboard**

Verify the overall system status for Session Manager as shown below:

 Avaya Aura[™] System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System Tools

Home / Elements / Session Manager / Dashboard - Dashboard

Help ?

Session Manager Dashboard

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

Session Manager Instances

Service State Shutdown System As of 12:52 PM

5 Items Refresh Show ALL Filter: Enable

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/> silasm3	Core	0/0/0		---	---	---	---	---	---
<input type="checkbox"/> silasm4	Core	0/0/0		Up	Accept New Service	0/14	0	12	6.1.0.0.610023
<input type="checkbox"/> silasm5	Core	0/0/12		Up	Accept New Service	0/6	0	0	6.1.0.0.610023
<input type="checkbox"/> silasm6	Core	0/3/222		Up	Accept New Service	0/7	0	0	6.1.0.0.610023
<input type="checkbox"/> silbsm1-slp	BSM	6/92/3		Up	Deny New Service	---	0	0	6.0.0.0.600019

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.

Avaya Aura™ System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager

Home

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

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

The following errors have occurred:
Unable to access status information for Security Modules, silasm3 - cannot connect to server, internal error.

Reset Synchronize Update Installed Certificates Connection Status

5 Items Refresh Show ALL Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)
	Show	silasm6	SM	Up	9	135.9.228.36/24	---	135.9.228.254	Disabled	7/7
	Show	silasm4	SM	Up	51	135.9.88.62/24	---	135.9.88.254	Disabled	14/14
	Show	silasm3	SM	---	---	---	---	---	Disabled	---
	Show	silbsm1-sip	BSM	Up	17	135.9.88.186/24	---	135.9.88.254	Disabled	2/2
	Show	silasm5	SM	Up	8	135.9.228.31/24	---	135.9.228.254	Disabled	6/6

Select : None

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 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

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

SIP Entity Link Monitoring Status Summary

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

The following errors have occurred:

Unable to access SIP monitoring data from Session Manager, silasm3 - cannot connect to server.

Entity Link Status for All Session Manager Instances

Run Monitor

4 Items Refresh

<input type="checkbox"/>	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
<input checked="" type="checkbox"/>	silasm4	0 / 14	0	0	1
<input checked="" type="checkbox"/>	silasm5	0 / 6	0	0	1
<input checked="" type="checkbox"/>	silasm6	0 / 7	0	0	1
<input type="checkbox"/>	silasm3	---	---	---	---

Select : All, None

All Monitored SIP Entities

Run Monitor

20 Items Refresh Show 15 Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	cm4 CLAN 01a10
<input type="checkbox"/>	cm4 CLAN 01a11
<input type="checkbox"/>	CMFS1
<input type="checkbox"/>	CMFSTG
<input type="checkbox"/>	CS1K_Rel7_5
<input type="checkbox"/>	G860-OC3-TP8
<input type="checkbox"/>	G860-OC3-TP9
<input type="checkbox"/>	iras-MPPs
<input type="checkbox"/>	m3kTPglobal
<input type="checkbox"/>	Presence-Element
<input type="checkbox"/>	s8800_cmes
<input type="checkbox"/>	sil-sbc
<input type="checkbox"/>	silasm3
<input type="checkbox"/>	silasm4
<input type="checkbox"/>	silasm5

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

5.1.3. Verify Registrations of SIP Endpoints

Verify SIP users have been created in the Session Manager. In the sample configuration, Extension 50095 SIP user was created as shown in the highlighted area below:

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail reads 'Home /Users / User Management / Manage Users- User Management'. The left sidebar contains a 'User Management' menu with sub-items: 'Manage Users', 'Public Contacts', 'Shared Addresses', and 'System Presence ACLs'. The main content area is titled 'User Management' and features a 'Users' section with buttons for 'View', 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these buttons is a table of users. The first row of the table is highlighted with a red border. The table has columns for 'Status', 'Name', 'Login Name', 'E164 Handle', and 'Last Login'.

Status	Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>	Michaels, Bret	50095@dr.avaya.com	50095	
<input type="checkbox"/>	SIL Video Lab	55000@dr.avaya.com	55000	

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



[Session Manager](#) [Home](#)

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location

Network Configuration

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Registration Summary

User Registrations

System Tools

Home / Elements / Session Manager / System Status / User Registrations- User Registrations

User Registrations

Select rows to send notifications to AST devices. Click on Details column for complete registration status.

