



Avaya Solution & Interoperability Test Lab

Configuring Avaya 9600 Series IP Deskphones running Avaya one-X® SIP firmware with Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Feature Server Release 6.0.1 – Issue 1.0

Abstract

These Application Notes describe the configuration of Avaya 9600 Series IP Deskphones running Avaya one-X® SIP firmware with Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Feature Server Release 6.0.1.

- 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 serves as a Feature Server within the Avaya Aura® architecture and supports the SIP endpoints registered to Avaya Aura® Session Manager.

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
2. Equipment and Software Validated.....	6
3. Configure Avaya Aura® Communication Manager Feature Server	7
3.1. Verify System Capacities and Licensing	7
3.1.1. Verify Off-PBX Telephones Capacity	8
3.1.2. Verify SIP Trunk Capacity	8
3.1.3. Verify AAR/ARS Routing is Enabled	9
3.1.4. Verify Private Networking is Enabled	9
3.2. Configure Trunk-to-Trunk Transfers	10
3.3. Configure IP Codec Set	10
3.4. Configure IP Network Region	11
3.5. Add Node Names and IP Addresses	11
3.6. Configure SIP Signaling Groups and Trunk Groups	12
3.6.1. Add Signaling Groups for SIP Trunks.....	12
3.6.2. Add SIP Trunk Groups	13
3.7. Configure Route Pattern	15
3.8. Administer Private Numbering Plan	16
3.9. Administer AAR Analysis	17
3.10. Configure Stations	17
3.11. Verify Off-PBX-Telephone Station-Mapping	19
3.12. Save Translations	20
4. Configure Avaya Aura® Session Manager	20
4.1. Define SIP Domains	21
4.2. Define Locations	22
4.3. Define SIP Entities.....	23
4.4. Define Entity Links	24
4.5. Define Entity Link between Avaya Aura® Session Managers.....	25
4.6. Define Routing Policy	26
4.7. Define Dial Pattern.....	27
4.8. Define Application.....	28
4.9. Define Application Sequence.....	29
4.10. Add SIP Users	30
4.11. Synchronize Changes with Avaya Aura® Communication Manager	34

5.	Configure Avaya Aura® Communication Manager Evolution Server	35
5.1.	Verify System Capabilities and Licensing	35
5.1.1.	Verify SIP Trunk Capacity	35
5.1.2.	Verify AAR/ARS Routing is Enabled	35
5.1.3.	Verify Private Numbering.....	35
5.2.	Configure Trunk-to-Trunk Transfers	36
5.3.	Configure IP Codec Set.....	36
5.4.	Configure IP Network Region	36
5.5.	Add Node Names and IP Addresses	36
5.6.	Configure SIP Signaling Groups and Trunk Groups	37
5.6.1.	Create Signaling Groups for SIP Trunks	37
5.6.2.	Add SIP Trunk Groups	37
5.7.	Configure Route Pattern.....	38
5.8.	Administer Numbering Plan	39
5.8.1.	Administer Uniform Dialplan	39
5.8.2.	Administer AAR analysis	39
6.	Manual Configuration of Avaya 9600 Series IP Deskphones	40
6.1.	Configuring IP Addresses	40
6.2.	Configure SIP Global and Proxy Settings	42
7.	Verification Steps.....	45
7.1.	Verify Avaya Aura® Session Manager Configuration	45
7.2.	Verify Avaya Aura® Communication Manager Feature Server.....	48
7.3.	Call Scenarios Verified	51
8.	Acronyms.....	52
9.	Conclusion.....	53
10.	Additional References.....	54

1. Introduction

These Application Notes present a sample configuration for a network that uses two Avaya Aura® Session Managers to support registration of Avaya 9600 Series SIP endpoints. Two Session Managers are deployed so that one Session Manager can serve as backup for the other in case of a network or Session Manager failure.

As shown in **Figure 1**, Avaya 9600 Series Deskphones configured as SIP endpoints utilize the Avaya Aura® Session Manager User Registration feature and are supported by Avaya Aura® Communication Manager Feature Server. To improve reliability of the configuration, SIP endpoints are registered to both Session Managers.

The sample configuration includes Avaya Aura® Communication Manager Feature Server supporting IP Multimedia Subsystem (IMS) SIP users registered to Avaya Aura® Session Manager. When Communication Manager is configured as a Feature Server, it uses the half call model defined in the IMS architecture. With this model, an Origination Application Sequence is applied to the originator of the call and a Termination Application Sequence is applied to the recipient of the call. For more information regarding configuring Communication Manager as a Feature Server, see **Reference [8]** in **Section 10**.

Avaya Aura® Communication Manager Feature Server is connected to both Session Managers via IMS-enabled SIP signaling groups and associated SIP trunk groups.

Avaya 9600 Series IP Deskphones (running Avaya one-X® H.323 firmware) and other non-SIP endpoints such as 2420 Digital Telephones are supported by a second Avaya Aura® Communication Manager which serves as an Evolution Server within the Avaya Aura® architecture. Communication Manager Evolution Server is also connected over SIP trunks to both Session Managers.

All intra-system calls are carried over these SIP trunks.

Avaya Aura® Session Manager is managed by Avaya Aura® System Manager. For the sample configuration, two Avaya Aura® Session Managers running on separate Avaya S8800 Servers are deployed as a pair of active-active redundant servers. Avaya Aura® Communication Manager Feature Server runs on an Avaya S8300 server with Avaya 450 Gateway.

These Application Notes will focus on the configuration of the SIP telephones, SIP trunks and call routing. Detailed administration of other aspects of Communication Manager Feature Server, Communication Manager Evolution Server, or Session Manager will not be described. See the appropriate documentation listed in **Section 10** for more information.

Note: IP addresses have been partially hidden in **Figure 1** for security.

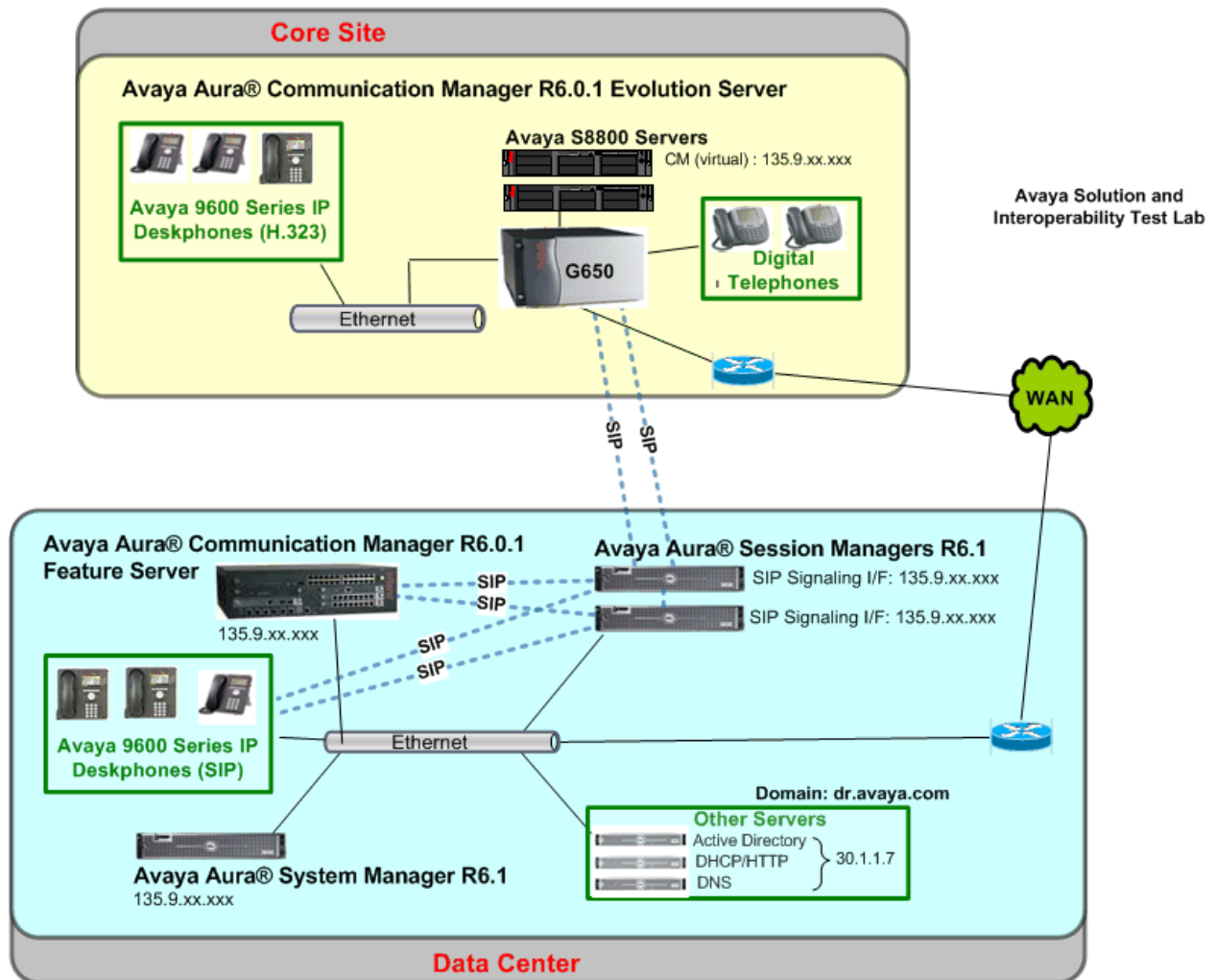


Figure 1 – Sample Configuration

2. Equipment and Software Validated

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

Component	Software Version
Avaya Aura® Session Manager on Avaya S8800 Server	Release 6.1 Build 6.1.0.0.610023
Avaya Aura® System Manager	Release 6.1 Version: 6.1.0.4.5072-6.1.4.11
Avaya Aura® Communication Manager Feature Server on Avaya S8300 Media Server	Release 6.0.1, SP1 Version R16x.00.1.510.1-18777
Avaya Aura® Communication Manager Evolution Server • Duplicated Avaya S8800 Servers • Avaya G650 Media Gateway	Release 6.0.1, SP1 Version R16x.00.1.510.1-18777
Avaya 9600 Series IP Deskphones (with Avaya one-X® SIP firmware)	Release 2.6.4
Avaya 9600 Series IP Deskphones (with Avaya one-X® H.323 firmware)	Release 3.1, version 111510
Avaya 9601 Series IP Deskphones (with Avaya one-X® SIP firmware)	Release 6.0.1, version 1r22_V4r52
Avaya 9601 IP Deskphone (with Avaya one-X® SIP firmware)	Release 6.0, version 1.0.11.3
Avaya 9601 Series IP Deskphone (with Avaya one-X® H.323 firmware)	Release 6.1, version: 031811 (r33)
Avaya Digital Telephones (2420D)	N/A

