



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Reliance Communications SIP Trunking with Avaya Aura® Communication Manager 7.0.1 SP2, Avaya Aura® Session Manager 7.0.1 SP2 and Avaya Session Border Controller for Enterprise 7.1 SP1 - Issue 1.0**

## **Abstract**

These Application Notes illustrate a sample configuration of Avaya Aura® Communication Manager Release 7.0.1 SP2 and Avaya Aura® Session Manager 7.0.1 SP2 with SIP trunks to the Avaya Session Border Controller for Enterprise 7.1 SP1 (Avaya SBCE) when used to connect to the Reliance Communications IMS network (India).

Reliance Communications provides PSTN access via SIP trunks between the enterprise and the Reliance Communications IMS network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Reliance Communications (RCOM) is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the RCOM IMS test lab in India.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1	Interoperability Compliance Testing.....	4
2.2	Test Results .....	5
2.3	Support .....	6
3.	Reference Configuration .....	6
4.	Equipment and Software Validated .....	8
5.	Configure Avaya Aura® Communication Manager .....	9
5.1	System-Parameters Customer-Options .....	9
5.2	System-Parameters Features .....	10
5.3	Dial Plan .....	11
5.4	IP Node Names.....	12
5.5	IP Interface for Procr.....	12
5.6	IP Network Regions .....	13
5.7	IP Codec Parameters .....	15
5.8	SIP Trunks.....	16
5.8.1	Signaling Group .....	16
5.8.2	Trunk Group.....	17
5.9	Calling Party Information.....	20
5.10	Incoming Call Handling Treatment .....	21
5.11	Outbound Routing .....	21
5.12	Avaya G430 Media Gateway Provisioning .....	24
5.13	Avaya Aura® Media Server Provisioning.....	25
5.13.1	Signaling Group for Media Server.....	25
5.13.2	Adding Media Server.....	26
5.14	Save Communication Manager Translations.....	26
6.	Configure Avaya Aura® Session Manager .....	27
6.1	Configure SIP Domain .....	28
6.2	Configure Locations .....	29
6.3	Configure SIP Entities.....	29
6.3.1	Configure Session Manager SIP Entity .....	30
6.3.2	Configure Communication Manager SIP Entity .....	31
6.3.3	Configure Avaya SBCE SIP Entity .....	32
6.4	Configure Entity Links.....	32
6.4.1	Configure Entity Link to Communication Manager.....	33
6.4.2	Configure Entity Link for Avaya SBCE.....	34
6.5	Configure Routing Policies .....	34
6.5.1	Configure Routing Policy for Communication Manager.....	34
6.5.2	Configure Routing Policy for Avaya SBCE .....	35
6.6	Configure Dial Patterns .....	35

7.	Configure Avaya Session Border Controller for Enterprise .....	38
7.1	System Management – Status .....	40
7.2	Global Profiles.....	40
7.2.1	Uniform Resource Identifier (URI) Groups.....	40
7.2.2	Server Interworking – Session Manager .....	41
7.2.3	Server Interworking – Reliance .....	44
7.2.4	Signaling Manipulation.....	45
7.2.5	Server Configuration – Session Manager .....	48
7.2.6	Server Configuration – Reliance.....	51
7.2.7	Routing – To Session Manager.....	54
7.2.8	Routing – To Reliance .....	55
7.2.9	Topology Hiding – Session Manager .....	56
7.2.10	Topology Hiding – Reliance .....	56
7.2.11	Domain Policies .....	57
7.2.12	Application Rules.....	57
7.2.13	Border Rules .....	57
7.2.14	Media Rules .....	57
7.2.15	Signaling Rules .....	57
7.2.16	Endpoint Policy Groups.....	60
7.3	Device Specific Settings.....	61
7.3.1	Network Management.....	61
7.3.2	Media Interfaces.....	62
7.3.3	Signaling Interface .....	63
7.3.4	Endpoint Flows – For Session Manager .....	64
7.3.5	Endpoint Flows – For Reliance.....	66
8.	Verification Steps.....	67
8.1	Avaya Session Border Controller for Enterprise.....	67
8.2	Avaya Aura® Communication Manager .....	69
8.3	Avaya Aura® Session Manager Status .....	70
8.4	Telephony Services .....	71
9.	Conclusion .....	71
10.	Additional References.....	71

# 1. Introduction

These Application Notes illustrate a sample configuration Avaya Aura® Communication Manager Release 7.0.1 SP2 and Avaya Aura® Session Manager 7.0.1 SP2 with SIP trunks to the Avaya Session Border Controller for Enterprise 7.1 SP1 (Avaya SBCE) when used to connect to the RCOM IMS network.

Avaya Aura® Session Manager 7.0.1 SP2 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 7.0.1 SP2 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya SBCE 7.1 SP1 is the point of connection between Avaya Aura® Session Manager and the RCOM SIP trunk service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The RCOM SIP trunk service allows enterprises in India to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

## 2. General Test Approach and Test Results

The general test approach was to make calls through the Avaya SBCE while DoS policies are in place using various codec settings and exercising common and advanced PBX features.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, the Avaya SBCE, and the RCOM IMS network.

The compliance testing was based on the Avaya DevConnect Generic SIP Trunk test plan. The testing covered functionality required for compliance as a solution supported on the RCOM IMS network. Calls were made to and from the PSTN across the RCOM IMS network. The following standard features were tested as part of this effort:

- Inbound PSTN calls to various phone types including SIP, H.323, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunks from RCOM IMS network.
- Outbound PSTN calls from various phone types including SIP, H323, digital and analog telephone at the enterprise. All outbound PSTN calls are routed from the enterprise across the SIP trunks from RCOM IMS network.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) and Avaya Communicator for Windows soft phones. The 1XC Computer Mode (where 1XC is used for call control as well as audio path) was tested.
- Dialing plans including local, outbound toll-free, emergency calls.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711A, G.711MU and G.729.
- Media and Early Media transmissions.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound calls.
- User features such as hold and resume, transfer, forward and conference.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.
- Network Call Redirection.
- Remote Worker which allows Avaya SIP endpoints to connect directly to the public Internet as enterprise phones.

## 2.2 Test Results

Interoperability testing of RCOM SIP trunk service was completed with successful results for all test cases with the exception of the observations/limitations described below.

Please refer to the test case document for a complete list of solution issues found when tested.

- **Direct Media** – It was observed that RCOM IMS rejected calls from Avaya when Direct Media was enabled on the SIP signaling of Avaya Aura® Communication Manager. Therefore, Direct Media must be disabled for the SIP signaling of Avaya Aura® Communication Manager.
- **Inbound call** – It was observed that in the inbound call from PSTN phone to Avaya phone, the SIP INVITE which RCOM IMS sent to the Avaya SBCE had the URI of the Request Line header containing the SIP trunk pilot number instead of the number of called party. Resolution of the issue was done by adding a sigma script on the Avaya SBCE to replace SIP trunk pilot number in the URI of the Request Line header with the User part of the URI of the To header in the SIP INVITE.
- **Outbound call** – It was observed that in the outbound call from Avaya phone to PSTN phone, when PSTN phone hung up after answering, there was no SIP BYE sent from

RCOM IMS to Avaya. The workaround of the issue was done by hanging up Avaya phone.

- **RCOM IMS rejected outbound call from Avaya due to long values of User-Agent header and Contact header** - Resolution of the issue was done by adding a sigma script on the Avaya SBCE to replace the value of User-Agent header with “Avaya” and to remove “epv” parameter of the Contact header’s URI.
- **Avaya phone was not able to make ad-hoc conference call with PSTN phone** - This was caused by the wrong Contact header in the SIP INVITE sent from Avaya to RCOM IMS to complete joining the parties. Resolution of the issue was done by adding a sigma script on the Avaya SBCE to remove that Contact header.
- **Call transfer using REFER** – It was observed that Avaya phone is not able to complete the transfer call to PSTN when REFER is used. This is because RCOM IMS did not accept the E.164 number in the Refer-To header and the value of Refer-To header is too long. Resolution of the issue was done by adding a sigma script on the Avaya SBCE to replace “+91” with “0” and remove unnecessary parts of the Refer-To header. This resolution should be adopted on a case by case basis.
- **Call redirection from PSTN to PSTN on Avaya phone** – This kind of call flow is not allowed on RCOM IMS. Examples of this call flow: PSTN phone calls to Avaya phone, Avaya phone enables call forwarding to or does transfer to another PSTN phone.
- **Calling line identification restriction (CLIR)** – RCOM IMS does not support CLIR.
- **FAX** – T.38 Fax functionality has known issue with Avaya SBCE 7.1 SP1 and RCOM IMS supports only T.38 for Fax. Hence Fax was not tested. The fix for T.38 Fax issue would be available in Avaya SBCE 7.1 SP2.

## 2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>.
- **RCOM:** Customers should contact their RCOM Business representative or follow the support links available on [http://www.rcom.co.in/Rcom/business/HTML/vso\\_SIPOverview.html](http://www.rcom.co.in/Rcom/business/HTML/vso_SIPOverview.html).