AST Device Notifications:

Reboot

Reload

Failback

As of 4:30 PM

42 Items

Refresh

Show 15

Filter: Enable

	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
									Prim	Sec	Surv
<input checked="" type="checkbox"/>	Hide	50095@dr.avaya.com	50095@dr.avaya.com	Bret	Michaels	135.9.88	135.9.88.179:5060	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>

Registration Detail

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

silasm4

Secondary SM

Survivable SM

Active Controller

silasm4

Registration Time

Thu Dec 16 13:38:19 MST 2010

Event Subscriptions

IP Address

135.9.88.179:5060

MAC Address

00:04:0d:ed:cc:4a

Device Vendor

Avaya

Device Type

lone-X Deskphone

Device Model

9620

Device Version

2.6.0

<input type="checkbox"/>	Show	---	55000@dr.avaya.com	SIL	Video Lab	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	55001@dr.avaya.com	55001@dr.avaya.com	Tom	Martinez	135.9.88	135.9.88.191:5060	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	55002@dr.avaya.com	55002@dr.avaya.com	SIL Demo	Video Lab	135.9.88	135.9.88.198:5060	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55003@dr.avaya.com	SIL Video	Lab 1XC	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55004@dr.avaya.com	SIL Demo	Room 1XC	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	55005@dr.avaya.com	55005@dr.avaya.com	1xC-1	x55005	135.9.88	135.9.88.237:5061	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55006@dr.avaya.com	Mojo1	x55006	20.20.20	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55007@dr.avaya.com	Mojo2	x55007	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55008@dr.avaya.com	SIL	Video Lab Mojo3	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55009@dr.avaya.com	1XC-2	x55009	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55010@dr.avaya.com	1XC-3	x55010	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55011@dr.avaya.com	Bob	McAdoo	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55012@dr.avaya.com	Cousin	MoJo	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Show	---	55013@dr.avaya.com	2ndCousin	MoJo	135.9.88	---	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select : All, None

< Previous Page 1 of 3 Next >

TJM Reviewed:
SPOC 2/8/2011

Solution Interoperability Lab Application Notes
©2011 Avaya Inc. All Rights Reserved.