3. Configure Avaya Aura® Communication Manager Feature Server

This section describes the steps needed to configure SIP trunks between Communication Manager Feature Server and both Session Managers to support calls between SIP telephones and stations on Communication Manager Evolution Server. These instructions assume the Avaya G450 Media Server is already configured on Communication Manager Feature Server. For information on how to administer these other aspects of Communication Manager Feature Server, see **References [5] through [10]** in **Section 10**.

This section describes the administration of Communication Manager Feature Server using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity.

The following administration steps will be described:

- Verify System Capabilities and Capacities
- Configure Trunk-to-Trunk Transfers
- Configure IP Codec Set
- Configure IP Network Region
- Configure IP Node Names and IP Addresses
- Configure SIP Signaling Groups and Trunk Groups
- Configure Route Pattern
- Administer Private Numbering Plan
- Administer AAR Analysis
- Configure Stations
- Verify Off-PBX-Telephone Station Mapping

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

3.1. Verify System Capacities and Licensing

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

3.1.1. Verify Off-PBX Telephones Capacity

On **Page 1** of the **display system-parameters customer-options** command, verify an adequate number of Off-PBX Stations (OPS) Telephones are administered for the system as shown below.

display system-parameters customer-options					Page	1 of	11
OPTIONAL FEATURES							
G3 Version: V16		Software Package: Enterprise					
Location: 2		System ID (SID): 1					
USED							
		Platform Maximum Ports: 6400				55	
...							
		Maximum Off-PBX Telephones - EC500: 9600				0	
		Maximum Off-PBX Telephones - OPS: 9600				11	
		Maximum Off-PBX Telephones - PBFMC: 9600				0	
...							

3.1.2. Verify SIP Trunk Capacity

On **Page 2** of the **display system-parameters customer-options** command, verify an adequate number of SIP Trunk Members are administered 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:			500	0	
Maximum Concurrently Registered IP Stations:			18000	0	
Max Concur Registered Unauthenticated H.323 Stations:			100	0	
...					
Maximum Video Capable IP Softphones:			0	0	
Maximum Administered SIP Trunks:			4000	40	
...					

3.1.3. Verify AAR/ARS Routing is Enabled

To simplify the dialing plan for calls between SIP endpoints and other types of stations on Communication Manager Evolution Server, verify the following AAR/ARS features are enabled on the system.

On **Page 3** of **system-parameters customer-options** command, verify the following features are enabled.

- **ARS?** Enter “y”.
- **ARS/AAR Partitioning?** Enter “y”.
- **ARS/AAR Dialing without FAC?** Enter “y”.

```
display system-parameters customer-options                               Page   3 of  11
                                OPTIONAL FEATURES

A/D Grp/Sys List Dialing Start at 01? n                               CAS Main? n
Answer Supervision by Call Classifier? n                             Change COR by FAC? n
                                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? n
...
```

3.1.4. Verify Private Networking is Enabled

On **Page 5** of **display system-parameters customer options** command, verify the **Private Networking** feature is set to “y”.

```
display system-parameters customer-options                               Page   5 of  11
                                OPTIONAL FEATURES

Port Network Support? y                                               Time of Day Routing? n
Posted Messages? n TN2501 VAL Maximum Capacity? y
                                Uniform Dialing Plan? y
                                Private Networking? y Usage Allocation Enhancements? y
Processor and System MSP? y
Processor Ethernet? y                                               Wideband Switching? n
...
```

3.2. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when an incoming call to a SIP station is transferred to a station on Communication Manager Evolution Server. For simplicity, the **Trunk-to-Trunk Transfer** field on **Page 1** was set to “**all**” to enable all trunk-to-trunk transfers on a system wide basis.

Note: Enabling this feature poses significant security risk by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, a COS could be defined to allow trunk-to-trunk transfers for specific trunk group(s). For more information regarding how to configure Communication Manager to minimize toll fraud, see **Reference [10]** in **Section 10**.

change system-parameters features	Page 1 of 18
FEATURE-RELATED SYSTEM PARAMETERS	
Self Station Display Enabled? n	
Trunk-to-Trunk Transfer: all	
Automatic Callback with Called Party Queuing? n	
Automatic Callback - No Answer Timeout Interval (rings): 3	
...	

3.3. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is the number used to identify the codec set.

Enter the following values:

- **Audio Codec:** Enter “**G.711MU**” and “**G.729**” as supported types.
- **Silence Suppression:** Retain the default value “**n**”.
- **Frames Per Pkt:** Enter “**2**”.
- **Packet Size (ms):** Enter “**20**”.
- **Media Encryption:** Enter the value based on the system requirement.
For the sample configuration, “**none**” was used.

change ip-codec-set 2

Page 1 of 2

IP Codec Set

Codec Set: 2

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

Media Encryption

1: none

3.4. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is an available network region.

Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration.
For the sample configuration, “**dr.avaya.com**” was used.
- **Name:** Enter descriptive name.
- **Codec Set:** Enter the number of the IP codec set configured in **Section 3.3.**
- **Intra-region IP-IP Direct Audio:** Enter “yes”.
- **Inter-region IP-IP Direct Audio:** Enter “yes”.

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: Authoritative Domain: dr.avaya.com		
Name: SIP calls for ASM		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 2		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? n
UDP Port Max: 16585		
...		

3.5. Add Node Names and IP Addresses

Use the **change node-names ip** command to add the node-name and IP Addresses for the “**procr**” interface on Communication Manager and the SIP signaling interface of each Session Manager, if not previously added.

In the sample configuration, the node-name of the SIP signaling interface for the first Session Manager is “**silasm3**” with an IP address of “**135.9.xx.xxx**”. The node-name of SIP signaling interface for the second Session Manager is “**silasm4**” with an IP address of “**135.9.xx.xxx**”.

Note: IP addresses have been partially hidden for security.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
silasm3	135.9.xx.xxx	
silasm4	135.9.xx.xxx	
default	0.0.0.0	
procr	135.9.xx.xxx	
gateway1	10.80.100.1	

3.6. Configure SIP Signaling Groups and Trunk Groups

3.6.1. Add Signaling Groups for SIP Trunks

Use the **add signaling-group n** command, where **n** is an available signaling group number to create SIP signaling groups. In the sample configuration, trunk groups “**1**” and “**10**” and signaling groups “**1**” and “**10**” were used for connecting to both Session Managers.

Enter the following values and use default values for remaining fields.

- **Group Type:** Enter “**sip**”.
- **IMS Enabled:** Enter “**y**”.
- **Transport Method:** Enter “**tcp**”.
- **Peer Detection Enabled?** Enter “**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:** Enter “**procr**” node name from **Section 3.5**.
- **Far-end Node Name:** Enter node name for the first Session Manager defined in **Section 3.5**.
- **Near-end Listen Port:** Verify “**5060**” is used.
- **Far-end Listen Port:** Verify “**5060**” is used.
- **Far-end Network Region:** Enter network region defined in **Section 3.4**.
- **Far-end Domain:** Enter domain name for **Authoritative Domain** field defined in **Section 3.4**.
- **DTMF over IP:** Verify “**rtp-payload**” is used.

Note: TCP was used in the sample configuration. However, TLS would typically be used in production environments.

add signaling-group 10		Page 1 of 1
SIGNALING GROUP		
Group Number: 10	Group Type: sip	
IMS Enabled? y	Transport Method: tcp	
Q-SIP? n		SIP Enabled LSP? n
IP Video? n		
Peer Detection Enabled? y	Peer Server: others	
Near-end Node Name: procr	Far-end Node Name: silasm3	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
Far-end Domain: dr.avaya.com	Far-end Network Region: 1	
DTMF over IP: rtp-payload	Bypass If IP Threshold Exceeded? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

Repeat this step to define a second signaling group to connect to the second Session Manager.

3.6.2. Add SIP Trunk Groups

Add the corresponding trunk groups controlled by the signaling groups defined **Section 3.6.1** using the **add trunk-group n** command where **n** is an available trunk group number.

Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Group Type:** Enter “**sip**”.
- **Group Name:** Enter a descriptive name.
- **TAC:** Enter an available trunk access code.
- **Direction:** Enter “**two-way**”.
- **Outgoing Display?** Enter “**y**”.
- **Service Type:** Enter “**tie**”.
- **Signaling Group:** Enter the number of the signaling group added in **Section 3.6.1**.
- **Number of Members:** Enter the number of members in the SIP trunk (must be within the limits for number of SIP trunks configured in **Section 3.1.2**).