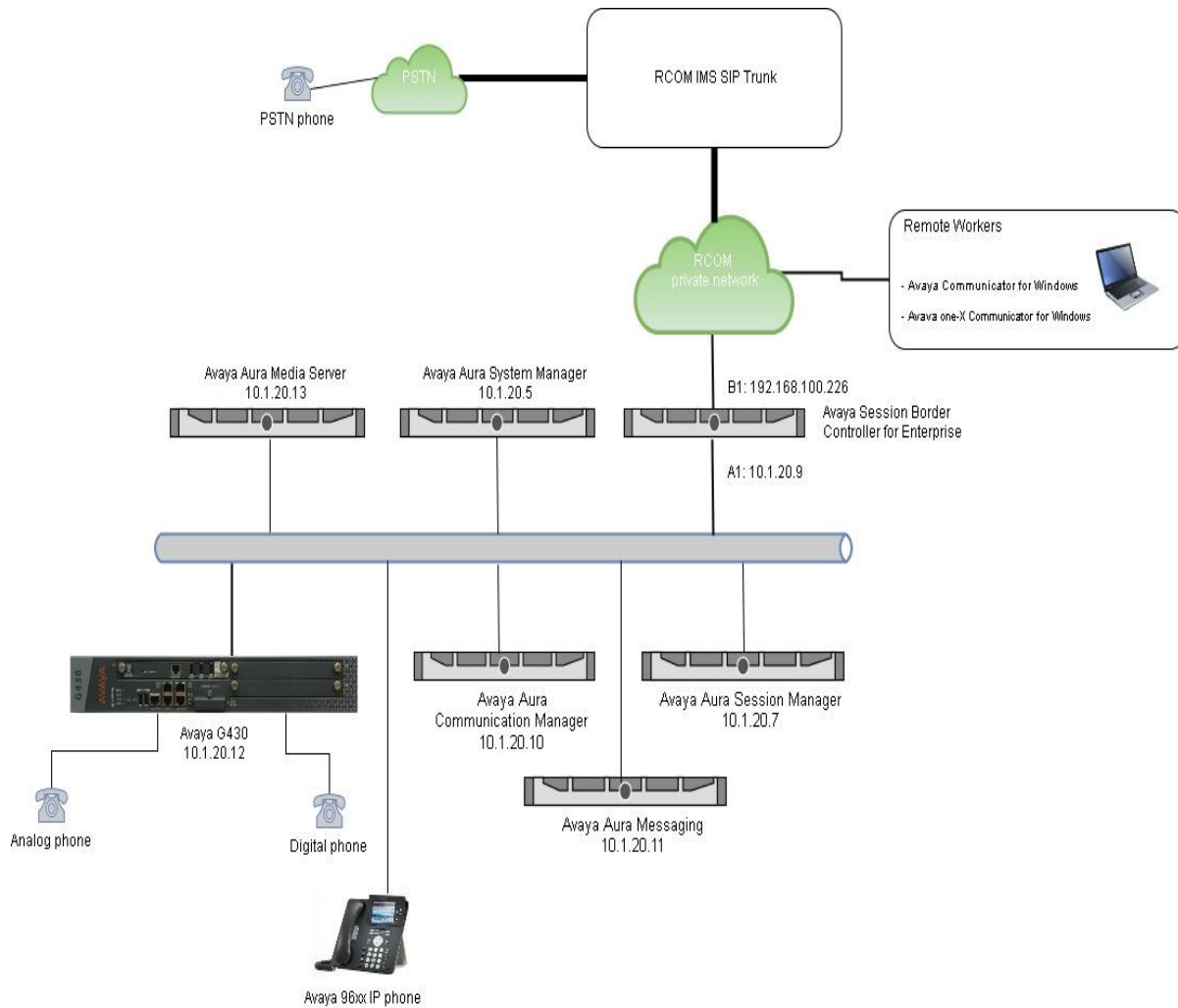
## 3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya Aura® Communication Manager running on VMware ESXi 5.5.
- Avaya Aura® Session Manager running on VMware ESXi 5.5.
- Avaya Session Border Controller for Enterprise running on VMware ESXi 5.5.
- Avaya Aura® System Manager running on VMware ESXi 5.5.
- Avaya Aura® Messaging running on VMware ESXi 5.5.
- Avaya Aura® Messaging running on VMware ESXi 5.5.
- Avaya G430 Media Gateway.
- Avaya Aura® Media Server running on VMware ESXi 5.5. The Media Server can act as a media gateway Gxxx series in providing tones, announcements or music on hold.

- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running H.323/SIP software.
- Avaya 1400 series digital phone.
- Analog phone.
- Avaya one-X® Communicator 6.2.
- Avaya Equinox™ Experience 3.0.

All IP addresses shown in the diagram are private IP addresses.



**Figure 1: Network Components as Tested**

## 4. Equipment and Software Validated

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

Component	Version
<b>Avaya</b>	
Avaya Aura Communication Manager 7.0.1 SP2	7.0.1.2 Service Pack 00.0.441.0-23523
Avaya Aura Session Manager 7.0.1 SP2	7.0.1.2.701230
Avaya Aura System Manager 7.0.1 SP2	7.0.1.2_r701216007
Avaya Aura Messaging 7.0 SP0	MSG-00.0.441.0-017_0004
Avaya Session Border Controller for Enterprise 7.1 SP1	7.1.0.1-07-12368
Avaya Media Gateway G430	g430_sw_37_41_0
Avaya Aura Media Server 7.7	7.7.0.375
Avaya One-X Communicator 6.2	6.2.12.04
Avaya Equinox™ Experience 3.0	3.0.1.8
Avaya One-X Agent H323 2.5.8	2.5.58020.0
Avaya 9600 series – SIP phone	7.0.1.4
Avaya 9600 series – H.323 phone	6.6.4
<b>Service Provider</b>	
RCOM IMS	N/A



## 5. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed.

**Note** – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these Application Notes. Other parameter values may or may not match based on local configurations.

### 5.1 System-Parameters Customer-Options

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes.

**NOTE - For any required features that cannot be enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.**

Follow the steps shown below:

1. Enter the **display system-parameters customer-options** command. On **Page 2** of the form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		4000	0
Maximum Concurrently Registered IP Stations:		2400	4
Maximum Administered Remote Office Trunks:		2400	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		0	0
Max Concur Registered Unauthenticated H.323 Stations:		0	0
Maximum Video Capable Stations:		2400	1
Maximum Video Capable IP Softphones:		2400	2
<b>Maximum Administered SIP Trunks:</b>		<b>4000</b>	<b>10</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0

2. On **Page 6** of the form, verify that the **Private Networking** and **Processor Ethernet** fields are set to **y**.

<b>display system-parameters customer-options</b>		<b>Page 6 of 12</b>
<b>OPTIONAL FEATURES</b>		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? n		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? n	
Port Network Support? y	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
<b>Private Networking? y</b>	Usage Allocation Enhancements? y	
Processor and System MSP? y		
<b>Processor Ethernet? y</b>	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

## 5.2 System-Parameters Features

Follow the steps shown below:

1. Enter the **display system-parameters features** command. On **Page 1** of the form, verify that the **Trunk-to-Trunk Transfer** is set to **all**.

<b>display system-parameters features</b>		<b>Page 1 of 19</b>
<b>FEATURE-RELATED SYSTEM PARAMETERS</b>		
Self Station Display Enabled? n		
<b>Trunk-to-Trunk Transfer: all</b>		
Automatic Callback with Called Party Queuing? n		
Automatic Callback - No Answer Timeout Interval (rings): 3		
Call Park Timeout Interval (minutes): 1		
Off-Premises Tone Detect Timeout Interval (seconds): 20		
AAR/ARS Dial Tone Required? y		
Music (or Silence) on Transferred Trunk Calls? no		
DID/Tie/ISDN/SIP Intercept Treatment: attendant		
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred		
Automatic Circuit Assurance (ACA) Enabled? n		
Abbreviated Dial Programming by Assigned Lists? n		
Auto Abbreviated/Delayed Transition Interval (rings): 2		
Protocol for Caller ID Analog Terminals: Bellcore		
Display Calling Number for Room to Room Caller ID Calls? n		

- On **Page 9** verify that a text string has been defined to replace the **Calling Party Number (CPN)** for restricted or unavailable calls. The compliance test used the value of **Restricted** for restricted calls and **Unavailable** for unavailable calls.

```
display system-parameters features                                     Page 9 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: Restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: Unavailable

DISPLAY TEXT
                                Identity When Bridging: principal
                                User Guidance Display? n
  Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
  Local Country Code:
  International Access Code:

SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
  Caller ID on Call Waiting Delay Timer (msec): 200
```

## 5.3 Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. The following dial plan was used in the reference configuration.

Follow the steps shown below:

- Enter the **change dialplan analysis** command to provision the following dial plan.
  - 4-digit extensions with a **Call Type** of **ext** beginning with 13 (which is a subset of DID numbers (+9122xxxx13xx) assigned by RCOM).
  - 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code \* for SIP Trunk Access Codes (TAC).

display dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page 1 of 12		
			Location: all			Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
6	1	fac						
13	4	ext						
9	1	fac						
*	3	dac						
#	4	fac						

## 5.4 IP Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration a Processor Ethernet (procr) based Communication Manager platform is used. Note that the Communication Manager procr name and IP address are entered during installation. The procr IP address was used to define the Communication Manager SIP Entities in **Section 6.3.2**.

Follow the steps shown below:

- Enter the **change node-names ip** command, and add node names and IP addresses for the following:
  - Session Manager SIP signaling interface (e.g., **asm** and **10.1.20.7**).
  - Media Server (e.g., **ams** and **10.1.20.13**).

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
asm	10.1.20.7	
ams	10.1.20.13	
default	0.0.0.0	
procr	10.1.20.10	
procr6	::	

## 5.5 IP Interface for Procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters defined during installation.

- Verify that **Enable Interface?** , **Allow H.323 Endpoints?** , and **Allow H248 Gateways?** fields are set to **y**.
- In the reference configuration the procr is assigned to **Network Region: 1**.
- The default values are used for the remaining parameters.

display ip-interface pro		Page 1 of 2
		IP INTERFACES
Type: PROCR		Target socket load: 19660
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	Gatekeeper Priority: 5
		IPV4 PARAMETERS
Node Name: procr	IP Address: 10.1.20.10	

## 5.6 IP Network Regions

For the compliance testing, ip-network-region 1 was created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is **sipinterop.net**. This domain name appears in the “From” header of SIP message originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to **yes**. Shuffling can be further restricted at the trunk level under the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.7**.
- Default values can be used for all other fields.

```
display ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: sipinterop.net
Name: mumbai     Stub Network Region: n
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: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 34
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y      RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
Subnet Mask: /24
```

On **Page 4**, define the IP codec set to be used for traffic in region 1. In the compliance testing, Communication Manager, the Avaya G430 Media Gateway, IP/SIP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure the IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields.

display ip-network-region 1										Page	4 of	20
Source Region: 1 Inter Network Region Connection Management										I	A	M
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c	G	A	t
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e		
1	1								all			
2								n				t
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												

Non-IP telephones (e.g., analog, digital) derive their network region from the IP interface of the Avaya G430 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

display ip-interface procr										Page	1 of	2
IP INTERFACES												
Type: PROCR										Target socket load: 19660		
Enable Interface? y										Allow H.323 Endpoints? y		
<b>Network Region: 1</b>										Allow H.248 Gateways? y		
										Gatekeeper Priority: 5		
										IPV4 PARAMETERS		
Node Name: procr										IP Address: 10.1.20.10		
Subnet Mask: /24												

To define network region 1 for the Avaya G430 Media Gateway, use **change media-gateway** command as shown in the following screen.

<pre> change media-gateway 1 MEDIA GATEWAY 1  Type: g430 Name: g430 Serial No: 10Nxxxxxxxxx Link Encryption Type: any-ptls/tls Network Region: 1 Recovery Rule: none  Registered? y FW Version/HW Vintage: 37 .41 .0 /1 MGP IPV4 Address: 10.1.20.12 MGP IPV6 Address: Controller IP Address: 10.1.20.10 MAC Address: 00:1b:xx:xx:xx:48  Mutual Authentication? optional </pre>	<p>Page 1 of 2</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------

## 5.7 IP Codec Parameters

Follow the steps shown below:

1. Enter the **change ip-codec-set x** command, where **x** is the number of the IP codec set specified in **Section 5.6**. On **Page 1** of the **ip-codec-set** form, ensure that **G.711A**, **G.711MU** and **G.729** are included in the codec list. Note that the packet interval size will default to 20ms.