38 of 45
SM61_ES601_10x0

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 12/20/2010 CM Release String cold-00.1.510.1-18599	
18:32:41	SIP<INVITE sip:55001@dr.avaya.com;transport=tcp SIP/2.0	
18:32:41	dial 55001# route:UDP AAR	
18:32:41	term trunk-group 10 cid 0x13fe	
18:32:41	dial 55001# 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 [135.9.88.191]:60304	
	rgn:2 [135.9.88.179]:60040	
18:32:44	G711MU ss:off ps:20	
	rgn:2 [135.9.88.179]:60040	
	rgn:2 [135.9.88.191]:60304	
18:32:44	SIP>SIP/2.0 200 OK	
18:32:44	Video: H264 [135.9.88.191]:60306	
18:32:44	Video: H264 [135.9.88.179]:60042	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:32:44	Video: H264 [135.9.88.179]:60042	
18:32:44	Video: H264 [135.9.88.191]:60306	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:32:44	SIP>INFO sip:50095@135.9.88.179;transport=tcp SIP/2.0	
18:32:44	SIP<ACK sip:55001@135.9.88.13;transport=tcp SIP/2.0	
18:32:44	SIP<SIP/2.0 200 OK	
18:32:51	SIP<BYE sip:55001@135.9.88.13;transport=tcp SIP/2.0	
18:32:51	SIP>SIP/2.0 200 OK	
18:32:51	idle station 50095 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 50095		Page 1
LIST TRACE		
time	data	
18:35:36	TRACE STARTED 12/20/2010 CM Release String cold-00.1.510.1-18599	
18:36:13	active station 50095 cid 0x13ff	
18:36:13	SIP>INVITE sip:55001@dr.avaya.com SIP/2.0	
18:36:13	dial 55001# route:UDP AAR	
18:36:13	term trunk-group 10 cid 0x13ff	
18:36:13	dial 55001# 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 55001	
18:36:13	Calling Number & Name *50095 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:55001@dr.avaya.com SIP/2.0	
18:36:13	SIP>INVITE sip:55001@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 [135.9.88.191]:60312	
	rgn:2 [135.9.88.179]:60048	
18:36:15	G711MU ss:off ps:20	
	rgn:2 [135.9.88.179]:60048	
	rgn:2 [135.9.88.191]:60312	
18:36:15	Video: H264 [135.9.88.191]:60314	
18:36:15	Video: H264 [135.9.88.179]:60050	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:36:15	Video: H264 [135.9.88.179]:60050	
18:36:15	Video: H264 [135.9.88.191]:60314	
	logChl:110 sessId:2 bw:21760 tx/rx:11520	
18:36:16	SIP<INFO sip:+50095@135.9.88.13;transport=tcp SIP/2.0	
18:36:16	SIP>SIP/2.0 200 OK	
18:36:16	SIP>ACK sip:55001@135.9.88.72;transport=tcp SIP/2.0	
18:36:22	SIP>BYE sip:55001@135.9.88.72;transport=tcp SIP/2.0	
18:36:22	idle station 50095 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 1020/1030/1040 video endpoint registered to SM (CMES) to another 1020/1030/1040 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 10x0 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 1020/1030/1040 video endpoint registered on SM (CMES). Answer the call and verify two-way video and talk path. Place a video conference call from 1040 to a 1020. 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 1020/1030/1040 video endpoint registered to SM (CMES) to another 1020/1030/1040 video endpoint registered on SM (CMES). Answer the call and verify two-way talk path for all combinations of calls between 10X0 video endpoints. Verify Call statistics on the endpoint GUI.
- Place a point-to-point audio call from a 1040 video endpoint registered to SM (CMES) to another 1020/1030/1040 video endpoint registered on SM (CMES). Answer the call and verify two-way talk path. Place an audio conference call from 1040 to a 1020/1030/1040. Answer the call and verify talk path on conference call. Add a fourth video endpoint to the call and verify 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 1020/1030/1040 video endpoint registered to SM (CMES) to another 1020/1030/1040 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 10x0 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 1020/1030/1040 video endpoint registered on SM (CMES). Answer the call and verify two-way video and talk path. Place a video conference call from 1040 to a 1020. 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 1020/1030/1040 video endpoint registered to SM (CMES) to another 1020/1030/1040 video endpoint registered on SM (CMES). Answer the call and verify two-way talk path for all combinations of calls between 10X0 video endpoints. Verify Call statistics on the endpoint GUI.
- Place a point-to-point audio call from a 1040 video endpoint registered to SM (CMES) to another 1020/1030/1040 video endpoint registered on SM (CMES). Answer the call and verify two-way talk path. Place an audio conference call from 1040 to a 1020/1030/1040. Answer the call and verify talk path on conference call. Add a fourth video endpoint to the call and verify 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 a Evolution Server to support the Avaya 10x0 Series 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 1040. 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) Avaya Aura[®] Session Manager Case Studies, dated January 2, 2010, available at <http://support.avaya.com>
- 4) Maintaining and Troubleshooting Avaya Aura[®] Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

Communication Manager

- 5) 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
- 6) SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206, May 2009, available at <http://support.avaya.com>.
- 7) Administering Avaya Aura® Communication Manager, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.
- 8) Administering Avaya Aura® Communication Manager as a Feature Server, Doc ID 03-603479, November 2009, available at <http://support.avaya.com>

Avaya 1000 Series Video Endpoints

- 9) Avaya 1010/1020 Installation Guide, Issue 1, June 2010, available at <http://support.avaya.com>
- 10) Avaya 1010/1020 User Guide, Issue 1, June 2010, available at <http://support.avaya.com>
- 11) Avaya 1030 Installation Guide, Issue 1, June 2010, available at <http://support.avaya.com>
- 12) Avaya 1040 Installation Guide, Issue 1, June 2010, available at <http://support.avaya.com>
- 13) Avaya 1050 Installation Guide, Issue 1, June 2010, available at <http://support.avaya.com>
- 14) Avaya Video Communications System Administrator Guide (1050/1040/1030) , Issue 1, June 2010, available at <http://support.avaya.com>
- 15) Avaya Video Communications System User Guide (1050/1040/1030) , Issue 1, June 2010, available at <http://support.avaya.com>
- 16) Avaya Video Camera 100 Installation Guide, Issue 1, June 2010, available at <http://support.avaya.com>
- 17) Avaya Video Conferencing Manager Deployment Guide, Issue 1, June 2010, available at <http://support.avaya.com>

©2011 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