



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunks among AudioCodes Mediant 1000 MSBG e-SBC, Avaya Aura® Session Manager, and Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe a sample configuration for a network that uses Avaya Aura® Session Manager to connect AudioCodes Mediant 1000 MSBG e-SBC and Avaya Aura® Communication Manager using SIP trunks.

The AudioCodes Mediant 1000 MSBG e-SBC is a SIP Session Border Controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted IP network. The compliance testing focused on telephony scenarios between an enterprise site, where the AudioCodes Mediant 1000 MSBG e-SBC, Session Manager, and Communication Manager were located, and a second site simulating a service provider service node.

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 Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a sample configuration for a network that uses Avaya Aura® Session Manager to connect AudioCodes Mediant 1000 MSBG e-SBC and Avaya Aura® Communication Manager using SIP trunks.

The Mediant 1000 MSBG is an all-in-one multi-service access solution for Service Providers offering managed services and distributed Enterprises. This multi-service business gateway is designed to provide converged Voice & Data services for business customers at wire speed, while maintaining SLA parameters for voice quality.

The compliance testing focused on telephony scenarios between an enterprise site, where the AudioCodes Mediant 1000 MSBG e-SBC, Session Manager, and Communication Manager were located, and a second site simulating a service provider service node.

2. General Test Approach and Test Results

The general test approach was to make calls between the main enterprise site and the 2nd site simulating a service provider service node using various codec settings and exercising common telephony features.

2.1. Interoperability Compliance Testing

The compliance testing focused on interoperability between AudioCodes Mediant 1000 MSBG e-SBC and Session Manager / Communication Manager by making calls between the enterprise site and a second site simulating a service provider service node that were connected through the Mediant 1000 MSBG e-SBC using direct SIP trunks. The following functions and features were tested:

- Calls from both SIP and non-SIP endpoints between sites.
- G.711MU and G.729AB codec support.
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference.
- Extended telephony features using Communication Manager Feature Name Extensions (FNE) such as Call Forwarding, Call Park, Call Pickup, Automatic Redial, Automatic Call Back, and Send All Calls.
- Proper system recovery after a Mediant 1000 MSBG e-SBC restart and/or re-establishment of broken IP connectivity.

2.2. Test Results

The AudioCodes Mediant 1000 MSBG e-SBC passed compliance testing.

2.3. Support

For technical support on the AudioCodes Mediant 1000 MSBG e-SBC, visit their online support at <http://www.audiocodes.com/support>.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows two sites connected via a SIP trunk across an untrusted IP network: the main enterprise site and a second site that simulates a service provider service node. The AudioCodes Mediant 1000 MSBG e-SBC Session Border Controller (SBC) is at the edge of the main site. The public side of the Mediant 1000 MSBG e-SBC is connected to the untrusted network and the private side is connected to the trusted corporate LAN.

All SIP traffic between two sites flows through the Mediant 1000 MSBG e-SBC. In this manner, the Mediant 1000 MSBG e-SBC can protect the main site's infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over TCP and RTP for the media streams.

Also connected to the LAN at the main site are:

- An Avaya S8300D Server running Avaya Aura® Communication Manager in an Avaya G450 Media Gateway. Avaya Aura® Communication Manager Messaging is also running on the Avaya S8300D Server to provide voice mail functionality.
- A Dell™ PowerEdge™ R610 Server running Avaya Aura® System Manager. System Manager provides management functions for Session Manager.
- An HP ProLiant DL360 G7 Server running Avaya Aura® Session Manager that provides SIP registrar and proxy server functions for SIP endpoints in the enterprise IP telephony network.

The Session Manager connects the Mediant 1000 MSBG e-SBC and Communication Manager using SIP trunks. Endpoints include both SIP and non-SIP endpoints. An ISDN-PRI trunk connects the media gateway to the PSTN.

The 2nd site (shown as a cloud), simulates a service provider service node, and also comprises of a Communication Manager, System Manager, and Session Manager, with both SIP and non-SIP endpoints.

The SIP endpoints located at both sites are registered to the local Session Manager.