Note: once the **add trunk-group** command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

add trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: SIP-IMS to SILASM3	COR: 1	TN: 1	TAC: #10
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: 20			

On **Page 2**, set the **Preferred Minimum Session Refresh Interval:** field 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**, fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Numbering Format** Enter **“private”**.
- **Show ANSWERED BY on Display** Enter **“y”**.

add trunk-group 10	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	UI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
Show ANSWERED BY on Display? y	

On **Page 4**, fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Support Request History** Enter **“y”**.
- **Telephone Event Payload Type** Enter **“120”**.

add trunk-group 10	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? y	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 120	

Repeat this step to define a SIP trunk group to connect to the second Session Manager.

3.7. Configure Route Pattern

This section provides the configuration of the route pattern used in the sample configuration for routing calls between stations on Communication Manager Evolution Server and SIP endpoints supported by Communication Manager Feature Server. To support routing when the primary Session Manager is not available, the route pattern should be configured to use look-ahead routing (LAR) to select a secondary route.

Use **change route-pattern n** command where **n** is an available route pattern.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Grp No** Enter a row for each trunk group defined in **Section 3.6.2**.
- **FRL** Enter **"0"**.
- **Numbering Format** Enter **"lev0-pvt"**.
- **LAR** Enter **"next"** for first row. Use default value for second row.

In the sample configuration, route pattern **"1"** was created as shown below.

change route-pattern 1												Page 1 of 3			
Pattern Number: 1 Pattern Name: IMS SIP to ASM															
SCCAN? n Secure SIP? n															
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits					QSIG			
							Dgts					Intw			
1:	1	0									n	user			
2:	10	0									n	user			
3:									n	user					
4:									n	user					
5:									n	user					
6:									n	user					
BCC		VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature		PARM	No.	Numbering	LAR
0	1	2	M	4	W	Request							Dgts	Format	
													Subaddress		
1:	y	y	y	y	y	n	n	rest					lev0-pvt	next	
2:	y	y	y	y	y	n	n	rest					lev0-pvt	none	
3:	y	y	y	y	y	n	n	rest						none	
4:	y	y	y	y	y	n	n	rest						none	
...															

3.8. Administer Private Numbering Plan

Extension numbers used for SIP Users registered to Session Manager must be added to either the private or public numbering table on Communication Manager Feature Server. For the sample configuration, private numbering was used and all extension numbers were unique within the private 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 **Reference [7]** in **Section 10**.

Use the **change private-numbering n** command, where **n** is the length of the private number.

Fill in the indicated fields as shown below.

- **Ext Len:** Enter length of extension numbers.
In the sample configuration, “5” was used.
- **Ext Code:** Enter leading digit (s) from extension number.
In the sample configuration, “506” was used.
- **Trk Grp(s):** Enter trunk groups defined in **Section 3.6.2**.
Note: if trunk group numbers are contiguous, a single row can be used. Else, add a row for each trunk group.
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix.
- **Total Length:** Enter “5” since a private prefix was not defined.

change private-numbering 5					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	506	1		5	Total Administered: 3
5	506	10		5	Maximum Entries: 540
...					

3.9. Administer AAR Analysis

This section provides the configuration of the AAR pattern used in the sample configuration for routing calls between SIP users supported by Communication Manager Feature Server and stations on Communication Manager Evolution Server. Entries should be added for extension numbers of stations on both Communication Managers.

In the sample configuration, extension numbers starting with digits “510xx” are assigned to stations on Communication Manager Evolution Server and extension numbers starting with digits “506xx” are assigned to SIP stations supported by Communication Manager Feature Server.

Note: Other methods of routing may be used.

Use the **change aar analysis n** command where **n** is the first digit of the extension numbers used in the system.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Dialed String** Enter leading digit (s) of extension numbers.
- **Min** Enter minimum number of digits that must be dialed.
- **Max** Enter maximum number of digits that may be dialed.
- **Route Pattern** Enter Route Pattern defined in **Section 3.7**.
- **Call Type** Enter “unku”.

change aar analysis 5						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
	506	5	5	1	unku		n
	510	5	5	1	unku		n
	777	5	5	10	unku		n

3.10. Configure Stations

For each SIP user defined in Session Manager, add a corresponding station on Communication Manager Feature Server. The extension number defined for the SIP station will be the number the SIP user enters to register to Session Manager.

Note: Instead of manually defining each station using the Communication Manager SAT interface, an alternative option is to automatically generate the SIP station when adding a new SIP user using System Manager. See **Section 4.10** for more information on adding SIP users.

Use the **add station n** command where **n** is a valid extension number defined in the system.

On **Page 1**, enter the following values and use defaults for remaining fields.

- **Type:** Enter station type corresponding to the specific device.
In sample configuration “**9630SIP**” was used.
- **Port:** Leave blank. Once the command is submitted, a virtual port will be assigned (e.g. S0000).
- **Name:** Enter a display name for user.
- **Security Code:** Enter the number used to log in station.
Note: this number should match the “**Communication Profile Password**” field defined when adding this user in System Manager. See **Section 4.10**.

add station 50641		Page 1 of 6	
STATION			
Extension: 50641	Lock Messages? n	BCC: 0	
Type: 9630SIP	Security Code: 123456	TN: 1	
Port:	Coverage Path 1: 1	COR: 1	
Name: SIP Station User	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 19		Time of Day Lock Table:	
		Message Lamp Ext: 50641	
...		IP Video? n	

On **Page 4**, add the desired number of **call-appr** entries in the **BUTTON ASSIGNMENTS** section. This governs how many concurrent calls can be supported. In the sample configuration, three call appearances were configured to support transfer and conferencing scenarios.

Note: Avaya 9601 IP Deskphones display only two local call appearance buttons when idle. So the number of entries shown below is not required to match the number of appearances displayed on the telephone.

add station 50641		Page 4 of 6	
STATION			
SITE DATA			
...			
BUTTON ASSIGNMENTS			
1: call-appr	5:		
2: call-appr	6:		
3: call-appr	7:		
4:	8:		

On **Page 6**, enter the following values and use defaults for remaining fields.

- **SIP Trunk:** Enter “**aar**” to use Route Pattern defined in **Section 3.7** so calls will be routed over the secondary route in case the primary Session Manager is not available.

add station 50641		Page 6 of 6
STATION		
SIP FEATURE OPTIONS		
Type of 3PCC Enabled: None		
SIP Trunk: aar		

3.11. Verify Off-PBX-Telephone Station-Mapping

Use the **change off-pbx-telephone station-mapping xxx** command where **xxx** is an extension assigned to a 9600 Series SIP Deskphone to verify an Off-PBX station mapping was automatically created for the SIP station.

On **Page 1**, verify the following fields were correctly populated.

- **Application** Verify “**OPS**” is assigned.
- **Trunk Selection** Verify “**aar**” is assigned.

change off-pbx-telephone station-mapping 50641							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
50641	OPS	-		50641	aar	1	
		-					
		-					

On **Page 2**, verify the following fields were correctly populated.

- **Call Limit:** Verify “**3**” is assigned corresponding to the number of **call-appr** entries assigned in **Section 3.10**.
- **Mapping Mode:** Verify “**both**” is assigned.
- **Calls Allowed:** Verify “**all**” is assigned.

change off-pbx-telephone station-mapping 50641							Page 2 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Appl Name	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	Location	
50641	OPS	3	both	all	none		
			-				

3.12. Save Translations

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

Note: After making a change on Communication Manager Feature Server which alters the dial plan or numbering plan, synchronization between Communication Manager Feature Server and System Manager must be completed and SIP telephones must be re-registered.

See **Section 4.11** for more information on how to perform an on-demand synchronization.

4. Configure Avaya Aura® Session Manager

This section describes the procedures for configuring Avaya Aura® Session Manager to support registrations of SIP endpoints.

These instructions assume other administration activities have already been completed such as defining SIP entities for Avaya Aura® Communication Manager Evolution Server and each Session Manager, defining the network connection between System Manager and each Session Manager, and defining Communication Manager Feature Server as a Managed Element. For more information on these additional actions, see **References [2]** and **[5]** in **Section 10**.

The following administration activities will be described:

- Define SIP Domain and Locations
- Define SIP Entity for Communication Manager Feature Server
- Define Entity Links, which describe the SIP trunk parameters used by Session Manager when routing calls between SIP Entities
- Define Entity Link between Session Managers
- Define Routing Policies and Dial Patterns which control routing between SIP Entities
- Define Applications and Application Sequences supporting SIP Users
- Add new SIP Users
- Synchronize changes with Avaya Aura® Communication Manager.

Note: Some administration screens have been abbreviated for clarity.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL “**http://<ip-address>/SMGR**”, where “**<ip-address>**” is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

4.1. Define SIP Domains

Expand **Elements** → **Routing** and select **Domains** from the left navigation menu.

Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter the Authoritative Domain Name specified in **Section 3.4**.
For the sample configuration, “**dr.avaya.com**” was used.
- **Type** Select “**sip**” from drop-down menu.
- **Notes** Add a brief description. [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation menu is expanded, and 'Domains' is selected. The main content area is titled 'Domain Management' and shows a table with one item. The table has columns for Name, Type, Default, and Notes. The item is 'dr.avaya.com' with Type 'sip' and Notes 'SIL Lab domain'. The 'Commit' button is visible in the top right corner.

Name	Type	Default	Notes
* dr.avaya.com	sip	☐	SIL Lab domain

4.2. Define Locations

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

Expand **Elements** → **Routing** and select **Locations** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional].

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
For the sample configuration, “135.9.228.*” was used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows a Location specified for the sample configuration.