<pre> change ip-codec-set 1 IP CODEC SET  Codec Set: 1  Audio      Silence      Frames      Packet Codec      Suppression  Per Pkt    Size(ms) 1: G.711A      n           2          20 2: G.711MU      n           2          20 3: G.729      n           2          20 4: 5: 6: 7:  Media Encryption      Encrypted SRTCP: enforce-unenc-srtcp 1: none 2: 3: 4: 5: </pre>	<p>Page 1 of 2</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------

2. On **Page 2** of the ip-codec-set form, set **FAX Mode** to **t.38-standard**.

change ip-codec-set 1		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? y			
Maximum Call Rate for Direct-IP Multimedia: 15360:Kbits			
Maximum Call Rate for Priority Direct-IP Multimedia: 15360:Kbits			
	Mode	Redundancy	Packet Size (ms)
FAX	t.38-standard	0	ECM: y
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

## 5.8 SIP Trunks

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group.

### 5.8.1 Signaling Group

This section describes the steps for administering the SIP trunk to Session Manager. This trunk corresponds to the **cm2010** SIP Entity defined in **Section 6.3.2**.

Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **1**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **IP Video?** is set to **n**.
- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **asm**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set the IP network region to **1**, as set in **Section 5.6**.
- **Far-end Domain** – Enter **sipinterop.net**. This is the domain provisioned for Session Manager in **Section 6.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **n** otherwise RCOM IMS will reject call.
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.



- Default values may be used for all other fields.

add signaling-group 1		Page 1 of 3
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: asm	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: sipinterop.net		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? n	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
	Alternate Route Timer(sec): 600	

## 5.8.2 Trunk Group

Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 1). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Name** – Enter a descriptive name.
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., \*01).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **5.8.1** (e.g., 1).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., 10).
- Default values may be used for all other fields.

add trunk-group 3		Page 1 of 22
TRUNK GROUP		
Group Number: 3	Group Type: sip	CDR Reports: y
Group Name: TO-SM	COR: 1	TN: 1
Direction: two-way	Outgoing Display? y	TAC: *01
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 1	
	Number of Members: 10	

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval (in milliseconds) should be equal to the time interval defined by the **Alternate Route Timer** on the signaling group form described in **Section 5.8.1**.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

<code>add trunk-group 1</code>	Page 2 of 22
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 30000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 600	
Disconnect Supervision - In? y Out? y	
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

<code>add trunk-group 1</code>	Page 3 of 22
TRUNK FEATURES	
ACA Assignment? n	Measured: none
Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: public
UI Treatment: service-provider	
Replace Restricted Numbers? y	
Replace Unavailable Numbers? y	
Hold/Unhold Notifications? y	
Modify Tandem Calling Number: no	

On **Page 5**, the **Network Call Redirection?** field may be set to **n** or **y**, both approaches are supported in this solution. Setting the **Network Call Redirection?** flag to **y** enables the use of the SIP REFER message for call transfer; otherwise the SIP INVITE message will be used for call transfer.

Set the **Send Transferring Party Information?** field to **y**, the **Send Diversion Header?** field to **y** and the **Support Request History?** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been redirected. These header modifications are needed to support the call display for call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Setting **n** for **Network Call Redirection**:

<b>add trunk-group 1</b>	<b>Page 5 of 21</b>
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? y	
Enable Q-SIP? n	

## Setting y for Network Call Redirection:

add trunk-group 3	Page 5 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? y	
Enable Q-SIP? n	

## 5.9 Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, the +9122xxxx13xx DID numbers provided for testing were assigned to the extensions 13xx. Thus, these same DID numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

change public-unknown-numbering 1

Page 1 of 2

NUMBERING - PUBLIC/UNKNOWN FORMAT

Ext	Ext	Trk	CPN	Total
Len	Code	Grp(s)	Prefix	CPN
4	13	1	9122xxxx	12

Total Administered: 1

Maximum Entries: 9999

Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.

Communication Manager automatically inserts a '+' digit in this case.

## 5.10 Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by RCOM can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 1                               Page 1 of 30
INCOMING CALL HANDLING TREATMENT
Service/      Number  Number      Del Insert
Feature       Len      Digits
public-ntwrk  13      +9122xxxx  9
public-ntwrk
```

## 5.11 Outbound Routing

In these Application Notes, the **Automatic Route Selection** (ARS) feature is used to route an outbound call via the SIP trunk to the service provider. In the compliance testing, a single digit 9 was used as the ARS access code. An enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) 9, use the **change dialplan analysis** command as shown below.

```
change dialplan analysis                                           Page 1 of 12
DIAL PLAN ANALYSIS TABLE

                                Location: all                      Percent Full: 2

Dialed  Total  Call  Dialed  Total  Call  Dialed  Total  Call
String  Length Type String  Length Type String  Length Type
6       1     fac
13      4     ext
9       1     fac
*       3     dac
#       4     fac
```

Use the **change feature-access-codes** command to define **9** as the **Auto Route Selection (ARS)** – **Access Code 1**.

<b>change feature-access-codes</b>	<b>Page 1 of 11</b>
<b>FEATURE ACCESS CODE (FAC)</b>	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code:	
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code:	
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>	<b>Access Code 2:</b>
Automatic Callback Activation: #002	Deactivation: #003
Call Forwarding Activation Busy/DA: #004 All: #005	Deactivation: #006
Call Forwarding Enhanced Status: #007 Act: #008	Deactivation: #009
Call Park Access Code: #010	
Call Pickup Access Code: #011	
CAS Remote Hold/Answer Hold-Unhold Access Code: #012	
CDR Account Code Access Code: #013	
Change COR Access Code:	
Change Coverage Access Code:	
Conditional Call Extend Activation:	Deactivation:
Contact Closure Open Code:	Close Code:

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance testing. All dialed strings are mapped to route pattern **1** for an outbound call which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0							Page	1 of	2	
ARS DIGIT ANALYSIS TABLE										
							Location: all		Percent Full: 0	
	Dialed	Total		Route	Call	Node	ANI			
	String	Min	Max	Pattern	Type	Num	Reqd			
02		10	10	3	pubu		n			
04		10	10	3	pubu		n			
0011		12	20	3	pubu		n			
000		3	3	3	emer		n			

As mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for **route pattern 1** in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group **1** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Numbering Format:** **unk-unk**. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.9**.

change route-pattern 1													Page 1 of 3			
Pattern Number: 1					Pattern Name: sip											
SCCAN? n					Secure SIP? n					Used for SIP stations? n						
Grp		FRL	NPA	Pfx	Hop	Toll	No.	Inserted					DCS/	IXC		
No				Mrk	Lmt	List	Del	Digits					QSIG			
													Intw			
1: 1		0												n	user	
2:															n	user
3:															n	user
4:															n	user
5:															n	user
6:															n	user
BCC		VALUE		TSC	CA-TSC		ITC		BCIE	Service/Feature		PARM	Sub	Numbering		LAR
0		1	2	M	4	W	Request						Dgts	Format		
1: Y		Y	Y	Y	Y	n	n	rest						unk-unk		none
2: Y		Y	Y	Y	Y	n	n	rest								none
3: Y		Y	Y	Y	Y	n	n	rest								none
4: Y		Y	Y	Y	Y	n	n	rest								none
5: Y		Y	Y	Y	Y	n	n	rest								none
6: Y		Y	Y	Y	Y	n	n	rest								none

## 5.12 Avaya G430 Media Gateway Provisioning

In the reference configuration, a G430 Media Gateways is provisioned. The G430 is used for local DSP resources, announcements, Music On Hold, etc.

**Note** – Only the Media Gateway provisioning associated with the G430 registration to Communication Manager is shown below.

1. SSH to the G430 (not shown). Note that the Media Gateway prompt will contain ??? if the Media Gateway is not registered to Communication Manager (e.g., **g430-???(super)#**).
2. Enter the **show system** command and note the G430 serial number (e.g., **10Nxxxxxxxx**).
3. Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Communication Manager Procr (e.g., **10.1.20.10**).
4. Enter the **copy running-config startup-config** command to save the G430 configuration.
5. On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **1**). The Media Gateway form will open (not shown).

Enter the following parameters:

- Set **Type** = **G430**.
- Set **Name** = Enter a descriptive name (e.g., **g430**).
- Set **Serial Number** = Enter the serial number copied from **Step 2** (e.g., **10Nxxxxxxxx**).
- Set the **Encrypt Link** parameter as desired (**n** was used in the reference configuration).
- Set **Network Region** = **1**.

When the Media Gateway registers, the SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., **g430-001(super)#**).

6. Enter the **display media-gateway 1** command, and verify that the G430 has registered.

```
display media-gateway 1                                     Page 1 of 2
MEDIA GATEWAY 1

      Type: g430
      Name: g430
      Serial No: 10Nxxxxxxxxxx
Link Encryption Type: any-ptls/tls      Enable CF? n
      Network Region: 1                  Location: 1
                                          Site Data: 1

      Recovery Rule: none

      Registered? y
FW Version/HW Vintage: 37 .41 .0 /1
      MGP IPV4 Address: 10.1.20.12
      MGP IPV6 Address:
Controller IP Address: 10.1.20.10
      MAC Address: 00:1b:xx:xx:xx:48

Mutual Authentication? optional
```



## 5.13 Avaya Aura® Media Server Provisioning

Starting from release 7.0 of Avaya Aura®, Avaya Aura® Media Server can be used as VOIP resources for tones, announcements and music on hold in conjunction with Avaya Aura® Communication Manager.

### 5.13.1 Signaling Group for Media Server

This section describes the steps for administering the SIP connection to Media Server.

Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **2**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tls**.
- Verify that **Peer Detection Enabled?** is set to **n**. Set the **Peer Server** to **AMS**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of the Media Server as administered in **Section 5.4** (e.g., **ams**).
- **Near-end Listen Port** – Set to **9061**.
- **Far-end Listen Port** – Set to **5061**.
- **Far-end Network Region** – Set to **1**.