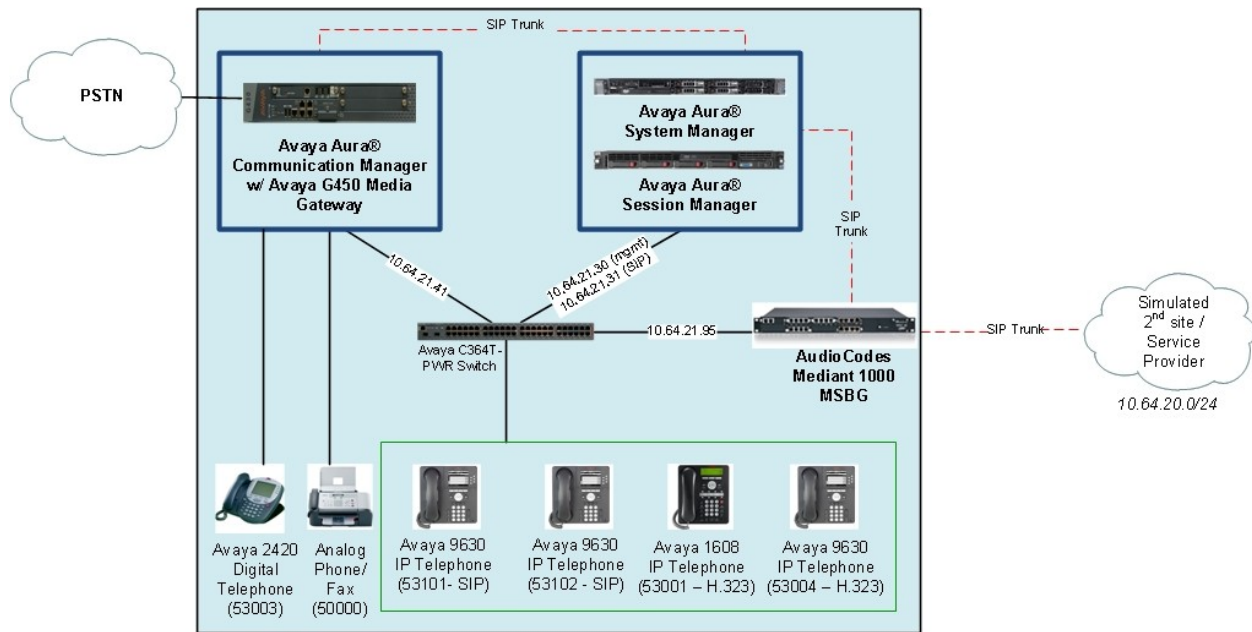


Figure 1: AudioCodes Mediant 1000 MSBG e-SBC SIP Trunking Test Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8300D Server with a Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1, R016x.00.1.510.1, Patch 18621 (Avaya Aura® System Platform: 6.0.2.1.5)
Dell™ PowerEdge™ R610 Server	Avaya Aura® System Manager: 6.1.0 (Build No. – 6.1.0.4.5072-6.1.4.11) (Avaya Aura® System Platform: 6.0.2.1.5)
HP ProLiant DL360 G7 Server	Avaya Aura® Session Manager 6.1.0 (Build No. – 6.1.0.0.42003-6.1.0.610012)
Avaya 9600 Series IP Telephones <ul style="list-style-type: none">• H.323• SIP	3.1. Service Pack 1 2.6.4
Fax Machine	-
AudioCodes Mediant 1000 MSBG e-SBC	6.2 <ul style="list-style-type: none">• MSBG based software: M1000_MSBG_SIP_F6.20A.014.003.zip• Firmware load: M1000_MSBG_SIP_F6.20A.014.003.zip

5. Configure Communication Manager

This section describes the Communication Manager configuration at the main enterprise site to support the network shown in **Figure 1**. It is assumed the procedures necessary to support SIP and connectivity to Session Manager have been performed as described in [2] and [3]; however, some of the configuration is shown in this section and the next section as a reference.

The configuration of Communication Manager was performed using the System Access Terminal (SAT). The screens in this section display the Communication Manager configuration that was administered and already in place prior to the start of compliance testing. After the completion of the configuration, a **save translation** command was performed to make the changes permanent.