Home /Elements / Routing / Locations- Location Details

Location Details

Commit Cancel Help ?

General

* Name: Subnet: 135.9.228

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 900

Multimedia Bandwidth: 900

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 900 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 900 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

	IP Address Pattern	Notes
☒	* 135.9.228.*	

4.3. Define SIP Entities

A SIP Entity must be added for Communication Manager Feature Server. To add a SIP Entity, expand **Elements** → **Routing** and select **SIP Entities** from the left navigation menu.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for new SIP Entity.
- **FQDN or IP Address:** Enter IP address of “**procr**” interface defined in **Section 3.5**
- **Type:** Select “**CM**” for Communication Manager.
- **Notes:** Enter a brief description. [Optional].

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select “**Use Session Manager Configuration**”.

Click **Commit** to save SIP Entity definition.

The following screen shows the SIP Entity defined for Communication Manager Feature Server.

Note: IP address of the “**procr**” interface has been partially hidden for security.

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: CMFS1

* FQDN or IP Address: 135.9.xx.xxx

Type: CM

Notes: CMFS 6.0

Adaptation: [v]

Location: [v]

Time Zone: America/Denver [v]

Override Port & Transport with DNS SRV: ☐

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

Credential name: [v]

Call Detail Recording: none [v]

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration [v]

Commit Cancel

4.4. Define Entity Links

A SIP trunk between Session Manager and Communication Manager is described by an Entity Link. In the sample configuration, SIP Entity Links were added between Communication Manager Feature Server and each Session Manager.

To add an Entity Link, expand **Elements** → **Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link to Communication Manager.
- **SIP Entity 1** Select one of Session Managers previously defined.
- **SIP Entity 2** Select the SIP Entity added for Communication Manager defined in **Section 4.3** from drop-down menu.
- **Protocol** After selecting both SIP Entities, select “**TCP**” as the required Protocol.
- **Port** Verify **Port** for both SIP entities is “**5060**”.
- **Trusted** Enter ☒.
- **Notes** Enter a brief description. [Optional].

Click **Commit** to save Entity Link definition.

Note: TCP was used in the sample configuration. However, TLS would typically be used in production environments.

The following screen shows the Entity Link defined between Communication Manager Feature Server and one of the Session Managers.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links- Entity Links

Entity Links

Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SILASM4-CMFS1	* silasm4	TCP	* 5060	* CMFS1	* 5060	☒	

Repeat this step to define Entity Link between Communication Manager and the second Session Manager.

4.5. Define Entity Link between Avaya Aura® Session Managers

To provide redundancy and enable sessions to be alternatively routed through the second Session Manager in the case of a network failure, define an Entity Link between Session Managers.

Expand **Elements** → **Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values.

- **Name** Enter an identifier for the link to each telephony system.
- **SIP Entity 1** Select one of Session Managers previously defined.
- **SIP Entity 2** Select second Session Manager.
- **Protocol** After selecting both SIP Entities, select “**TCP**” as the required Protocol.
- **Port** Verify **Port** for both SIP entities is “**5060**”.
- **Trusted** Enter ☒.
- **Notes** Enter a brief description. [Optional].

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Session Managers in the sample configuration.

AVAYA Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Entity Links- Entity Links

Entity Links

Commit Cancel Help ?

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* silasm3 - silasm4	* silasm3	TCP	* 5060	* silasm4	* 5060	☒	Link between asm3 and

* Input Required

Commit Cancel

4.6. Define Routing Policy

Routing policies describe the conditions under which calls will be routed to Communication Manager Evolution Server.

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

To add a routing policy, expand **Elements** → **Routing** and select **Routing Policies**.

Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier for Communication Manager Evolution Server.
- **Disabled:** Leave unchecked.
- **Notes:** Enter a brief description. [Optional].

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown).

- Select the previously defined SIP Entity associated with Communication Manager Evolution Server and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: the routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screen shows the Routing Policy for Communication Manager Evolution Server.

Routing Policy Details

General

* Name: to CMES

Disabled: ☐

Notes: Route to CMES aka cm4

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
s8900_cmes	135.9.0.100	CM	CMES 6.0

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	☒	☒	☒	☒	☒	☒	☒	00:00	23:59	Time Range 24/7

Select : All, None

4.7. Define Dial Pattern

This section describes the steps to define a dial pattern to route calls to Communication Manager Evolution Server. In the sample configuration, 5-digit extensions beginning with “51xxx” are assigned to non-SIP stations managed by Communication Manager Evolution Server.

Note: Since the SIP users are registered to Session Manager, a dial pattern does not need to be defined for Communication Manager Feature Server.

To define a dial pattern, expand **Elements** → **Routing** and select **Dial Patterns**.

Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for extension numbers for non-SIP stations.
- **Min:** Enter the minimum number digits that must be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select “ALL” if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional].

In the **Originating Locations and Routing Policies** section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select “ALL” .
- In **Routing Policies** table, select the appropriate Routing Policy defined for Communication Manager Evolution Server in **Section 4.6**.
- Click **Select** to save these changes and return to **Dial Patterns Details** page.

Click **Commit** to save the new definition. The following screen shows the Dial Pattern defined for routing calls to Communication Manager Evolution Server.

Dial Pattern Details

General

* Pattern: 51

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes: h.323 endpoints on CMES

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

☐	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☒	-ALL-	Any Locations	to CMES	0	☐	s8800_cmes	Route to CMES aka cm4

Select : All, None

4.8. Define Application

To support SIP IMS users registered to Session Manager, an Application must be defined for Communication Manager Feature Server.

To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications** from the left navigational menu.

Click **New** (not shown). In the **Application Editor** section, enter the following values.

- **Name** Enter name for the application.
- **SIP Entity** Select SIP Entity for Communication Manager Feature Server defined in **Section 4.3**.
- **CM System for SIP Entity:** Select name of Managed Element previously defined for Communication Manager Feature Server. In the sample configuration, “**cmfs1**” was used.
- **Description:** Enter description [Optional].

Leave fields in the **Application Attributes (optional)** section blank.

The screen below shows the Application defined for Communication Manager Feature Server.

The screenshot displays the 'Application Editor' interface. On the left is a navigation menu with 'Applications' highlighted. The main area shows the 'Application' configuration section with a red box around the required fields: Name (s8800-G450-APP), SIP Entity (CMFS1), CM System for SIP Entity (cmfs1), and Description (CM as FS only). Below this is the 'Application Attributes (optional)' section with empty fields for Application Handle and URI Parameters. Buttons for 'Commit' and 'Cancel' are at the top right.

Name	Value
Application Handle	
URI Parameters	

4.9. Define Application Sequence

The second step in defining an Application to support SIP IMS Users registered to Session Manager is to define an Application Sequence.

Navigate to **Elements** → **Session Manager** → **Application Configuration** → **Application Sequences** from the left navigation menu.

Click **New** (not shown). In the **Sequence Name** section, enter the following values.

- **Name** Enter name for the application.
- **Description** Enter description [Optional].

In the **Available Applications** table, click **+** icon associated with the Application for Communication Manager Feature Server defined in **Section 4.8** to select this application.

Verify a new entry is added to the **Applications in this Sequence** table as shown below.

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

Help ?

Application Sequence Editor

Commit Cancel

Application Sequence

*Name CMFS1 App Seq 1

Description s8800-G450 Endpoints

Applications in this Sequence

Move First Move Last Remove

1 Item

☐	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
☐	1	s8800-G450-APP	CMFS1	☒	CM as FS only

Select : All, None

Available Applications

3 Items Refresh Filter: Enable

Name	SIP Entity	Description
+ cmes_cm4	s8800_cmes	CM4 CMES
+ ps1	Presence-Element	IPS6.1
+ s8800-G450-APP	CMFS1	CM as FS only

Repeat this step if multiple applications are needed as part of the Application Sequence.

Click **Commit** to save the new Application Sequence.

4.10. Add SIP Users

Add new SIP users for each 9600 Series SIP station defined in **Section 3.10**. Alternatively, use the option in **Step 5** below to automatically generate the station after adding a new SIP user.

To add new SIP users, expand **Users** → **User Management** and select **Manage Users** from left navigation menu.

Note: to support failover, each SIP user was defined with multiple SIP Registrations.

Step 1: Click **New** (not shown). Enter values for the following required attributes for a new SIP user in the **Identity** section and use default values for remaining fields.

- **Last Name:** Enter last name of user.
- **First Name:** Enter first name of user.
- **Login Name:** Enter “**extension number@<domain>**” where “**<domain>**” matches the domain defined in **Section 4.1**.
- **Authentication Type:** Verify “**Basic**” is selected.
- **Password:** Enter password used to log into System Manager.
- **Confirm Password:** Repeat value entered above.
- **Localized Display Name:** Enter display name for user [Optional].

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

The screenshot shows the 'New User Profile' form in the System Manager interface. The form is titled 'New User Profile' and has tabs for Identity, Communication Profile, Membership, and Contacts. The Identity tab is active. The form contains several fields: Last Name (SIP), First Name (Model 9641), Middle Name, Description, Login Name (50641@dr.avaya.com), Authentication Type (Basic), Password, Confirm Password, Localized Display Name, Endpoint Display Name, Honorific, Language Preference, and Time Zone. The fields for Last Name, First Name, Login Name, Authentication Type, Password, and Confirm Password are highlighted with red boxes.

Step 2: Select **Communication Profile** tab on **New User Profile** page and enter value used to log in endpoint in the **Communication Profile Password** and **Confirm Password** fields.

Note: **Communication Profile Password** should match the **Security Code** field defined in **Section 3.10**.