```
add signaling-group 2                                     Page 1 of 2
                                     SIGNALING GROUP
Group Number: 1           Group Type: sip
                          Transport Method: tls
Peer Detection Enabled? n Peer Server: AMS
Near-end Node Name: procr           Far-end Node Name: ams
Near-end Listen Port: 5061          Far-end Listen Port: 5061
                                   Far-end Network Region: 1
Far-end Domain: 10.1.20.13
```

### 5.13.2 Adding Media Server

Enter the **add media-server x** command, where **x** is the number of an unused media server (e.g., **1**), and provision the following:

- **Signaling Group** – Set to signaling group administered in **Section 5.13.1** (e.g., **2**).
- **Voip Channel License Limit** – Set to **10**.
- **Dedicated Voip Channel Licenses** – Set to **10**.
- **Network Region** – Set to the network region administered in **Section 5.6** (e.g., **1**).

add media-server 1	MEDIA SERVER	Page	1 of	1
Media Server ID: 1				
Signaling Group: 2				
Voip Channel License Limit: 10				
Dedicated Voip Channel Licenses: 10				

### 5.14 Save Communication Manager Translations

After the Communication Manager provisioning is completed, enter the command **save translation**.

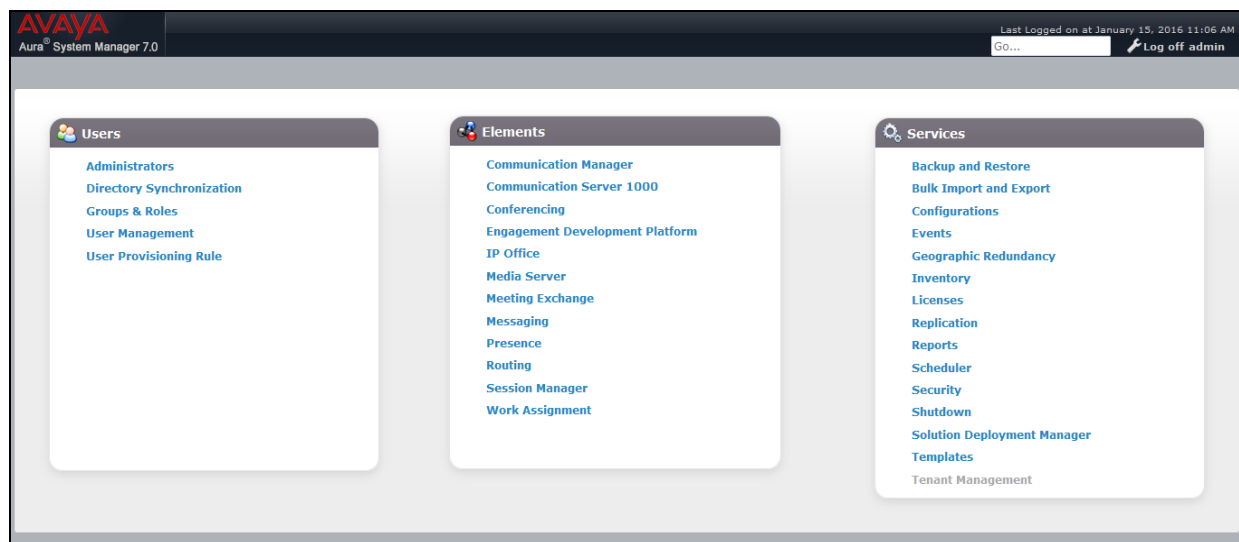
## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Location that can be used by SIP Entities.
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

It may not be necessary to configure all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

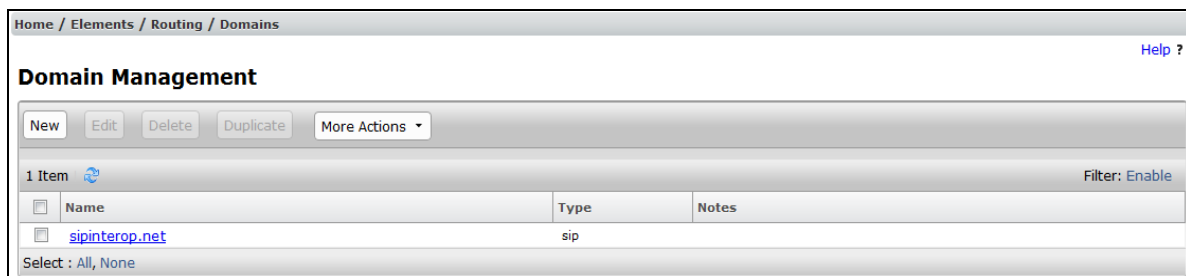
Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



## 6.1 Configure SIP Domain

Follow the steps shown below:

1. Select **Domains** from the left navigation menu. In the reference configuration, domain **sipinterop.net** was defined.
2. Click **New** (not shown). Enter the following values and use default values for remaining fields.
  - **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **sipinterop.net** is shown.
  - **Type:** Verify **sip** is selected.
  - **Notes:** Add a brief description.
3. Click **Commit** to save (not shown).



The screenshot shows a web interface for "Domain Management". At the top, there is a breadcrumb trail: "Home / Elements / Routing / Domains". A "Help ?" link is in the top right. Below the title, there are buttons: "New", "Edit", "Delete", "Duplicate", and a "More Actions" dropdown. A status bar indicates "1 Item" with a refresh icon and a "Filter: Enable" link. The main table has three columns: "Name", "Type", and "Notes". It contains one row with the domain "sipinterop.net" and type "sip". At the bottom left, it says "Select : All, None".

	Name	Type	Notes
<input type="checkbox"/>	sipinterop.net	sip	

## 6.2 Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, location **mumbai** is configured.

Follow the steps shown below:

1. Select **Locations** from the left navigational 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 (e.g., **mumbai**).
  - **Notes:** Add a brief description.
  - Select and enter desired numbers for **Overall Managed Bandwidth**.
2. Click **Commit** to save.

Home / Elements / Routing / Locations

### Location Details

**Commit** **Cancel**

**General**

\* **Name:**

**Notes:**

**Dial Plan Transparency in Survivable Mode**

**Enabled:** ☐

**Listed Directory Number:**

**Associated CM SIP Entity:**

**Overall Managed Bandwidth**

**Managed Bandwidth Units:**

**Total Bandwidth:**

**Multimedia Bandwidth:**

**Audio Calls Can Take Multimedia Bandwidth:** ☒

## 6.3 Configure SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and Avaya SBCE.

### 6.3.1 Configure Session Manager SIP Entity

Follow the steps shown below

1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
  - **Name** – Enter a descriptive name (e.g., **sm206**).
  - **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (not the management interface), provisioned during installation (e.g., **10.1.20.7**).
  - **Type** – Verify **Session Manager** is selected.
  - **Location** – Select location **mumbai**.
  - **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
  - **Time Zone** – Select the time zone in which Session Manager resides.
3. In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:
  - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
  - Use the default values for the remaining parameters.
  - Click **Commit** to save.

Home / Elements / Routing / SIP Entities

## SIP Entity Details

Commit Cancel

### General

\* Name: sm206

\* FQDN or IP Address: 10.1.20.7

Type: Session Manager

Notes:

Location: mumbai

Outbound Proxy:

Time Zone: Asia/Kolkata

Credential name:

### SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

### 6.3.2 Configure Communication Manager SIP Entity

Follow the steps shown below:

1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
  - **Name** – Enter a descriptive name (e.g. **cm2010**).
  - **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) (e.g. **10.1.20.10**).
  - **Type** – Select **CM**.
  - **Location** – Select a Location **mumbai** administered in **Section 6.2**.
  - **Time Zone** – Select the time zone in which Communication Manager resides.
  - Use the default values for the remaining parameters.
3. Click on **Commit**.

Home / Elements / Routing / SIP Entities

### SIP Entity Details

Commit Cancel

General

\* Name: cm2010

\* FQDN or IP Address: 10.1.20.10

Type: CM

Notes:

Adaptation:

Location: mumbai

Time Zone: Asia/Kolkata

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

Credential name:

Securable: ☐

Call Detail Recording: none

### 6.3.3 Configure Avaya SBCE SIP Entity

Repeat the steps in **Section 6.3.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **sbce\_A1**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.1.20.9**).
- **Type** – Verify **SIP Trunk** is selected.
- **Location** – Select location **mumbai** (**Section 6.2**).

Home / Elements / Routing / SIP Entities

## SIP Entity Details

Commit Cancel

General

\* Name: sbce\_A1

\* FQDN or IP Address: 10.1.20.9

Type: SIP Trunk

Notes:

Adaptation:

Location: mumbai

Time Zone: Asia/Kolkata

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

Credential name:

Securable: ☐

Call Detail Recording: egress

### 6.4 Configure Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Communication Manager and another one for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager defined in **Section 6.3.1**.
- **Protocol:** Select the transport protocol used for this link, **TLS** for the Entity Link to Communication Manager and **TLS** for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager.



- **SIP Entity 2:** Select the name of the other systems. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.3.2**. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section 6.3.3**
- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

#### 6.4.1 Configure Entity Link to Communication Manager

Follow the steps shown below:

1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).
2. Continuing in the **Entity Links** page, provision the following:
  - **Name** – Enter a descriptive name (or have it created automatically) for this link to Communication Manager (e.g., **sm206\_cm2010\_5061\_TLS**).
  - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.3.1** for Session Manager (e.g., **sm206**).
  - **SIP Entity 1 Port** – Enter **5061**.
  - **Protocol** – Select **TLS**.
  - **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.2** for the Communication Manager internal entity (e.g., **cm2010**).
  - **SIP Entity 2 Port** - Enter **5061**.
  - **Connection Policy** – Select **Trusted**.
3. Click on **Commit**.

Home / Elements / Routing / Entity Links

**Entity Links** Commit Cancel Help ?

1 Item Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Conne Poli
* sm206_cm2010_5061_T	* Q sm206	TLS	* 5061	* Q cm2010	<input type="checkbox"/>	* 5061	trusted

Select : All, None

## 6.4.2 Configure Entity Link for Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.4.1**, with the following changes:

- **Name** – Enter a descriptive name (or have it created automatically) for this link to the Avaya SBCE (e.g., **sm206\_sbce\_A1\_5061\_TLS**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.3.3** for the Avaya SBCE entity (e.g., **sbce\_A1**).

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* sm206_sbce_A1_5061_T	* sm206	TLS	* 5061	* sbce_A1	<input type="checkbox"/>	* 5061	trusted

## 6.5 Configure Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. Two routing policies were added, one for Communication Manager and another for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click the **New** button in the right pane (not shown). The following screen is displayed.

In the **General** section, enter the following values:

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

### 6.5.1 Configure Routing Policy for Communication Manager

This Routing Policy is used for inbound calls from RCOM.

1. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing RCOM calls to Communication Manager (e.g., **cm2010**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.

4. In the **SIP Entity List** page, select the SIP Entity administered in **Section 6.3.2** for the Communication Manager SIP Entity (**cm2010**), and click on **Select**.
5. Note that once the **Dial Patterns** are defined they will appear in the **Dial Pattern** section of this form.
6. No **Regular Expressions** were used in the reference configuration.
7. Click on **Commit**.

Home / Elements / Routing / Routing Policies

**Routing Policy Details** Commit Cancel Help ?

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
cm2010	10.1.20.10	CM	