Step	Description
1.	<p>System Capacities</p> <p>On Page 2 of the display system-parameters customer-options form, verify that the Maximum Administered SIP Trunks is sufficient for the combination of trunks to AudioCodes and any other SIP trunking entities. Be aware that for each call between a non-SIP endpoint at the enterprise site and Audio Codes, one SIP trunk is used for the duration of the call. An Avaya SIP endpoint uses two SIP trunks for the duration of the call.</p>
	<pre> display system-parameters customer-options Page 2 of 11 OPTIONAL FEATURES IP PORT CAPACITIES USED Maximum Administered H.323 Trunks: 12000 22 Maximum Concurrently Registered IP Stations: 18000 3 Maximum Administered Remote Office Trunks: 12000 0 Maximum Concurrently Registered Remote Office Stations: 18000 0 Maximum Concurrently Registered IP eCons: 414 0 Max Concur Registered Unauthenticated H.323 Stations: 100 0 Maximum Video Capable Stations: 18000 0 Maximum Video Capable IP Softphones: 18000 1 Maximum Administered SIP Trunks: 24000 20 Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0 Maximum Number of DS1 Boards with Echo Cancellation: 522 0 Maximum TN2501 VAL Boards: 128 0 Maximum Media Gateway VAL Sources: 250 0 Maximum TN2602 Boards with 80 VoIP Channels: 128 0 Maximum TN2602 Boards with 320 VoIP Channels: 128 0 Maximum Number of Expanded Meet-me Conference Ports: 300 0 (NOTE: You must logoff & login to effect the permission changes.) </pre>

Step	Description
2.	<p>IP network region</p> <p>All equipment at the main site were located in a single IP network region (IP network region 1) using the parameters described below. Use the display ip-network-region command to view these settings. The example below shows the values used during compliance testing.</p> <ul style="list-style-type: none"> ▪ Authoritative Domain: <i>avaya.com</i> This field was configured to match the domain name configured on Session Manager. The domain will appear in the “From” header of SIP messages originating from this IP region. ▪ Name: Any descriptive name may be used (if desired). ▪ Intra-region IP-IP Direct Audio: <i>yes</i> Inter-region IP-IP Direct Audio: <i>yes</i> By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the Signaling Group form. ▪ Codec Set: <i>1</i> The codec set contains the list of codecs available for calls within this IP network region. <pre> display ip-network-region 1 IP NETWORK REGION Page 1 of 20 Region: 1 Location: Authoritative Domain: avaya.com Name: MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes Codec Set: 1 Inter-region IP-IP Direct Audio: yes UDP Port Min: 2048 IP Audio Hairpinning? n UDP Port Max: 3329 DIFFSERV/TOS PARAMETERS Call Control PHB Value: 46 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 AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS RSVP Enabled? n H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 20 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5 </pre>

Step	Description
3.	<p>Codecs</p> <p>IP codec set 1 was used during compliance testing. Multiple codecs were listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The example below shows the values used during compliance testing. It should be noted that when testing the use of each individual codec, only the single codec under test was included in the list.</p> <pre>display ip-codec-set 1</pre> <p style="text-align: right;">Page 1 of 2</p> <pre> IP Codec Set Codec Set: 1 Audio Silence Frames Packet Codec Suppression Per Pkt Size (ms) 1: G.711MU n 2 20 2: G.729AB n 2 20 3: 4: 5: 6: 7: </pre>
4.	<p>Node Names</p> <p>Use the change node-names ip command to create a node name for the IP address of Session Manager. Enter a descriptive name in the Name column and the IP address assigned to Session Manager in the IP address column.</p> <pre>change node-names ip</pre> <p style="text-align: right;">Page 1 of 2</p> <pre> IP NODE NAMES Name IP Address CM_20_40 10.64.20.40 SM_20_31 10.64.20.31 SM_21_31 10.64.21.31 default 0.0.0.0 msgserver 10.64.21.41 procr 10.64.21.41 procr6 :: </pre>

Step	Description
5.	<p>Signaling Group Signaling group 1 was used for the signaling group associated with the SIP trunk group between Communication Manager and Session Manager. Signaling group 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Near-end Node Name: <i>procr</i> This node name maps to the IP address of the Avaya S8300D Server. Node names are defined using the change node-names ip command. ▪ Far-end Node Name: <i>SM_21_31</i> This node name maps to the IP address of Session Manager. ▪ Far-end Network Region: <i>1</i> This defines the IP network region which contains Session Manager. ▪ Far-end Domain: <i>avaya.com</i> This domain is sent in the “To” header of SIP messages of calls using this signaling group. ▪ Direct IP-IP Audio Connections: <i>y</i> This field must be set to <i>y</i> to enable media shuffling on the SIP trunk. <pre> display signaling-group 1 SIGNALING GROUP Group Number: 1 Group Type: sip IMS Enabled? n Transport Method: tls Q-SIP? n SIP Enabled LSP? n IP Video? n Enforce SIPS URI for SRTP? y Peer Detection Enabled? y Peer Server: SM Near-end Node Name: procr Far-end Node Name: SM_21_31 Near-end Listen Port: 5061 Far-end Listen Port: 5061 Far-end Network Region: 1 Far-end Domain: avaya.com Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Direct IP-IP Audio Connections? y Session Establishment Timer(min): 3 IP Audio Hairpinning? n Enable Layer 3 Test? y Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6 </pre>