Verify there is a default entry identified as the **Primary** profile as shown below:

New User Profile [Commit] [Cancel]

Identity * **Communication Profile *** Membership Contacts

Communication Profile ▾

Communication Profile Password: [password field]
Confirm Password: [password field]

[New] [Delete] [Done] [Cancel]

Name
Primary

Select : None

* Name: Primary
Default : ☒

If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name:** Enter **“Primary”**.
- **Default:** Verify ☒ has been entered.

Step 3: Expand **Communication Address** sub-section and select **New** to define a **Communication Address** for the new user. Enter values for the following required attributes:

- **Type:** Select **“Avaya SIP”** from drop-down menu.
- **Fully Qualified Address:** Enter same extension number as used for **Login Name** in **Step 1**.
Note: value is shown in **Handle** field after address is added.
- **Domain:** Verify value matches Domain name defined in **Section 4.1**.

Click **Add** (not shown) to save the Communication Address. The screen below shows results from **Step 3**:

Communication Address ▾

[New] [Edit] [Delete]

Type	Handle	Domain
Avaya SIP	50641	dr.avaya.com

Select : All, None

Step 4: Scroll down to the **Session Manager Profile** section and enter  to expand section.

Enter the following values.

- **Primary Session Manager** Select one of the Session Managers.
- **Secondary Session Manager** Select the second Session Manager as the backup SIP Registrar.
- **Origination Application Sequence** Select **Application Sequence** defined in **Section 4.9** for Feature Server.
- **Termination Application Sequence** Select **Application Sequence** defined in **Section 4.9** for Feature Server.
- **Survivability Server** Select “(None)” from drop-down menu.
- **Home Location** Select **Location** defined in **Section 4.2**.

The screen below shows results from **Step 4**.

☒ **Session Manager Profile** ▼

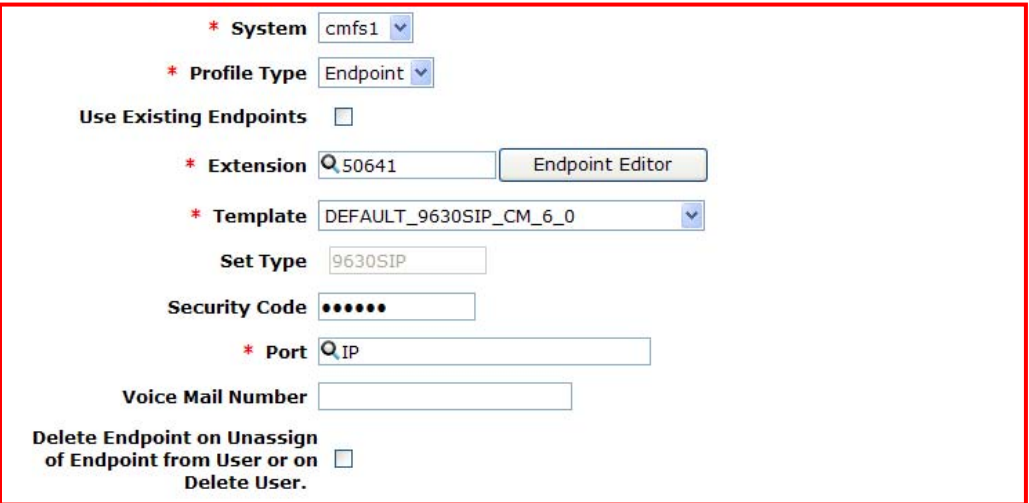
* Primary Session Manager	silasm3	<table><tr><th>Primary</th><th>Secondary</th><th>Maximum</th></tr><tr><td>5</td><td>4</td><td>9</td></tr></table>	Primary	Secondary	Maximum	5	4	9
Primary	Secondary	Maximum						
5	4	9						
Secondary Session Manager	silasm4	<table><tr><th>Primary</th><th>Secondary</th><th>Maximum</th></tr><tr><td>50</td><td>4</td><td>54</td></tr></table>	Primary	Secondary	Maximum	50	4	54
Primary	Secondary	Maximum						
50	4	54						
Origination Application Sequence	CMFS1 App Seq 1							
Termination Application Sequence	CMFS1 App Seq 1							
Survivability Server	(None)							
* Home Location	Subnet: 135.9.228							

Step 5: Scroll down to the **Endpoint Profile** section and enter  to expand section

Enter the following values and use defaults for remaining fields.

- **System** Select Managed Element defined for Communication Manager Feature Server.
- **Profile Type** Select “**Endpoint**”.
- **Use Existing Endpoints** Leave unchecked to automatically create new endpoint when new user is created.
Else, enter  if endpoint is already defined.
- **Extension** Enter same extension number used for **Login Name** in **Step 1**.
- **Template** Select template for type of SIP phone.
- **Security Code** Enter numeric value used to log on to SIP telephone.
Note: this field should match the value entered for the **Communication Profile Password** field in **Step 2**.
- **Port** Select “**IP**” from drop down menu.
- **Voice Mail Number** Enter **Pilot Number** for Avaya Modular Messaging or Avaya Aura® Messaging if installed. Else, leave field blank.
- **Delete Station on Unassign of Endpoint** Enter  to automatically delete station when **Endpoint Profile** is un-assigned from user [Optional].

The screen below shows the results from **Step 5** when adding a new SIP user in the sample configuration.



The screenshot shows the 'Endpoint Profile' configuration form. At the top, there is a header 'Endpoint Profile' with a dropdown arrow. Below it, the form contains several fields and checkboxes:

- * System:** A dropdown menu showing 'cmfs1'.
- * Profile Type:** A dropdown menu showing 'Endpoint'.
- Use Existing Endpoints:** An unchecked checkbox.
- * Extension:** A text input field containing '50641' and a magnifying glass icon. To its right is a button labeled 'Endpoint Editor'.
- * Template:** A dropdown menu showing 'DEFAULT_9630SIP_CM_6_0'.
- Set Type:** A text input field containing '9630SIP'.
- Security Code:** A text input field containing six dots '.....'.
- * Port:** A dropdown menu showing 'IP'.
- Voice Mail Number:** An empty text input field.
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:** An unchecked checkbox.

Click **Commit** (not shown) to save definition of the new user.

4.11. Synchronize Changes with Avaya Aura® Communication Manager

After completing these changes in System Manager, perform an on demand synchronization. Navigate to **Elements** → **Inventory** → **Synchronization** → **Communication System**.

On the **Synchronize CM Data and Configure Options** page, expand the **Synchronize CM Data/Launch Element Cut Through** table and select the row associated with Communication Manager Feature Server as shown below.

Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Inventory * Routing * Home

Home / Elements / Inventory / Synchronization / Communication System- Synchronize CM Data and Configure Options

Synchronize CM Data and Configure Options

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

Synchronize CM Data/Launch Element Cut Through

2 Items Refresh Show ALL Filter: Enable

☐	Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version
☒	cmfs1	135.9. [REDACTED]	April 20, 2011 9:01:34 AM - 06:00	10:00 pm TUE APR 19, 2011	Incremental	Synchronizing Version		R016x.00.1.510.1
☐	silcm4	135.9. [REDACTED]	April 20, 2011 2:02:04 AM - 06:00	10:00 pm TUE APR 19, 2011	Incremental	Completed		R016x.00.1.510.1

Select : All, None

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

Now Schedule Cancel Launch Element Cut Through

Click ☒ to select **Incremental Sync data for selected devices** option. Click **Now** to start the synchronization.

Use the **Refresh** button in the table header to verify status of the synchronization.

Verify synchronization successfully completes by verifying the status in the **Sync Status** column shows **“Completed”**.

Note: Depending on the number of administration changes made, synchronization might take several minutes to complete.

5. Configure Avaya Aura® Communication Manager Evolution Server

This section describes the administration of Communication Manager Evolution Server using a System Access Terminal (SAT). Some administrative screens are not shown in this section, as the screens might be similar to **Section 3**.

The following administration steps will be described:

- Verify System Capabilities and Communication Manager Licensing
- Configure Trunk-to-Trunk transfers
- Configure IP Codec Set
- Configure IP Network Region
- Configure IP Node Names
- Configure SIP Signaling Group and Trunk Group
- Administer Route Patterns
- Administer Numbering Plan

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

5.1. 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.

5.1.1. Verify SIP Trunk Capacity

On **Page 2** of the **display system-parameters customer-options** command, verify an adequate number of SIP Trunk Members are administered for the system.

See **Section 3.1.2** to view the screen for the sample configuration.

5.1.2. Verify AAR/ARS Routing is Enabled

To simplify the dialing plan for calling SIP stations from a station on Communication Manager Evolution Server, verify that the **ARS**, **ARS/AAR Partitioning** and **ARS/AAR Dialing without FAC** features are enabled on **Page 3** of **system-parameters customer options** command.

See **Section 3.1.3** to view the screen for the sample configuration.

5.1.3. Verify Private Numbering

On **Page 5** of **display system-parameters customer options** command, verify the **Private Networking** feature is set to “y”.

See **Section 3.1.4** to view the screen for the sample configuration.

5.2. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when an incoming call to a Communication Manager station is transferred to a SIP station. For simplicity, the **Trunk-to-Trunk Transfer** field on **Page 1** was set to “all” to enable all trunk-to-trunk transfers on a system wide basis.

See **Section 3.2** for more information.

5.3. Configure IP Codec Set

Use the **change ip-codec-set n** command where **n** is the number used to identify the codec set and repeat the step defined in **Section 3.3**.

5.4. Configure IP Network Region

Use the **change ip-network-region n** command where **n** is an available network region to define a network region.

Enter the following values and use default values for remaining fields.