## 6.5.2 Configure Routing Policy for Avaya SBCE

This Routing Policy is used for outbound calls to the RCOM IMS network. Repeat the steps in **Section 6.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sbce\_A1**).
- **SIP Entity List** – Select the SIP Entity administered in **Section 6.3.3** for the Avaya SBCE entity (e.g., **sbce\_A1**).

Home / Elements / Routing / Routing Policies

**Routing Policy Details** Commit Cancel Help ?

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
sbce_A1	10.1.20.9	SIP Trunk	

## 6.6 Configure Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to RCOM IMS network and vice versa. Dial Patterns define which routing policy will be selected for a particular

call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click **New** button in the right pane (not shown).

In the **General** section, enter the following values:

- **Pattern:** Enter a dial string that will be matched against the “Request-URI” of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance testing are shown below, one for outbound calls from the enterprise to the PSTN, one for inbound calls from the PSTN to the enterprise.

The first example shows that an 11-digit dialed number that has a destination domain of “sipinterop.net” uses route policy to Avaya SBCE as defined in **Section 6.5.2**.

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** Commit Cancel Help ?

**General**

\* Pattern: 022

\* Min: 10

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	mumbai		sbce_A1	0	<input type="checkbox"/>	sbce_A1	

The second example shows that a 13-digit pattern that starts with +9122xxxx13 is used for inbound calls from RCOM IMS network to DID numbers on Avaya Aura® Communication Manager.

Home / Elements / Routing / Dial Patterns Help ?

### Dial Pattern Details

#### General

\* Pattern: +9122xxxx13

\* Min: 13

\* Max: 13

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

Notes:

#### Originating Locations and Routing Policies

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	mumbai		cm2010	0	<input type="checkbox"/>	cm2010	

Select : All, None

## 7. Configure Avaya Session Border Controller for Enterprise

**Note:** The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

As described in Section 3, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (10.1.20.8), with access to the **mumbai** location. The connection to RCOM IMS uses the Avaya SBCE public interface B1 (IP address **192.168.100.226**). The following provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

1. Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and click on **Continue**.

3. Enter the password and click on **Log In**.

The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾

## Session Border Controller for Enterprise

**Dashboard**

Administration  
Backup/Restore  
System Management  
▸ Global Parameters  
▸ Global Profiles  
▸ PPM Services  
▸ Domain Policies  
▸ TLS Management  
▸ Device Specific Settings

**Dashboard**

This system contains one or more Avaya demo certificates. These certificates have been compromised and should not be used for any production traffic.

Information	
System Time	02:01:51 PM IST <a href="#">Refresh</a>
Version	7.1.0.1-07-12368
Build Date	Fri Nov 11 09:21:54 EST 2016
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	02/15/2017 12:47:52 IST
Failed Login Attempts	0

Installed Devices
EMS
sbce

## 7.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned** (not shown).
2. Click on **View** to display the **System Information** screen.

System Information: sbce

General Configuration

Appliance Name

sbce

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 20

20

Advanced Sessions

Requested: 20

20

Scopia Video Sessions

Requested: 0

0

CES Sessions

Requested: 0

0

Transcoding Sessions

Requested: 0

0

Encryption

☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.1.20.9	10.1.20.9	255.255.255.0	10.1.20.1	A1
192.168.100.226	192.168.100.226	255.255.255.248	192.168.100.225	B1
192.168.100.227	192.168.100.227	255.255.255.248	192.168.100.225	B1

DNS Configuration

Primary DNS

192.168.100.225

Secondary DNS

DNS Location

DMZ

DNS Client IP

192.168.100.226

Management IP(s)

IP #1 (IPv4)

10.1.20.8

## 7.2 Global Profiles

### 7.2.1 Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

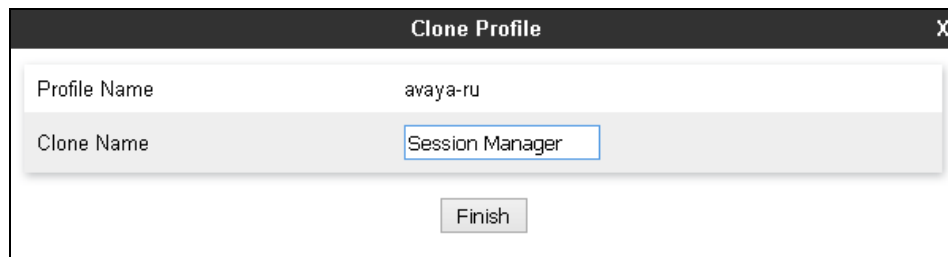
For this configuration testing, “\*” is used for all incoming and outgoing traffic.



## 7.2.2 Server Interworking – Session Manager

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the profile for the connection to Session Manager.

1. Navigate to **Global Profiles > Server Interworking** from the left-hand menu.
2. Select **avaya-ru** then click on **Clone** button.
3. Enter profile name: (e.g., **SessionManager**), and click on **Finish**.



Clone Profile	
Profile Name	avaya-ru
Clone Name	Session Manager
<div>Finish</div>	

4. Click on **Edit** in the **General** tab (not shown).
- Check **T38 Support** box.
  - Click on **Finish**.

The screenshot shows a dialog box titled "Editing Profile: Session Manager" with a close button (X) in the top right corner. The "General" tab is selected. The dialog contains various settings for session management, including handling options for hold, 180, 181, 182, 183, refer, 3xx, diversion, delayed SDP, re-invite, prack, and allow 18X SDP. The "T38 Support" checkbox is checked and highlighted with a red box. The "Finish" button is also highlighted with a red box.

Editing Profile: Session Manager	
<b>General</b>	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
<b>T38 Support</b>	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<b>Finish</b>	

5. Click on **Edit** in the **Advanced** tab (not shown).
- **Record Routes:** Choose **None**.
  - Click on **Finish**.

**Editing Profile: Session Manager**

**Record Routes**

☒ None

☐ Single Side

☐ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

**Include End Point IP for Context Lookup** ☒

**Extensions** Avaya

**Diversion Manipulation** ☐

**Diversion Condition** None

**Diversion Header URI**

**Has Remote SBC** ☒

**Route Response on Via Port** ☐

**Relay INVITE Replace for SIPREC** ☐

**DTMF**

**DTMF Support**

☒ None

☐ SIP Notify

☐ SIP Info

☐ Inband

**Finish**

### 7.2.3 Server Interworking – Reliance

Navigate to **Global Profiles > Server Interworking** from the left-hand menu to add an Interworking Profile for the connection to RCOM IMS network.

- Click on **Add** (not shown) then enter **Reliance** as the **profile name** and click on **Next** (not shown).
- In **General** window: Check **T.38 Support** then click on **Next**.

The screenshot shows the 'General' configuration window for Server Interworking. The window contains the following settings:

- Hold Support:** Radio buttons for None (selected), RFC2543 - c=0.0.0.0, and RFC3264 - a=sendsonly.
- 180 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 181 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 182 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- 183 Handling:** Radio buttons for None (selected), SDP, and No SDP.
- Refer Handling:** Check box (unchecked).
- URI Group:** Dropdown menu set to None.
- Send Hold:** Check box (checked).
- Delayed Offer:** Check box (checked).
- 3xx Handling:** Check box (unchecked).
- Diversion Header Support:** Check box (unchecked).
- Delayed SDP Handling:** Check box (unchecked).
- Re-Invite Handling:** Check box (unchecked).
- Prack Handling:** Check box (unchecked).
- Allow 18X SDP:** Check box (unchecked).
- T.38 Support:** Check box (checked) - highlighted with a red rectangle.
- URI Scheme:** Radio buttons for SIP (selected), TEL, and ANY.
- Via Header Format:** Radio buttons for RFC3261 (selected) and RFC2543.

At the bottom of the window, there are two buttons: 'Back' and 'Next'. The 'Next' button is highlighted with a red rectangle.

- Leave default values in **SIP Timers** window and **Privacy** window (not shown).
- In **Advance** window: Select **None** for **Record Routes** then click on **Finish**.

The screenshot shows the 'Interworking Profile' configuration window. It contains several sections with configuration options:

- Record Routes:** Radio buttons for 'None' (selected), 'Single Side', 'Both Sides', 'Dialog-Initiate Only (Single Side)', and 'Dialog-Initiate Only (Both Sides)'. The 'None' option is highlighted with a red box.
- Include End Point IP for Context Lookup:** A checkbox that is currently unchecked.
- Extensions:** A dropdown menu showing 'None'.
- Diversion Manipulation:** A checkbox that is currently unchecked.
- Diversion Condition:** A dropdown menu showing 'None'.
- Diversion Header URI:** An empty text input field.
- Has Remote SBC:** A checkbox that is checked.
- Route Response on Via Port:** A checkbox that is currently unchecked.
- Relay INVITE Replace for SIPREC:** A checkbox that is currently unchecked.
- DTMF:** A section header.
- DTMF Support:** Radio buttons for 'None' (selected), 'SIP Notify', 'SIP Info', and 'Inband'.
- Buttons:** 'Back' and 'Finish' buttons at the bottom. The 'Finish' button is highlighted with a red box.

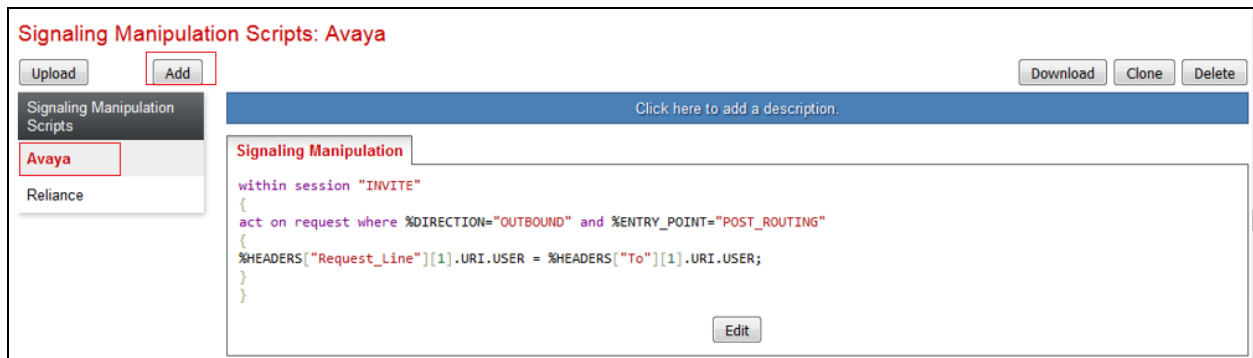
## 7.2.4 Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa. The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE.

### 7.2.4.1 Signaling Manipulation for Session Manager

As stated in **Section 2.2**, a SigMa script needs to be added for Session Manager to correct the Request Line header in the SIP INVITE sent from RCOM IMS network.

To define the signaling manipulation, navigate to **Global Profiles > Signaling Manipulation** in the main menu on the left hand side (not shown). Click on **Add** and enter **Avaya** for the **Title** in the script editor (not shown).



The script text is displayed below.