Step	Description
6.	<p>Trunk Group</p> <p>Trunk group 1 was used for the SIP trunk group between Communication Manager and Session Manager. Trunk group 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Group Type: sip This field sets the type of the trunk group. ▪ TAC: 101 Enter an valid value consistent with the Communication Manager dial plan ▪ Member Assignment Method: auto Set to Auto. ▪ Signaling Group: 1 This field is set to the signaling group shown in the previous step. ▪ Number of Members: 10 This field represents the number of trunk group members in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk. <pre> display trunk-group 1 Page 1 of 21 TRUNK GROUP Group Number: 1 Group Type: sip CDR Reports: y Group Name: to SM_21_31 COR: 1 TN: 1 TAC: 101 Direction: two-way Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Member Assignment Method: auto Signaling Group: 1 Number of Members: 10 </pre>

Step	Description
	<p>Trunk Group – continued</p> <p>On Page 3:</p> <ul style="list-style-type: none"> The Numbering Format field was set to <i>unk-pvt</i>. This field specifies the format of the calling party number sent to the far-end. The default values may be retained for the other fields.
	<pre> display trunk-group 1 TRUNK FEATURES ACA Assignment? n Measured: none Maintenance Tests? y Numbering Format: unk-pvt UUI Treatment: service-provider Replace Restricted Numbers? n Replace Unavailable Numbers? n Modify Tandem Calling Number: no Show ANSWERED BY on Display? y </pre> <p>Page 3 of 21</p>
7.	<p>Private Numbering</p> <p>Private Numbering defines the calling party number to be sent to the far-end. In the example shown below, all calls originating from a 5-digit extension beginning with 5 and routed across any trunk group will be sent as a 5 digit calling number. The calling party number is sent to the far-end in the SIP “From” header.</p>
	<pre> display private-numbering 0 NUMBERING - PRIVATE FORMAT Page 1 of 2 Ext Len Ext Code Trk Private Total Len Code Grp(s) Prefix Len 5 5 Total Administered: 1 Maximum Entries: 540 </pre>

Step	Description
8.	<p>Automatic Alternate Routing</p> <p>Automatic Alternate Routing (AAR) was used to route calls to Session Manager. In the example shown, dialed numbers that begin with 3 and are 5 digits long use route pattern 1. Route pattern 1 routes calls to the trunk group defined in Step 6.</p> <pre> display aar analysis 3 Page 1 of 2 AAR DIGIT ANALYSIS TABLE Location: all Percent Full: 1 Dialed Total Route Call Node ANI String Min Max Pattern Type Num Req'd 3 5 5 1 aar n 4 7 7 999 aar n 531 5 5 1 unku n 532 5 5 1 unku n 59997 5 5 99 aar n </pre>
9.	<p>Route Pattern</p> <p>Route pattern 1 was used for calls destined for the 2nd site through Session Manager and the Mediant 1000 MSBG e-SBC. Route pattern 1 was configured using the parameters highlighted below.</p> <ul style="list-style-type: none"> ▪ Pattern Name: Any descriptive name. ▪ Grp No: 1 This field is set to the trunk group number defined in Step 6. ▪ FRL: 0 This field sets the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive. <pre> display route-pattern 1 Page 1 of 3 Pattern Number: 1 Pattern Name: to SM_21_31 SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 1 0 2: 3: 4: 5: 6: n user n user n user n user n user n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Format Subaddress 1: y y y y y n n rest lev0-pvt 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 </pre>

6. Configure Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

The Session Manager server contains an SM-100 security module that provides the network interface for all inbound and outbound SIP signaling and media transport to all provisioned SIP entities. During compliance testing, the IP address assigned to the SM-100 interface is 10.64.21.31 as specified in **Figure 1**. The Session Manager server also has a separate network interface used for connectivity to System Manager for provisioning Session Manager. The IP address assigned to the Session Manager management interface is 10.64.21.30. The SM-100 interface and the management interface were both connected to the same IP network. If desired, the SM-100 interface can be configured to use a different network than the management interface.