- **Authoritative Domain:** Enter the correct SIP domain for the configuration. For the sample configuration, “**dr.avaya.com**” was used.
- **Codec Set:** Enter the number of the IP codec set configured in **Section 5.3**.
- **Intra-region IP-IP Direct Audio:** Enter “yes”.
- **Inter-region IP-IP Direct Audio:** Enter “yes”.

change ip-network-region 2		Page 1 of 19
IP NETWORK REGION		
Region: 2		
Location:	Authoritative Domain: dr.avaya.com	
Name:		
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		
...		

5.5. Add Node Names and IP Addresses

Use the **change node-names ip** command to add the node-name and IP Addresses for the “procr” interface on Communication Manager and the SIP signaling interface of each Session Manager, if not previously added.

For the sample configuration, the same node names for each Session Manager were configured on both Communication Managers. See **Section 3.5** for more information.

5.6. Configure SIP Signaling Groups and Trunk Groups

5.6.1. Create Signaling Groups for SIP Trunks

Use the **add signaling-group n** command, where **n** is an available signaling group number to create SIP signaling groups. In the sample configuration, trunk groups “10” and “14” and signaling groups “10” and “14” were used for connecting to both Session Managers.

Enter the same values as described in **Section 3.6.1**, except for the **IMS Enabled?** field. For the SIP trunk between Communication Manager Evolution Server and each Session Manager, enter “n” as shown below.

- **IMS Enabled?** Enter “n”.

Note: TCP was used for the sample configuration. However, TLS would typically be used in production environments.

add 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? n		
Peer Detection Enabled? y	Peer Server: others	
Near-end Node Name: procr	Far-end Node Name: ASM1-SM100	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 2	
Far-end Domain: avaya.com		
DTMF over IP: rtp-payload	Bypass If IP Threshold Exceeded? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

Repeat this step to define a second signaling group to connect to the second Session Manager.

5.6.2. Add SIP Trunk Groups

Add the corresponding trunk groups controlled by the signaling groups defined **Section 5.6.1** using the **add trunk-group n** command where **n** is an available trunk group number.

Fill in the indicated fields as described in **Section 3.6.2**.

Repeat this step to define a SIP trunk group to connect to the second Session Manager.

5.7. Configure Route Pattern

This section provides the configuration of the route pattern used in the sample configuration for routing calls between stations on Communication Manager Evolution Server and SIP endpoints supported by Communication Manager Feature Server. To support routing when the primary Session Manager is not available, the route pattern should be configured to use look-ahead routing to select a secondary route.

Use **change route-pattern n** command where **n** is an available route pattern.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Grp No** Enter row for each trunk group defined in **Section 5.6.2**.
- **FRL** Enter **"0"**.
- **Numbering Format** Enter **"lev0-pvt"**.
- **LAR** Enter **"next"** for first row. Use default value for second row.

In the sample configuration, route pattern **"10"** was created as shown below:

change route-pattern 10												Page 1 of 3			
Pattern Number: 10 Pattern Name: IMS SIP to ASM															
SCCAN? n Secure SIP? n															
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits					QSIG			
							Dgts					Intw			
1:	10	0										n	user		
2:	14	0										n	user		
3:											n	user			
4:											n	user			
5:											n	user			
6:											n	user			
BCC	VALUE		TSC	CA-TSC		ITC	BCIE	Service/Feature		PARM	No.	Numbering	LAR		
0	1	2	M	4	W						Dgts	Format			
											Subaddress				
1:	y	y	y	y	y	n	n	rest			lev0-pvt	next			
2:	y	y	y	y	y	n	n	rest			lev0-pvt	none			
3:	y	y	y	y	y	n	n	rest				none			
4:	y	y	y	y	y	n	n	rest				none			
...															

5.8. Administer Numbering Plan

5.8.1. Administer Uniform Dialplan

Use the **change uniform-dialplan n** command, where **n** is the first digit of the extension numbers used for SIP stations in the system.

In the sample configuration, 5-digit extension numbers starting with “**506xx**” are used for extensions associated with the 9600 Series SIP stations.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Matching Pattern** Enter digit pattern of extensions associated with SIP endpoints.
- **Len** Enter extension length.
- **Net** Enter “**aar**”.

change uniform-dialplan 5						Page	1 of 2
UNIFORM DIAL PLAN TABLE						Percent Full: 0	
Matching Pattern	Len	Del	Insert Digits	Net	Conv Num		
506	5	0		aar	n		
777	5	0		aar	n		

5.8.2. Administer AAR analysis

This section provides the configuration of the AAR pattern used in the sample configuration for routing calls between stations on Communication Manager Evolution Server and SIP users registered to Session Manager.

Use the **change aar analysis n** command where **n** is the first digit of the extension numbers used for SIP endpoints in the system.

Fill in the indicated fields as shown below and use default values for remaining fields.

- **Dialed String** Enter leading digit (s) of extension number for SIP stations.
- **Min** Enter minimum number of digits that must be dialed.
- **Max** Enter maximum number of digits that may be dialed.
- **Route Pattern** Enter Route Pattern defined in **Section 5.7**.
- **Call Type** Enter “**unku**”.

change aar analysis 5						Page	1 of 2
AAR DIGIT ANALYSIS TABLE						Percent Full: 1	
Dialed String	Total		Location: all	Call Type	Node Num	ANI	
	Min	Max	Route Pattern			Reqd	
506	5	5	10	unku		n	
777	7	5	20	lev0		n	

6. Manual Configuration of Avaya 9600 Series IP Deskphones

This section defines the steps to manually configure Avaya 9600 Series IP Deskphones running Avaya one-X® SIP firmware to register to both Session Managers.

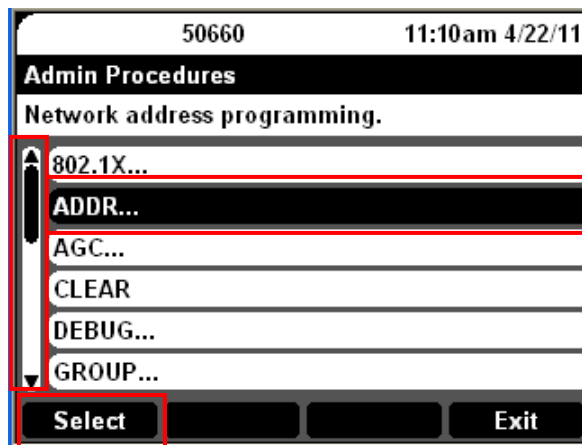
6.1. Configuring IP Addresses

To access the Avaya 9600 Series IP Deskphone **Administration Procedure**, enter the following buttons on the keypad:

Mute c r a f t # (mute 2 7 2 3 8 #).

The screen shown below will be displayed on the Deskphone.

Note: These screens are from an Avaya 9630 IP Deskphone although all Avaya 9600 Series Deskphones use the same basic settings and procedures.



Using down arrow of left side of the screen, scroll down one row to highlight **ADDR....** field. Press **Select**.

Using the **up** and **down** arrows, select the appropriate fields from the **Address Procedures** menu to specify settings for the specific network configuration and press **Change** to edit each field.

To manually configure the telephone, select “**No**” for **Use DHCP** field and enter appropriate IP addresses for **Phone**, **Router**, **Mask**, **HTTPS File Server** and **HTTP File Server** fields.

The screen below shows the configuration of these fields in the sample configuration.

Note: IP addresses have been partially hidden for security.

50660		11:09am 4/22/11	
Address Procedures			
Obtain network settings automatically			
Use DHCP	No		
Phone:	136.9		
Router:	135.9		
Mask:	255.255.255.0		
HTTPS File Server:	0.0.0.0		
HTTP File Server:	135.9		
Change		Back	

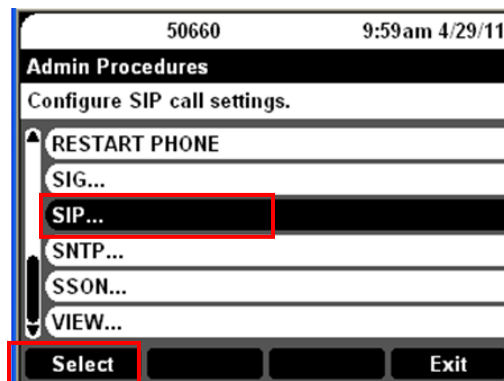
Continue scrolling down to see the fields for **DNS Server**, **802.1Q**, **VLAN ID**, and **VLAN Test**. Enter appropriate values for each field for the specific network configuration.

Once all fields in this section have been entered, press **Save** (not shown) to save the new values and return to the main **Admin Procedures** menu.

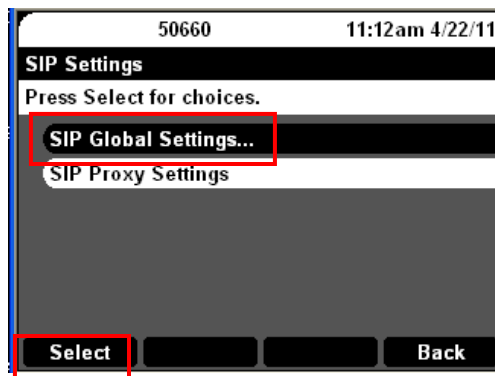
6.2. Configure SIP Global and Proxy Settings

The section describes the administration steps to configure the SIP Domain, the SIP Proxy Server IP address and other SIP settings.

Step 1: From the main **Admin Procedures** menu, scroll down and highlight **SIP...** field. Press **Select** to edit SIP settings.



Step 2: Highlight **SIP Global Settings...** on the **SIP Settings** menu and press **Select**.