```
within session "INVITE"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["Request_Line"][1].URI.USER = %HEADERS["To"][1].URI.USER;
  }
}
```

### 7.2.4.2 Signaling Manipulation for Reliance

As stated in **Section 2.2** SigMa scripts need to be added for Reliance so that User-Agent header, Contact header and Refer-To header have proper values which RCOM IMS network accepts.

Repeat steps defined in **Section 7.2.4.1** with the script text shown below.

```
/*Replace value of User-Agent header with “Avaya” and remove “epv” parameter in the Contact header*/
```

```
within session "ALL"
```

```
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%HEADERS["User-Agent"][1] = "Avaya";
remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
}
act on response where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%HEADERS["User-Agent"][1] = "Avaya";
}
```

```
/*Remove Contact header when Contact header contains “Conference”*/
```

```
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
if(%HEADERS["Contact"][1].regex_match(" CONFERENCE ")) then
{ remove(%HEADERS["Contact"][1]); }
}
}
```

```
/*Modify Refer-To header for call transfer using REFER*/
```

```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING" and %METHOD="REFER"
{
%HEADERS["Refer-To"][1].URI.USER.regex_replace("\+91","0");
%HEADERS["Refer-To"][1].URI.regex_replace("\?Replaces.*","");
}
}
```

## 7.2.5 Server Configuration – Session Manager

This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

1. Navigate to **Global Profiles > Server Configuration** from the left-hand menu.
2. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Manager**) and click on **Next** (not shown).
3. The **Edit Server Configuration Profile - General** window will open.
  - Select **Server Type: Call Server**.
  - **SIP Domain:** Enter **sipinterop.net** as defined in **Section 6.1**.
  - **IP Address / FQDN:** **10.1.20.7** (Session Manager signaling IP Address as configured in **Section 6.3.1**).
  - **Transport:** Select **TLS**.
  - **Port:** **5061**.
  - **TLS Client Profile:** Select **Avaya**.
  - Click on **Next**.

**Edit Server Configuration Profile - General**

Server Type: Call Server

SIP Domain: sipinterop.net

TLS Client Profile: Avaya

Add

IP Address / FQDN	Port	Transport
10.1.20.7	5061	TLS

Delete

Back Next

4. The **Add Server Configuration Profile - Authentication** window will open (not shown).
  - Click on **Next** to accept default values.



5. The **Add Server Configuration Profile - Heartbeat** window will open.
  - Check **Enable Heartbeat** box.
  - **Method**: Select **OPTIONS**.
  - **Frequency**: Enter **30**.
  - **From URI** and **To URI**: Enter **ping@sipinterop.net**.
  - Click on **Next** button.

Edit Server Configuration Profile - Heartbeat X

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▼
Frequency	30 seconds
From URI	ping@sipinterop.net
To URI	ping@sipinterop.net

Finish

6. The **Add Server Configuration Profile - Advanced** window will open.
  - Check **Enable Grooming** box.
  - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.2**.
  - **Signaling Manipulation Script**: Select **Avaya** as defined in **Section 7.2.4.1**.
  - Click on **Finish**.

**Edit Server Configuration Profile - Advanced** X

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Session Manager ▼

Signaling Manipulation Script Avaya ▼

Securable ☐

Enable FGDN ☐

TCP Failover Port

TLS Failover Port

Finish

Repeat the steps in **Section 7.2.5**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to RCOM IMS network.

1. Select **Add Profile** and enter a Profile Name (e.g., **Reliance**) and click on **Next** (not shown).
2. On the **Edit Server Configuration Profile - General** window, enter the following.
  - Select **Server Type: Trunk Server**.
  - **SIP Domain:** Enter SIP domain of RCOM IMS network.
  - **IP Address / FQDN:** **192.168.70.141** (RCOM IMS SBC IP address)
  - **Transport:** Select **UDP**.
  - **Port:** **5060**.
  - Click on **Next** (not shown).

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

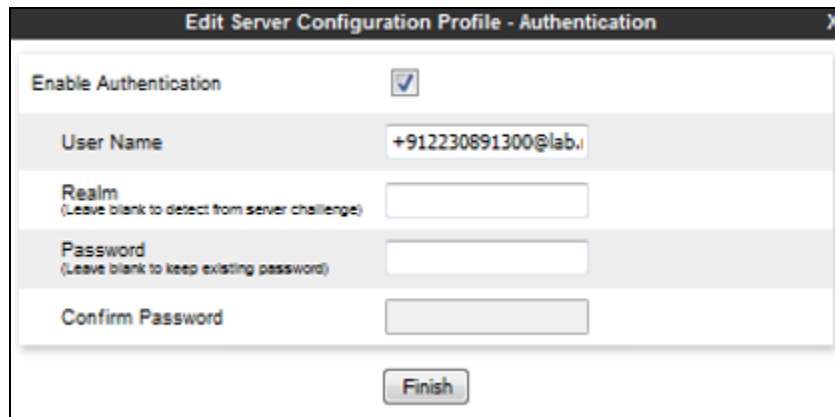
SIP Domain: lab.relianceims.in

TLS Client Profile: None

IP Address / FQDN	Port	Transport
192.168.70.141	5060	UDP

Buttons: Add, Delete, Finish

3. Under **Authentication** window, enter the following.
  - Check to **Enable Authentication**.
  - **User Name**: Enter SIP trunk pilot number assigned by RCOM (e.g., [+9122xxxx1300@lab.relianceims.in](mailto:+9122xxxx1300@lab.relianceims.in)).
  - **Realm**: Leave blank.
  - **Password** and **Confirm Password**: Enter password of SIP trunk pilot number.
  - Click on **Next** (not shown).



Enable Authentication ☒

User Name

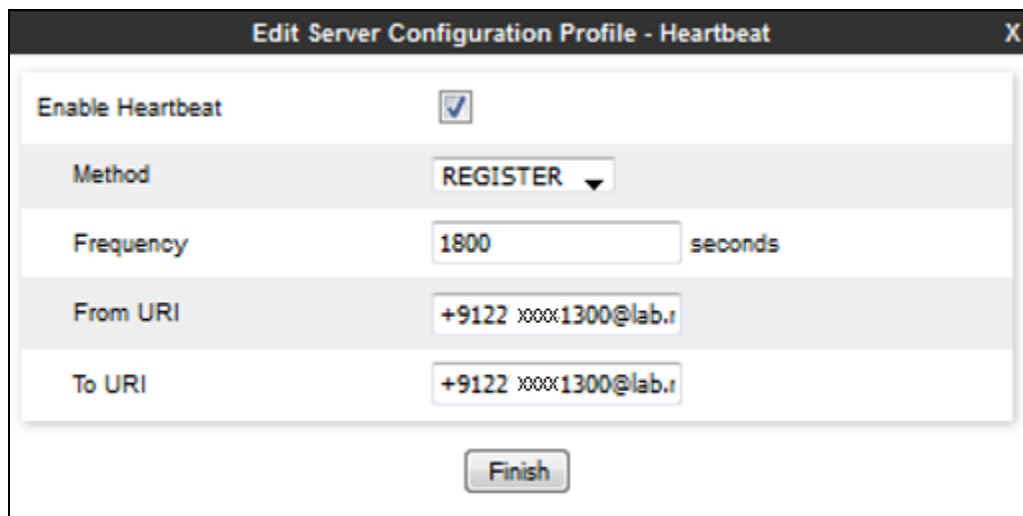
Realm   
(Leave blank to detect from server challenge)

Password   
(Leave blank to keep existing password)

Confirm Password

Finish

4. Under **Heartbeat** window:
  - Check to **Enable Heartbeat**.
  - **Method**: Select **REGISTER**.
  - **Frequency**: Enter **1800**.
  - **From URI** and **To URI**: Enter SIP trunk pilot number as in **step 3**.
  - Click on **Next** (not shown).



Enable Heartbeat ☒

Method

Frequency  seconds

From URI

To URI

Finish

5. Under **Advanced** window:

- Select **Reliance** for **Interworking Profile** as defined in **Section 7.2.3**.
- Select **Reliance** for **Signaling Manipulation Script** as defined in **Section 7.2.4.2**.
- Click on **Finish** (not shown).

The screenshot shows a configuration window with four tabs: General, Authentication, Heartbeat, and Advanced. The Advanced tab is selected and highlighted in red. Below the tabs is a list of configuration options, each with a checkbox on the right. The options are: Enable DoS Protection, Enable Grooming, Interworking Profile, Signaling Manipulation Script, Securable, and Enable FGDN. The 'Interworking Profile' and 'Signaling Manipulation Script' rows are highlighted with a red border, and both show 'Reliance' as the selected value.

Option	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Reliance
Signaling Manipulation Script	Reliance
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>

## 7.2.7 Routing – To Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.

1. Navigate to **Global Profiles > Routing** from the left-hand menu, and click on **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **Session Manager**) and click **Next** (not shown).
3. The **Routing Profile** window will open. Using the default values shown, click on **Add**.
4. Populate the following fields:
  - **Priority/Weight = 1.**
  - **Server Configuration = Session Manager.**
  - **Next Hop Address:** Verify that the **10.1.20.7:5061 (TLS)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
  - Click on **Finish**.

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

ENUM	ENUM Suffix
<input type="checkbox"/>	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Session Manager	10.1.20.7 : 5061 (TLS)	None

Delete

Back

Finish

## 7.2.8 Routing – To Reliance

Repeat the steps in **Section 7.2.7**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to RCOM IMS network.

1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **Reliance**).
2. On the **Routing Profile** window, populate the following fields:
  - **Server Configuration: Reliance.**
  - **Next Hop Address:** Verify that the **192.168.70.141:5060 (UDP)** entry from the drop down menu is selected.
3. Click on **Finish**.

The screenshot shows the 'Profile : Reliance - Edit Rule' window. It contains several configuration fields and a table of rules.

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

ENUM	ENUM Suffix
<input type="checkbox"/>	

[Add](#)

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Reliance	192.168.70.141:5060 (UDP)	None	<a href="#">Delete</a>

[Finish](#)

## 7.2.9 Topology Hiding – Session Manager

The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

1. Navigate to **Global Profiles > Topology Hiding** from the left-hand side menu.
2. Click on **Add** button (not shown), enter **Profile Name:** (e.g., **Session Manager**), and click **Next** (not shown).
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button (not shown) repeatedly to add headers.
4. Populate the fields as shown below, and click on **Finish** (not shown).

The screenshot shows the 'Topology Hiding' configuration window. At the top, there is a blue bar with the text 'Click here to add a description.' and three buttons: 'Rename', 'Clone', and 'Delete'. Below this is a tab labeled 'Topology Hiding'. The main area contains a table with four columns: 'Header', 'Criteria', 'Replace Action', and 'Overwrite Value'. The table lists the following headers and their configurations:

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sipinterop.net
Refer-To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sipinterop.net
Referred-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sipinterop.net
SDP	IP/Domain	Auto	---

At the bottom of the table is an 'Edit' button.

## 7.2.10 Topology Hiding – Reliance

Repeat the steps in **Section 7.2.9**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to RCOM IMS network.

1. Enter a **Profile Name:** (e.g., **Reliance**).
2. Click on the **Add Header** button (not shown) repeatedly to add headers.
3. Populate the fields as shown below, and click on **Finish** (not shown). Note that the **Overwrite Value** is **lab.relianceims.in** which is the SIP domain of RCOM IMS network.

The screenshot shows the 'Topology Hiding' configuration window for the 'Reliance' profile. It has the same layout as the previous window, with a blue bar at the top and a table of headers. The 'Overwrite Value' for most headers is 'lab.relianceims.in'.

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	lab.relianceims.in
Refer-To	IP/Domain	Overwrite	lab.relianceims.in
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	lab.relianceims.in
Referred-By	IP/Domain	Overwrite	lab.relianceims.in
Request-Line	IP/Domain	Overwrite	lab.relianceims.in
SDP	IP/Domain	Auto	---

An 'Edit' button is located at the bottom of the table.



### 7.2.11 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

### 7.2.12 Application Rules

Ensure that the Application rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the default rule was used.

Note: It is not recommended to edit default rules. New rules should be added or cloned from default rules.

### 7.2.13 Border Rules

The Border rules specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses. In the solution as tested, the **default** rule was utilized. No customization was required.

### 7.2.14 Media Rules

The Media rules will be applied to both directions. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

### 7.2.15 Signaling Rules

Signaling rules are a mechanism on the Avaya SBCE to manipulate the signaling beyond simple header manipulation. Signaling rules allow action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message.

#### 7.2.15.1 Signaling Rules for Session Manager

In the flow to RCOM IMS network, the SIP messages are manipulated to avoid the overhead of re-assembling fragmented UDP packets, reduce packet size and removed unnecessary headers. This is achieved by removing Avaya proprietary and unnecessary headers to reduce the SIP messages packet size to below the Maximum Transmission Unit (MTU) so that fragmentation does not occur.

As RCOM IMS does not allow OPTIONS sent from the enterprise so the Avaya SBCE should block OPTIONS sent from Session Manager.

To define the signaling rule, navigate to **Domain Policies > Signaling Rules** in the main menu on the left hand side.

1. Click on **Add** (not shown) and enter details in the **Signaling Rule** pop-up box. In the **Rule Name** field enter a descriptive name such as **Avaya** for the signaling rule to remove Avaya proprietary and unnecessary headers.
2. Click on **Next** and **Next** again, then **Finish** (not shown).

Select the **Request** tab (not shown) and define the rule to block OPTIONS sent from Session Manager with 200 OK as shown below.

**Edit Request Control**

Proprietary Request ☐

Method Name: OPTIONS

In Dialog Action: Block with... 200 OK