The procedures described in this section include configurations in the following areas:

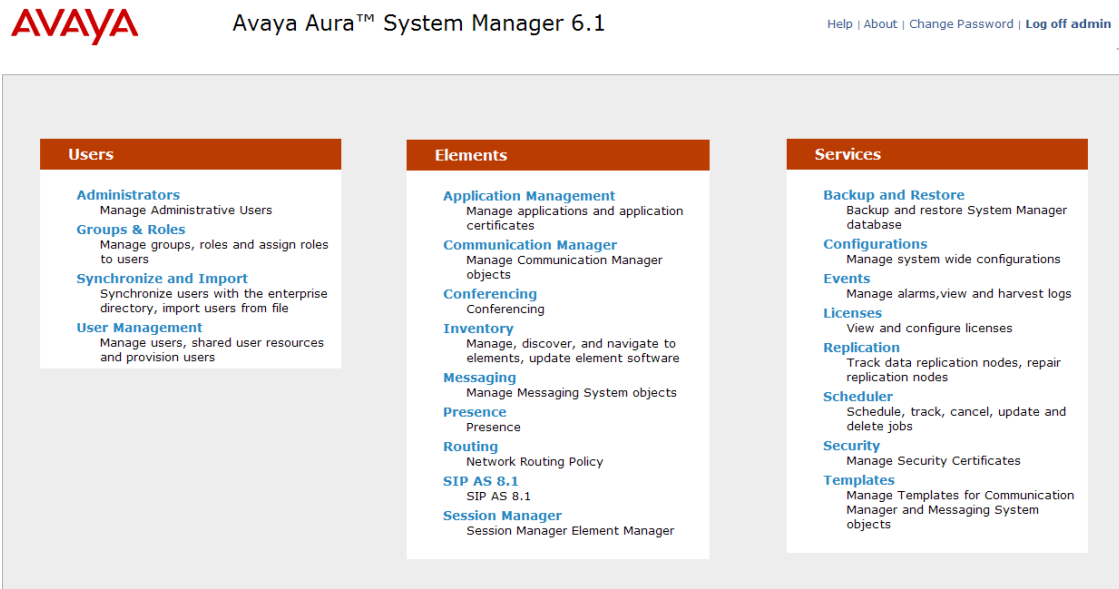
- **SIP domain**
- Logical/physical **Locations** that can be occupied by SIP Entities
- **SIP Entities** corresponding to the SIP telephony systems (including Communication Manager and Session Border Controller) and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Time Ranges** during which routing policies are active
- **Routing Policies** which control call routing between the SIP Entities
- **Dial Patterns** which govern to which SIP Entity a call is routed

1.

Login

Access the Session Manager administration web interface by entering `https://<ip-addr>/network-login/` as the URL in an Internet browser, where `<ip-addr>` is the IP address of the System Manager server.

Log in with the appropriate credentials. The main page for the administrative interface is shown below.



2.

Add SIP Domain

The **Routing** menu contains all the configuration tasks listed at the beginning of this section.

During compliance testing, one SIP Domain was configured on each Session Manager since all SIP entities were located within the same authoritative domain.

Navigate to **Routing→Domains**, and click the **New** button (not shown) to add the SIP domain with

- **Name:** *avaya.com* (as set in **Section 5, Step 2**)
- **Notes:** Optional descriptive text.

Click **Commit** to save the configuration.

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Domains- Domain Management

Domain Management [Help ?](#)

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

1 Item [Refresh](#) Filter: Enable

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

* Input Required [Commit](#) [Cancel](#)

3.

Add Location

Locations identify logical and/or physical locations where SIP entities reside. Only one Location was configured at each site for compliance testing.

Navigate to **Routing**→**Locations** and click the **New** button (not shown) to add the Location.

Under **General**:

- **Name:** A descriptive name.
- **Notes:** Optional descriptive text.

Under **Location Pattern**, click the **Add** button to add a new line:

- **IP Address Pattern:** *10.64.21.**
- **Notes:** Optional descriptive text.

Click **Commit** to save the configuration.