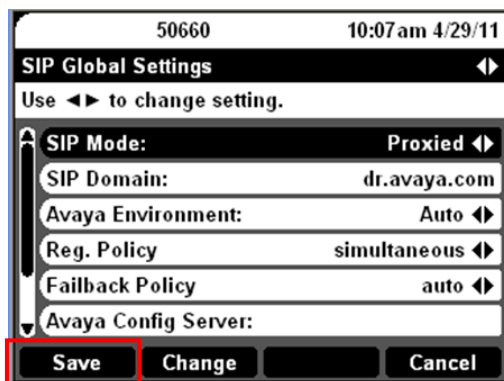


Step 3: Press **Change** to edit **SIP Global Settings**.

Enter the following values and use defaults for remaining fields:

- **SIP Mode:** Select “**Proxied**”.
- **SIP Domain:** Enter appropriate domain name.
For the sample configuration, “**dr.avaya.com**” was used.
- **Avaya Environment:** Select “**Auto**”.
- **Reg. Policy** Select “**simultaneous**” to support registration to both Session Managers.
- **Failback Policy** Select “**auto**”.
- **User ID field** Select “**no**” (not shown).

The screens below show the results from **Step 3** for the sample configuration.



The screenshot shows a mobile device screen with the title "SIP Global Settings". At the top, it displays "50660" and "10:07 am 4/29/11". Below the title is a header bar with "SIP Global Settings" and a back arrow. A message "Use <|> to change setting." is displayed. The settings list includes: "SIP Mode:" with value "Proxied", "SIP Domain:" with value "dr.avaya.com", "Avaya Environment:" with value "Auto", "Reg. Policy" with value "simultaneous", "Failback Policy" with value "auto", and "Avaya Config Server:" which is empty. At the bottom, there are three buttons: "Save", "Change", and "Cancel". The "Save" button is highlighted with a red rectangle.

Press **Save** to save updated settings and return to **SIP Settings** menu.

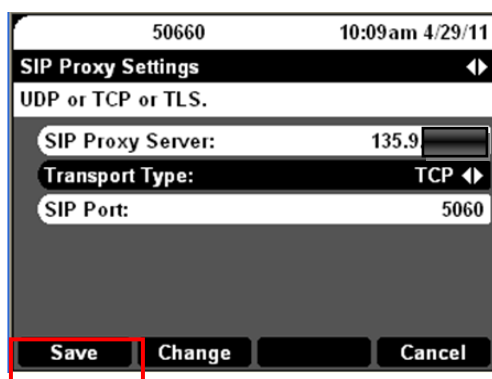
Step 4: On the **SIP Settings** menu, highlight **SIP Proxy Settings** (not shown) and press **Select**.

Select **NEW** (not shown).

Enter the following information for the primary Session Manager.

- **SIP Proxy Server:** Enter IP Address of SIP signaling interface for Session Manager.
- **Transport Type:** Select “**TCP**”.
- **SIP Port:** Enter “**5060**”.

The screen below shows the results from **Step 4** for the sample configuration.



The screenshot shows a mobile device screen with a status bar at the top displaying '50660' and '10:09am 4/29/11'. Below the status bar is a title bar 'SIP Proxy Settings' with a double arrow icon. The main content area is titled 'UDP or TCP or TLS.' and contains three input fields: 'SIP Proxy Server:' with the value '135.9', 'Transport Type:' with the value 'TCP' and a double arrow icon, and 'SIP Port:' with the value '5060'. At the bottom of the screen are four buttons: 'Save', 'Change', and 'Cancel'. The 'Save' button is highlighted with a red rectangular box.

Step 5: Press **Save**. Repeat the above step to enter the information for the second Session Manager.

Step 6: Press **Save** to save the information for the second Session Manager. Press **Back** two times to return to the main **Admin Procedures** menu.

Step 7: Press **Exit** to complete the configuration. The phone will reboot.

7. Verification Steps

7.1. Verify Avaya Aura® Session Manager Configuration

Step 1: Verify Avaya Aura® Session Manager is Operational

Expand **Elements** → **Session Manager** and select **Dashboard** to verify the overall system status for both Session Managers.

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

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

✓
Up
Accept New Service

The screenshot shows the 'Session Manager Dashboard' with a sidebar menu on the left. The 'Dashboard' option is highlighted. The main content area displays 'Session Manager Instances' with a table of system status. A red box highlights the 'Tests Pass', 'Security Module', and 'Service State' columns for both instances.

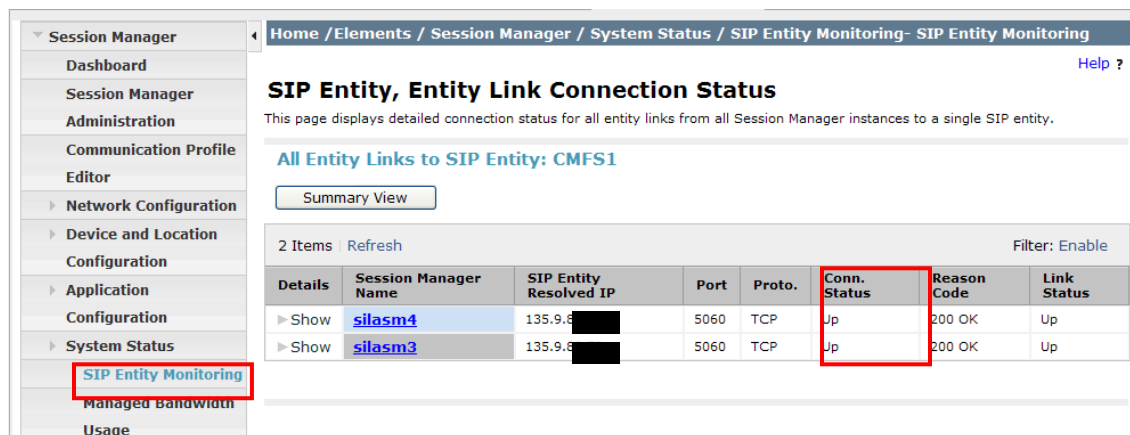
Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations
silasm3	Core	14/2/46	✓	Up	Accept New Service	0/6	0	6
silasm4	Core	11/495/725	✓	Up	Accept New Service	1/15	0	22

Step 2: Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** to view more detailed status information for the specific SIP Entity Links used for calls between SIP endpoints and non-SIP stations on Communication Manager Evolution Server.

Select the SIP Entity for Communication Manager Feature Server from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: CMFS1** table, verify the **Conn. Status** for both links is “Up” as shown below:



The screenshot displays the 'SIP Entity, Entity Link Connection Status' page. The left sidebar shows the navigation menu with 'SIP Entity Monitoring' highlighted. The main content area shows the title 'SIP Entity, Entity Link Connection Status' and a subtitle 'All Entity Links to SIP Entity: CMFS1'. Below this is a table with 2 items. The 'Conn. Status' column is highlighted with a red box.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	silasm4	135.9.8.1	5060	TCP	Up	200 OK	Up
Show	silasm3	135.9.8.2	5060	TCP	Up	200 OK	Up

Repeat the steps to verify the Entity Link status for Communication Manager Evolution Server.

Step 3: Verify Registrations of SIP Endpoints

Navigate to **Elements → Session Manager → System Status → User Registrations** to verify the SIP endpoints have successfully registered with both Session Managers.

For example, the screen below highlights three SIP users who have successfully registered with both Session Managers.

The screenshot displays the 'User Registrations' page in a management console. The left sidebar shows a navigation menu with 'User Registrations' highlighted. The main content area shows a table of registered SIP endpoints. The table has columns for 'Details', 'Address', 'Login Name', 'First Name', 'Last Name', 'Location', 'IP Address', 'AST Device', and 'Registered'. The 'Registered' column has sub-columns for 'Prim', 'Sec', and 'Surv'. Three rows are highlighted with a red box, indicating successful registration for both Session Managers.

	Details	Address	Login Name	First Name	Last Name	Location	IP Address	AST Device	Registered		
									Prim	Sec	Surv
☐	► Show	---	50670@dr.avaya.com	Not Assigned	H323	Subnet: 135.9.228	---	☐	☐	☐	☐
☐	► Show	---	50641@dr.avaya.com	Model 9641	SIP	Subnet: 135.9.228	---	☐	☐	☐	☐
☐	► Show	50655@dr.avaya.com	50655@dr.avaya.com	Model 9650	SIP	Subnet: 135.9.228	135.9.228.2	☒	☒ (AC)	☒	☐
☐	► Show	50601@dr.avaya.com	50601@dr.avaya.com	Model 9601	SIP	Subnet: 135.9.228	135.9.228.2	☒	☒ (AC)	☒	☐
☐	► Show	50644@dr.avaya.com	50644@dr.avaya.com	Model 9641	SIP	135.9.88	135.9.228.2	☒	☒ (AC)	☒	☐

Select : All, None

7.2. Verify Avaya Aura® Communication Manager Feature Server

Verify the status of one of SIP trunk groups on Communication Manager Feature Server by using the **status trunk n** command, where **n** is one of the trunk group numbers administered in **Section 3.6.2**.

Verify that all trunks in the trunk group are in the “**in-service/idle**” state as shown below:

status trunk 1			
TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
001/001	T00006	in-service/idle	no
001/002	T00007	in-service/idle	no
001/003	T00008	in-service/idle	no
001/004	T00009	in-service/idle	no
001/005	T00014	in-service/idle	no
001/006	T00015	in-service/idle	no
001/007	T00043	in-service/idle	no
001/008	T00044	in-service/idle	no
001/009	T00045	in-service/idle	no
001/010	T00046	in-service/idle	no

Verify the status of one of the SIP signaling groups by using the **status signaling-group n** command, where **n** is one of the signaling group numbers administered in **Section 3.6.1**.