Out of Dialog Action: Block with... 200 OK

Finish

Select the **Request Headers** tab (not shown) and define the rules to remove Avaya proprietary headers and unnecessary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Request Header** box to remove Avaya proprietary headers or uncheck it to remove unnecessary headers.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove Header**.
- Click on **Finish**.

The following examples show configuration for removal of **Alert-Info** and AV-Global-Session-ID header from request messages.

**Edit Header Control**

Proprietary Request Header ☐

Header Name: Alert-Info

Method Name: ALL

Header Criteria: ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action: Remove header 486 Busy Here

Finish

**Edit Header Control**
X

Proprietary Request Header ☒

Header Name

Method Name

Header Criteria:
 ☒ Forbidden
 ☐ Mandatory
 ☐ Optional

Presence Action:

**Note:** During the test, the same was done for **Allow-Events**, **Endpoint-View**, **P-AV-Message-Id**, **P-Charging-Vector**, **P-Conference**, **P-Early-Media**, **P-Location** and **Server** headers.

Select the **Response Headers** tab (not shown) and define the rules to remove the same headers as in **Request Headers** tab for 1XX and 2XX **Response Code**.

Signaling Rules: Avaya
Filter By Device...
Rename Clone Delete

Add

Click here to add a description

Add In Header Control

Add Out Header Control

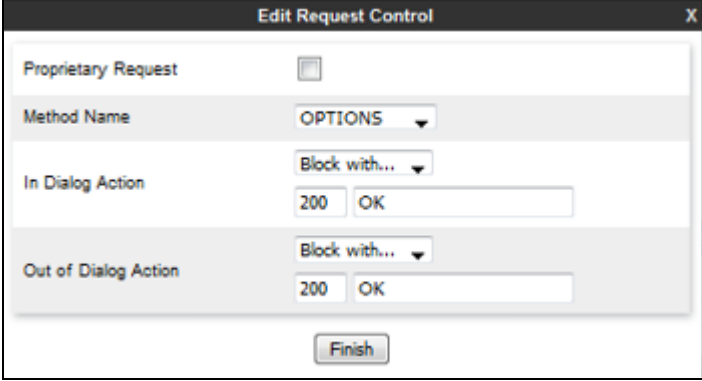
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	Alert-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Av-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Av-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	Endpoint-view	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	Endpoint-view	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	P-Charging-Vector	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
10	P-Charging-Vector	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
11	P-Conference	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
12	P-Conference	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
13	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
14	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
15	Server	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
16	Server	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

### 7.2.15.2 Signaling Rules for Reliance

As RCOM IMS expects response for OPTIONS sent from RCOM IMS so the Avaya SBCE should block those OPTIONS with 200 OK.

To define the signaling rule, navigate to **Domain Policies > Signaling Rules** in the main menu on the left hand side.

1. Click on **Add** and enter details in the **Signaling Rule** pop-up box. In the **Rule Name** field enter a descriptive name such as **Reliance** for the signaling rules.
2. Click on **Next** and **Next** again, then **Finish** (not shown).
3. Select the **Request** tab (not shown) and define the rule to block OPTIONS sent from RCOM IMS with 200 OK as shown below.

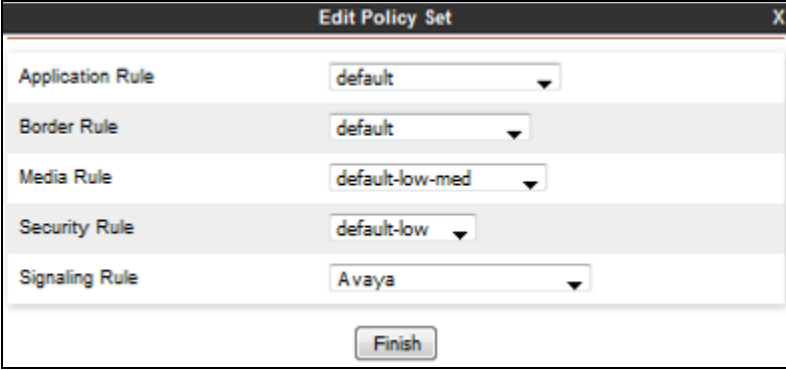


The screenshot shows the 'Edit Request Control' dialog box. It has a title bar with 'Edit Request Control' and a close button 'X'. The dialog contains several fields: 'Proprietary Request' with an unchecked checkbox, 'Method Name' with a dropdown menu showing 'OPTIONS', 'In Dialog Action' with a dropdown menu showing 'Block with...' and a text input field containing '200 OK', and 'Out of Dialog Action' with a dropdown menu showing 'Block with...' and a text input field containing '200 OK'. At the bottom, there is a 'Finish' button.

### 7.2.16 Endpoint Policy Groups

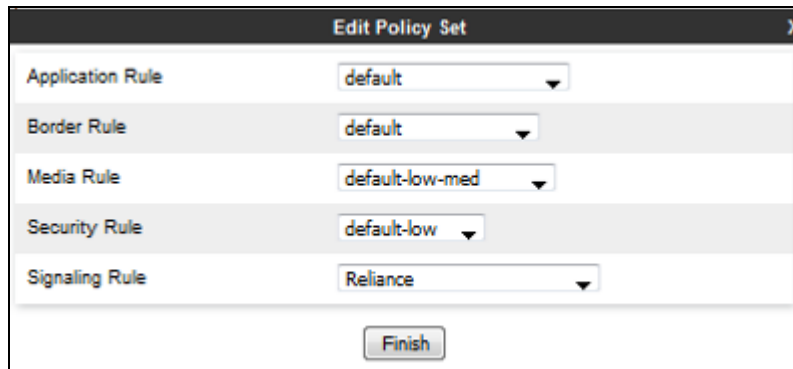
In the solution as tested, the **Avaya** and **Reliance** rules were defined. This rule incorporated the Signaling Rules specified above, as well as other policies.

Endpoint Policy Groups for Session Manager:



The screenshot shows the 'Edit Policy Set' dialog box. It has a title bar with 'Edit Policy Set' and a close button 'X'. The dialog contains several fields: 'Application Rule' with a dropdown menu showing 'default', 'Border Rule' with a dropdown menu showing 'default', 'Media Rule' with a dropdown menu showing 'default-low-med', 'Security Rule' with a dropdown menu showing 'default-low', and 'Signaling Rule' with a dropdown menu showing 'Avaya'. At the bottom, there is a 'Finish' button.

Endpoint Policy Groups for Reliance:



Rule Type	Value
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Reliance

Finish

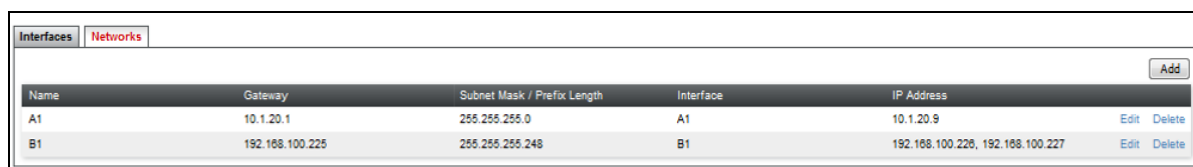
## 7.3 Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows.

### 7.3.1 Network Management

1. Select **Device Specific Settings > Network Management** from the menu on the left-hand side.
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

Note: B1 has two IP Addresses configured. One is used for SIP trunking, another one is used for Remote worker. Configuration for Remote worker is out of scope of this document.



Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1	10.1.20.1	255.255.255.0	A1	10.1.20.9	<a href="#">Edit</a> <a href="#">Delete</a>
B1	192.168.100.225	255.255.255.248	B1	192.168.100.226, 192.168.100.227	<a href="#">Edit</a> <a href="#">Delete</a>

### 7.3.2 Media Interfaces

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
  - **Name:** int\_med.
  - **IP Address:** 10.1.20.9 (Avaya SBCE A1 address).
  - **Port Range:** 35000-40000.
4. Click on **Finish** (not shown).
5. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
  - **Name:** ext\_med\_trunking.
  - **IP Address:** 192.168.100.226 (Avaya SBCE B1 address).
  - **Port Range:** 35000-40000.
6. Click on **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.

Media Interface: sbce

Media Interface		
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from <a href="#">System Management</a>		
Name	Media IP Network	Port Range
int_med	10.1.20.9 A1 (A1, VLAN 0)	35000 - 40000
ext_med_trunking	192.168.100.226 B1 (B1, VLAN 0)	35000 - 40000
ext_med_nw	192.168.100.227 B1 (B1, VLAN 0)	35000 - 40000

### 7.3.3 Signaling Interface

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Click on **Add** (not shown) and enter the following:
  - **Name:** `int_sig`.
  - **IP Address:** `10.1.20.9` (Avaya SBCE A1 address).
  - **TLS Port:** `5061`.
  - **TLS Profile:** `Avaya`.
4. Click on **Finish** (not shown).
5. Click on **Add** again, and enter the following:
  - **Name:** `ext_sig_trunking`.
  - **IP Address:** `192.168.100.226` (Avaya SBCE B1 address).
  - **UDP Port:** `5060`.
6. Click on **Finish** (not shown). Note that changes to these values require an application restart.

Signaling Interface						
Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from <a href="#">System Management</a> .						
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
int_sig	10.1.20.9 A1 (A1, VLAN 0)	---	---	5061	Avaya	
ext_sig_trunking	192.168.100.226 B1 (B1, VLAN 0)	---	5060	---	None	
ext_sig_rw	192.168.100.227 B1 (B1, VLAN 0)	5060	5060	---	None	

### 7.3.4 Endpoint Flows – For Session Manager

1. Select **Device Specific Settings** → **Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
  - **Name: Session Manager.**
  - **Server Configuration: Session Manager.**
  - **URI Group: \*.**
  - **Transport: \*.**
  - **Remote Subnet: \*.**
  - **Received Interface: ext\_sig\_trunking.**
  - **Signaling Interface: int\_sig.**
  - **Media Interface: int\_med.**
  - **End Point Policy Group: Avaya.**
  - **Routing Profile: Reliance.**
  - **Topology Hiding Profile: Session Manager.**
  - Let other values default.
4. Click **Finish**.



Edit Flow: Session ManagerX

Flow Name	Session Manager
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	ext_sig_trunking
Signaling Interface	int_sig
Media Interface	int_med
Secondary Media Interface	None
End Point Policy Group	Avaya
Routing Profile	Reliance
Topology Hiding Profile	Session Manager
Signaling Manipulation Script	None
Remote Branch Office	Any

Finish

### 7.3.5 Endpoint Flows – For Reliance

Repeat step 1 through 4 from Section 7.3.4, with the following changes:

- **Name:** Reliance.
- **Server Configuration:** Reliance.
- **Received Interface:** int\_sig.
- **Signaling Interface:** ext\_sig\_trunking.
- **Media Interface:** ext\_med\_trunking.
- **Endpoint Policy Groups:** Reliance.
- **Routing Profile:** Session Manager.
- **Topology Hiding Profile:** Reliance.

Edit Flow: Reliance	
Flow Name	Reliance
Server Configuration	Reliance
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	int_sig
Signaling Interface	ext_sig_trunking
Media Interface	ext_med_trunking
Secondary Media Interface	None
End Point Policy Group	Reliance
Routing Profile	Session Manager
Topology Hiding Profile	Reliance
Signaling Manipulation Script	None
Remote Branch Office	Any
<b>Finish</b>	

## 8. Verification Steps

The following steps may be used to verify the configuration.

### 8.1 Avaya Session Border Controller for Enterprise

Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms, Incidents, Logs, and Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

#### Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
  - Select the desired **Interface** from the drop down menu (e.g., **All**).
  - Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
  - Specify a **Capture Filename** (e.g., **TEST.pcap**).
  - Unless specific values are required, the default values may be used for the **Local Address, Remote Address, and Protocol** fields.
  - Click **Start Capture** to begin the trace.

The screenshot shows the 'Trace: sbce' window with the 'Packet Capture' tab selected. The 'Captures' sub-tab is also active. The 'Packet Capture Configuration' section displays the following settings: Status is 'Ready', Interface is 'B1', Local Address is '10.2.2.135', Remote Address is '\*', Protocol is 'All', Maximum Number of Packets to Capture is '3000', and Capture Filename is 'test.pcap'. There are 'Start Capture' and 'Clear' buttons at the bottom.

The capture process will initialize and then display the following **In Progress** status window:

The screenshot shows the 'Trace: sbce' window with the 'Packet Capture' tab selected. The 'Captures' sub-tab is active. A blue banner at the top states: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.' The 'Packet Capture Configuration' section displays the following settings: Status is 'In Progress', Interface is 'B1', Local Address is '10.2.2.135', Remote Address is '\*', Protocol is 'All', Maximum Number of Packets to Capture is '3000', and Capture Filename is 'test.pcap'. There is a 'Stop Capture' button at the bottom.

3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.

Trace: sbce

Devices
sbce

Packet Capture
Captures

Refresh

File Name	File Size (bytes)	Last Modified	
<a href="#">test_20160405184126.pcap</a>	0	April 5, 2016 6:41:26 PM AEST	<a href="#">Delete</a>

The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the RCOM IMS network and the customer SIP PABX is the customer SBC.

On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the SBC to the RCOM IMS network.
- Ping from the SBC to the Session Manager.
- Ping from the RCOM IMS network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.

Full Diagnostic Ping Test

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Start Diagnostic

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (192.168.1.1)	Average ping from 192.168.1.16[A1] to 192.168.1.1 is 1.469ms.
✓ Ping: SBC (A1) to Primary DNS (135.10.209.250)	Average ping from 192.168.1.16[A1] to 135.10.209.250 is 111.287ms.
✓ Ping: SBC (B1) to Gateway (10.240.249.129)	Average ping from 10.240.249.130 [B1] to 10.240.249.129 is 0.268ms.

Incident Viewer

AVAYA

Device All Category All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 44.

Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	729881580397602	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580396121	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580393451	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881402194116	4/4/16	7:40 PM	Policy	sbce	Heartbeat Successful, Server is UP

## 8.2 Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager.

- Verify signaling status, trunk status.