AVAYA Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home /Elements / Routing / Locations- Location Details

Location Details [Help ?](#) [Commit](#) [Cancel](#)

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

General

* Name:

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:

Location Pattern

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.21.*	

Select : All, None

* Input Required [Commit](#) [Cancel](#)

4.	<p>Add SIP Entities</p> <p>A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. During compliance testing, a SIP Entity was added for the Session Manager, Communication Manager, and the AudioCodes Mediant 1000 MSBG e-SBC.</p> <p>Navigate to Routing→SIP Entities, and click the New button (not shown) to add a SIP Entity. The configuration details for the SIP Entity defined for Session Manager are as follows:</p> <p>Under General:</p> <ul style="list-style-type: none"> • Name: A descriptive name. • FQDN or IP Address: <i>10.64.21.31</i> as specified in Figure 1. This is the IP address assigned to the SM-100 security module installed in the Session Manager. • Type: select <i>Session Manager</i>. <p>Under Port, click Add, then edit the fields in the resulting new row as shown below:</p> <ul style="list-style-type: none"> • Port: <i>5060</i>. This is the port number on which the system listens for SIP requests. • Protocol: <i>UDP</i>. UDP was used between Session Manager and AudioCodes during compliance testing. These steps were repeated to add Port 5061 and Protocol TLS for communication between Session Manager and Communication Manager. • Default Domain: Select the SIP Domain created in Step 2. <p>Default settings can be used for the remaining fields. Click Commit to save the SIP Entity definition.</p>
----	--

Add SIP Entities (continued) – Session Manager

The screens below show the SIP Entity configuration details for the Session Manager.



Avaya Aura™ System Manager
6.1

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

[Routing](#) * [Home](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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

SIP Entity Details

Commit

Cancel

Help ?

General

* Name: SM_21_31

* FQDN or IP Address: 10.64.21.31

Type: Session Manager

Notes:

Location:

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add

Remove

7 Items Refresh

Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM_21_31	TCP	* 5060	AuraSBC	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_20_40	* 5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	CM_21_41	* 5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TLS	* 5061	RedSky	* 5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM_21_31	TCP	* 5060	IngateRmtEndpt	* 5060	<input type="checkbox"/>

Port

Add

Remove

3 Items Refresh

Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	avaya.com	
<input type="checkbox"/>	5060	TCP	avaya.com	
<input type="checkbox"/>	5061	TLS	avaya.com	

Select : All, None

Add SIP Entities (continued) – Communication Manager

The screen below shows the SIP Entity configuration details for the Communication Manager. Note the **CM** selection for **Type**.

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) * [Home](#)

[Home / Elements / Routing / SIP Entities- SIP Entity Details](#)

[Help ?](#)

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

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring

SIP Link Monitoring:

Entity Links

[Add](#) [Remove](#)

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	<input type="text" value="SM_21_31"/>	<input type="text" value="TLS"/>	<input type="text" value="* 5061"/>	<input type="text" value="CM_21_41"/>	<input type="text" value="* 5061"/>	<input checked="" type="checkbox"/>

Add SIP Entities (continued) – AudioCodes Mediant 1000 MSBG e-SBC

The screen below shows the SIP Entity configuration details for the AudioCodes Mediant 1000 MSBG e-SBC. Note the *Other* selection for **Type**.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar shows a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains the following configuration fields:

- Name:** AudioCodes_ESBC_MSBC
- FQDN or IP Address:** 10.64.21.95
- Type:** Other (selected from a dropdown)
- Notes:** (empty text field)
- Adaptation:** (empty dropdown)
- Location:** .21 Subnet (selected from a dropdown)
- Time Zone:** America/Denver (selected from a dropdown)
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (selected from a dropdown)
- SIP Link Monitoring:**
 - SIP Link Monitoring:** Link Monitoring Enabled (selected from a dropdown)
 - Proactive Monitoring Interval (in seconds):** 120
 - Reactive Monitoring Interval (in seconds):** 60
 - Number of Retries:** 1
- Entity Links:** Add Remove

At the bottom, there is a table with 1 item and a 'Refresh' button. A 'Filter: Enable' button is also present.

5.

Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created: one between Session Manager and Communication Manager; the other between Session Manager and AudioCodes Mediant 1000 MSBG e-SBC.

Navigate to **Routing**→**Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager to Communication Manager.

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager SIP Entity.
- **Port: 5061.** This is the port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the Communication Manager SIP Entity.
- **Port: 5061.** This is the port number on which the other system receives SIP requests.
- **Trusted:** Check this box.
- **Protocol:** Select **TLS** as the transport protocol.
- **Notes:** Optional descriptive text.

Click **Commit** to save the configuration.