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

Use the SAT command, **list trace tac #**, where **tac #** is the trunk access code for one of the trunk groups defined in **Section 3.6.2** to trace trunk group activity for the SIP trunk between Session Manager and Communication Manager Feature Server. For example, the trace below illustrates a call from a SIP telephone to an IP station on Communication Manager Evolution Server.

list trace tac #001		Page 1
time	data	LIST TRACE
10:43:54	TRACE STARTED 04/29/2011 CM Release String cold-00.1.510.1-18777	
10:44:03	SIP>INVITE sip:50655@dr.avaya.com SIP/2.0	
10:44:03	dial 50655 route:AAR	
10:44:03	term trunk-group 1 cid 0x9fa	
10:44:03	calltype 50655# match=5	
10:44:03	calltype 50655 call_type AAR, loc=ALL, match=5	
10:44:03	dial 50655 route:AAR	
10:44:03	route-pattern 1 preference 1 cid 0x9fa	
10:44:03	seize trunk-group 1 member 49 cid 0x9fa	
10:44:03	Setup digits 50655	
10:44:03	Calling Number & Name 50644 SIP, Model 96	
10:44:03	SIP<SIP/2.0 100 Trying	
10:44:03	Proceed trunk-group 1 member 49 cid 0x9fa	
10:44:03	SIP<SIP/2.0 180 Ringing	
10:44:03	Alert trunk-group 1 member 49 cid 0x9fa	
10:44:03	SIP>PRACK sip:+19085050655@135.9.88.13;transport=tcp SI	
10:44:03	SIP>P/2.0	
10:44:03	SIP<SIP/2.0 200 OK	
10:44:04	SIP<SIP/2.0 200 OK	
10:44:04	active trunk-group 1 member 49 cid 0x9fa	
10:44:04	G711MU ss:off ps:20	
	rgn:1 [135.9.88.143]:5100	
	rgn:1 [135.9.228.212]:5004	

On Communication Manager, use the SAT command, **list trace station xxx**, where **xxx** is a valid extension number for a SIP telephone. For example, the trace below illustrates the same call from a SIP telephone to an IP station on Communication Manager Evolution Server.

list trace station 50644		Page 1
time	data	LIST TRACE
10:46:23	TRACE STARTED 04/29/2011 CM Release String cold-00.1.510.1-18777	
10:46:30	SIP<INVITE sip:50644@dr.avaya.com;avaya-cm-fnu=off-hook	
10:46:30	SIP< SIP/2.0	
10:46:30	SIP>SIP/2.0 183 Session Progress	
10:46:30	active station 50644 cid 0x9fb	
10:46:31	SIP>SIP/2.0 484 Address Incomplete	
10:46:31	SIP<INVITE sip:50655@dr.avaya.com SIP/2.0	
10:46:31	SIP>SIP/2.0 100 Trying	
10:46:31	dial 50655 route:AAR	
10:46:31	term trunk-group 1 cid 0x9fb	
10:46:31	calltype 50655# match=5	
10:46:31	calltype 50655 call_type AAR,loc=ALL,match=5	
10:46:31	dial 50655 route:AAR	
10:46:31	route-pattern 1 preference 1 cid 0x9fb	
10:46:31	seize trunk-group 1 member 50 cid 0x9fb	
10:46:31	Calling Number & Name NO-CPNumber NO-CPName	
10:46:31	SIP<ACK sip:50644@dr.avaya.com;avaya-cm-fnu=off-hook;ro	
10:46:31	SIP<uteinfo=0-0-0 SIP/2.0	
10:46:31	Proceed trunk-group 1 member 50 cid 0x9fb	
10:46:32	SIP>SIP/2.0 180 Ringing	
10:46:32	Alert trunk-group 1 member 50 cid 0x9fb	
10:46:32	SIP<PRACK sip:+19085050655@135.9.88.72;transport=tcp SI	
10:46:32	SIP<P/2.0	
10:46:32	SIP>SIP/2.0 200 OK	
10:46:33	SIP>SIP/2.0 200 OK	
10:46:33	active trunk-group 1 member 50 cid 0x9fb	
10:46:33	G711MU ss:off ps:20	
	rgn:1 [135.9.88.33]:6464	
	rgn:1 [135.9.228.212]:5004	

Repeat these commands to verify the status of Communication Manager Evolution Server.

7.3. Call Scenarios Verified

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

Basic Calls:

- Place a call from a SIP endpoint to other SIP stations or to non-SIP stations on Communication Manager Evolution Server. Answer the call and verify talk path.
- Place a call from a SIP endpoint to other SIP stations or to non-SIP stations on Communication Manager Evolution Server. Answer the call and place the call on Hold. Return to the held call and verify talk path.
- Verify calls can be transferred from a SIP endpoint to other SIP stations or to IP stations on Communication Manager Evolution Server.
- Verify calls can be forwarded from a SIP endpoint to other SIP stations or to IP stations on Communication Manager Evolution Server.
- Verify that a SIP endpoint can create a conference with other SIP endpoints and stations on Communication Manager Evolution Server.
- Repeat the above scenarios with calls originating from stations on Communication Manager Evolution Server to SIP endpoints registered to Session Manager.

Failure Scenarios:

- Change Management State of the primary Session Manager to **“Deny New Service”**.
 - Verify a SIP endpoint can still make calls to other SIP stations or to non-SIP stations. Answer the calls and verify talk path.
 - Verify a SIP endpoint can still make calls to other SIP stations or to non-SIP stations. Answer the call and place the call on Hold. Return to the held call and verify talk path.
- During an active call, disable network connectivity to primary Session Manager.
 - Verify talk path on the active call after the failover. Disconnect the call and verify the call is properly cleared.
 - Verify talk path on the active call after the failover. Place the call on Hold. Return to the held call and verify talk path.
 - During failover, verify a SIP endpoint can still make calls to another station (including both SIP and non-SIP stations). Answer the call and verify talk path.
 - During failover, verify a SIP endpoint can still make calls to another station (including both SIP and non-SIP stations). Answer the call and place the call on Hold. Return to the held call and verify talk path.
- Disable the SIP trunk between Communication Manager Feature Server and the primary Session Manager.
 - Verify a SIP endpoint can still make calls to other SIP stations or non-SIP stations. Answer the calls and verify talk path.
 - Verify a SIP endpoint can still make calls to other SIP stations or non-SIP stations. Answer the calls and place the call on Hold. Return to the held call and verify talk path.
- Repeat the above scenarios with calls originating from stations on Communication Manager Evolution Server to a SIP endpoint.

8. Acronyms

AAR	Automatic Alternate Routing (Routing on Communication Manager)
ARS	Automatic Route Selection (Routing on Communication Manager)
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LAR	Look-ahead Routing
RTP	Real Time Protocol
SAT	System Access Terminal (Communication Administration Interface)
SIP	Session Initiation Protocol
SMGR	Avaya Aura® 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
URL	Uniform Resource Locator

9. Conclusion

These Application Notes describe how to configure a network with Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Release 6.0.1. Avaya Aura® Communication Manager serves as a Feature Server within the Avaya Aura® architecture and supports Avaya 9600 Series SIP endpoints registered to Avaya Aura® Session Manager. Avaya 9600 Series IP Deskphones (running Avaya one-X® H.323 firmware) and 2420 Digital Telephones are supported by a second Avaya Aura® Communication Manager which serves as an Evolution Server within the Avaya Aura® architecture.

The network in the sample configuration uses two Avaya Aura® Session Managers deployed as a pair of active-active redundant servers. Two Session Managers are deployed so that one Session Manager can serve as backup for the other in case of network or a Session Manager failure.

Interoperability testing included making bi-directional calls between SIP endpoints and several different types of stations on Communication Manager Evolution Server. In addition, various features including hold, transfer and conference were tested on these calls. Finally, testing was performed to verify calls between SIP endpoints and stations on Avaya Aura® Communication Manager Evolution Server were successful even when there were network connectivity issues or when one of the Session Managers was not available.

10. Additional References

Avaya Product documentation relevant to these Application Notes is available at <http://support.avaya.com>.

Avaya Aura® Session Manager

- 1) Avaya Aura® Session Manager Overview, Doc ID 100068105.
- 2) Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473.
- 3) Avaya Aura® Session Manager Case Studies, Doc ID 03-603478.
- 4) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325.
- 5) Administering Avaya Aura® Session Manager, Doc ID 03-603324.

Avaya Aura® Communication Manager

- 6) SIP Support in Avaya Aura® Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206.
- 7) Administering Avaya Aura® Communication Manager, Doc ID 03-300509.
- 8) Administering Avaya Aura® Communication Manager Server Options, Doc ID 03-603479.
- 9) Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide, Doc ID 210-100-500.
- 10) Avaya Toll Fraud Security Guide, Doc ID 555-025-600.

Avaya IP Deskphones (SIP)

- 11) Avaya one-X® Deskphone SIP Administrator Guide. December 6, 2010.
- 12) Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6. June 7, 2010.
- 13) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.1 for 9601 IP Deskphone, December 6, 2010.
- 14) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 6.0 for 9608, 9611G, 9621G and 9641G IP Deskphones, November 22, 2010.
- 15) Avaya one-X® Deskphone SIP Installation and Maintenance Guide Release 2.6, June 7, 2010.

Avaya Application Notes

- 16) Configuring 9600 Series IP Deskphones running SIP firmware with Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Evolution Server Release 6.0.1.
- 17) Configuring multiple Avaya Aura® Session Managers to address different Network Failure Scenarios.
- 18) Configuring Avaya 10x0 Series SIP Video Endpoints with Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Communication Manager Feature Server Release 6.0.1.

©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