```
status signaling-group 1
STATUS SIGNALING GROUP

Group ID: 1
Group Type: sip

Group State: in-service
```

```
status trunk 1
TRUNK GROUP STATUS

Member      Port      Service State      Mtce Connected Ports
Busy

0001/001 T00001  in-service/idle    no
0001/002 T00002  in-service/idle    no
0001/003 T00003  in-service/idle    no
0001/004 T00004  in-service/idle    no
0001/005 T00005  in-service/idle    no
0001/006 T00006  in-service/idle    no
0001/007 T00007  in-service/idle    no
0001/008 T00008  in-service/idle    no
0001/009 T00009  in-service/idle    no
0001/010 T00010  in-service/idle    no
```

## 8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

1. Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.

**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 2:09 PM

1 Item Show All Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	Version
<input type="checkbox"/>	<a href="#">sm206</a>	Core	✓	0/0/0	Up	Accept New Service	0/3	1	1/1	✓	✓	Normal	7.0.1.2.701230

Select : All, None

2. The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status. In the **Entity Monitoring Column**, Session Manager shows that there are **0** (zero) alarms out of the **3** Entities defined.
3. Clicking on the **0/3** entry in the **Entity Monitoring** column, results in the following display:

**Session Manager Entity Link Connection Status**

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: sm206

Summary View

Status Details for the selected Session Manager:

3 Items Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">sbce_A1</a>	10.1.20.9	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">cm2010</a>	10.1.20.10	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">aam</a>	10.1.20.11	5060	TCP	FALSE	UP	200 OK	UP

Options messages between Avaya SBCE and Session Manager:

sbce_A1		SM100	
14:12:58.400	--OPTIONS-->		(2) sip:sipinterop.net
14:12:58.401	<--200 OK--		(2) 200 OK (OPTIONS)
14:13:09.487	--OPTIONS-->		(4) sip:sipinterop.net
14:13:09.489	<--200 OK--		(4) 200 OK (OPTIONS)
14:13:28.401	--OPTIONS-->		(2) sip:sipinterop.net
14:13:28.402	<--200 OK--		(2) 200 OK (OPTIONS)
14:13:29.606	--OPTIONS-->		(7) sip:sipinterop.net
14:13:29.608	<--200 OK--		(7) 200 OK (OPTIONS)

## 8.4 Telephony Services

1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

## 9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 7.0.1 SP2, Avaya Aura® Session Manager 7.0.1 SP2, and Avaya Session Border Control for Enterprise 7.1 SP1 can be configured to interoperate successfully with RCOM SIP trunk service. This solution allows enterprise users access to the PSTN using the RCOM SIP trunk service connection. Please refer to **Section 2.2** for exceptions.

## 10. Additional References

This section references the documentation relevant to these Application Notes. Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Deploying Avaya Aura® System Manager Release 7.0.1.*
- [2] *Administering Avaya Aura® System Manager for Release 7.0.1.*
- [3] *Administering Avaya Aura® Session Manager Release 7.0.1.*
- [4] *Deploying Avaya Aura Session Manager Release 7.0.1.*
- [5] *Deploying Avaya SBCE on VMware in Virtualized Environment Release 7.1.*
- [6] *Administering Avaya Session Border Controller Release 7.1*
- [7] *Document Library for Avaya Aura Communication Manager 7.0.1.*
- [8] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [9] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [10] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for RCOM IMS SIP trunk service is available from RCOM.

---

**©2017 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 DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).