Avaya Aura™ System Manager 6.1

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

[Routing](#) * [Home](#)

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Entity Links- Entity Links

Entity Links

1 Item

Refresh

Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CM_21_41	* SM_21_31	TLS	* 5061	* CM_21_41	* 5061	<input checked="" type="checkbox"/>	

* Input Required

Commit

Cancel

Add Entity Links (continued)

The Entity Link for connecting Session Manager to AudioCodes Mediant 1000 MSBG e-SBC was similarly defined as shown in the screen below, using the UDP protocol and port 5060.

Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Entity Links

Commit Cancel Help ?

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* to AudioCodes	* SM_21_31	UDP	* 5060	* AudioCodes_ESBC_MSBG	* 5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

6.


Add Time Ranges

Before adding routing policies (configured in next step), time ranges must be defined during which the policies will be active. One Time Range was defined that would allow routing to occur at anytime.

Navigate to **Routing→Time Ranges**, and click the **New** button to add a new Time Range:

- **Name:** A descriptive name.
- **Mo through Su:** Check the box under each of these headings.
- **Start Time:** Enter **00:00**.
- **End Time:** Enter **23:59**.

Click **Commit** to save this time range. The screen below shows the configured Time Range.


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

Routing
Home

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Time Ranges- Time Ranges

Time Ranges

Edit
New
Duplicate
Delete
More Actions

1 Item Refresh
Filter: Enable

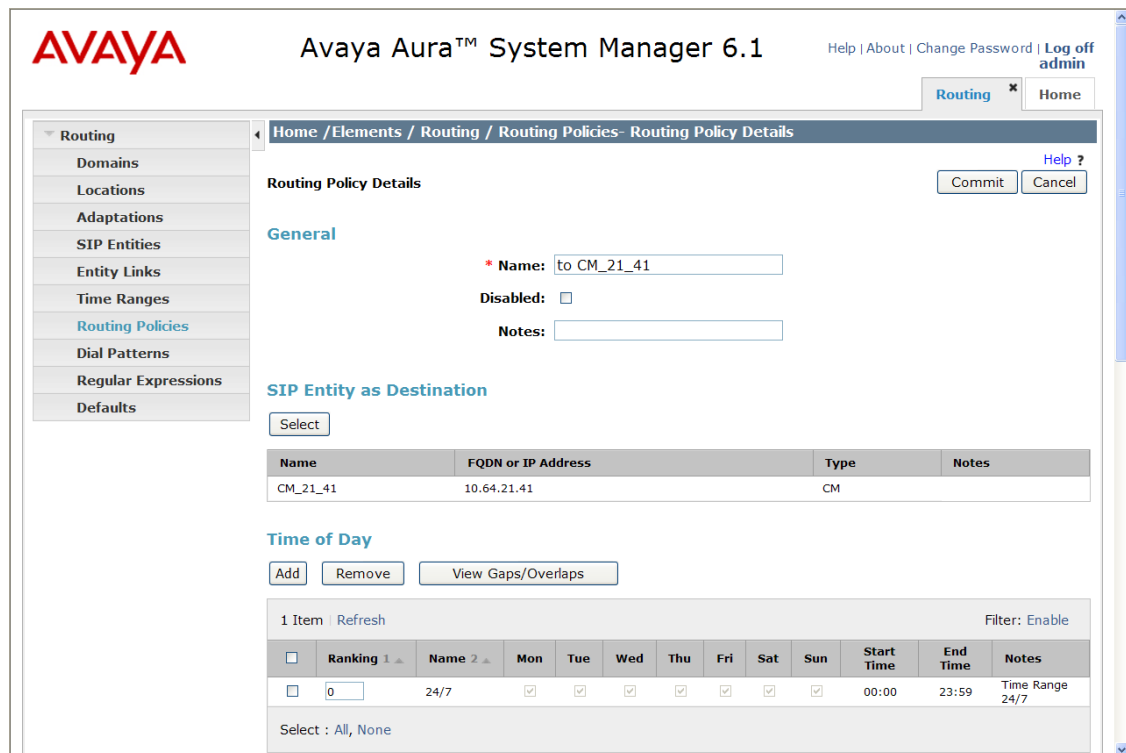
	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

7.	<p>Add Routing Policies</p> <p>Routing policies describe the conditions under which calls will be routed to the SIP Entities connected to the Session Manager. Two routing policies were added – one for routing calls to Communication Manager, and the other for routing calls to AudioCodes Mediant 1000 MSBG e-SBC.</p> <p>Navigate to Routing→Routing Policies, and click the New button (not shown) to add a new Routing Policy.</p> <p>Under General:</p> <ul style="list-style-type: none"> • Name: A descriptive name. • Notes: Optional descriptive text. <p>Under SIP Entity as Destination</p> <p>Click Select to select the appropriate SIP Entity to which the routing policy applies (not shown).</p> <p>Under Time of Day</p> <p>Click Add to select the Time Range configured in the previous step (not shown).</p> <p>Default settings can be used for the remaining fields. Click Commit to save the configuration.</p>
----	---

Add Routing Policies (continued)

The screens below show the configuration details for the two Routing Policies used during compliance testing.



AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details [Help ?](#) [Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
CM_21_41	10.64.21.41	CM	

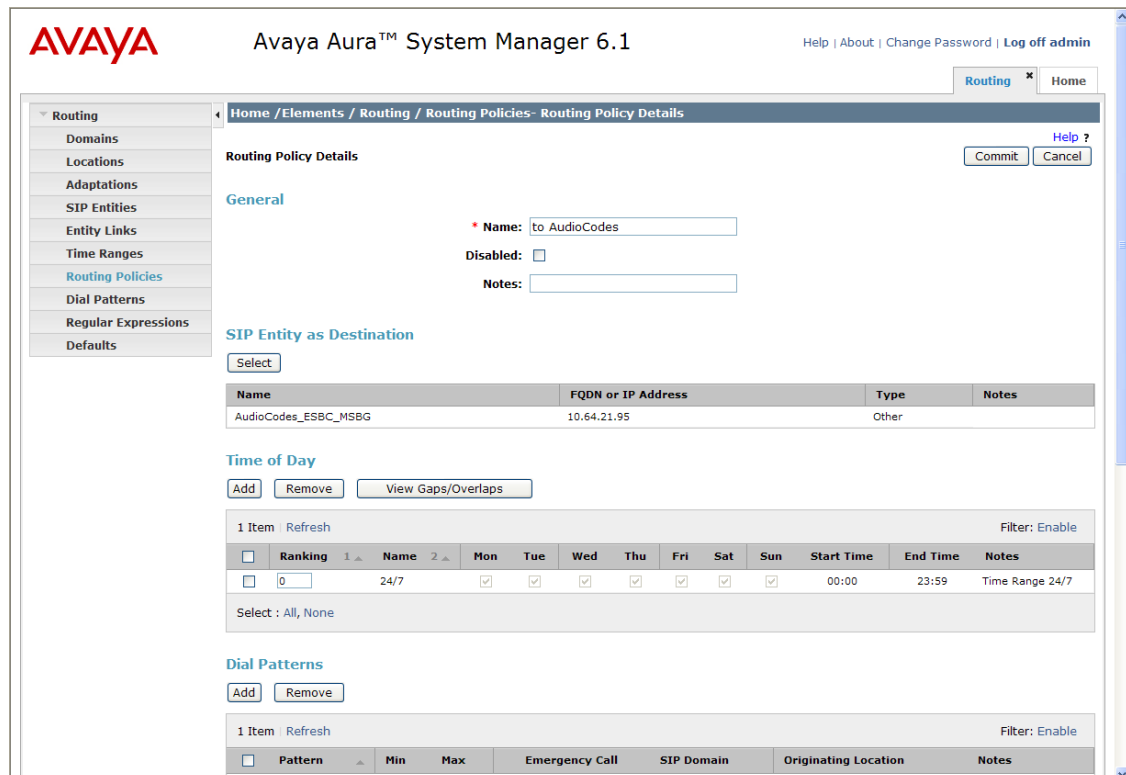
Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None



AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details [Help ?](#) [Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
AudioCodes_ESBC_MSBG	10.64.21.95	Other	

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

[Add](#) [Remove](#)

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	-----------	-----	-----	----------------	------------	----------------------	-------

8.	<p>Add Dial Patterns</p> <p>Dial Patterns define digit strings to be matched against dialed numbers for directing calls to the appropriate SIP Entities. 5-digit extensions beginning with “5” resided on Communication Manager at the main enterprise site. 5-digit extensions beginning with “3” should were routed to AudioCodes Mediant 1000 MSBG e-SBC for onward routing to the 2nd site. Therefore two Dial Patterns were created accordingly.</p> <p>Navigate to Routing→Dial Patterns, click the New button (not shown) to add a new Dial Pattern.</p> <p>Under General:</p> <ul style="list-style-type: none"> • Pattern: Dialed number or prefix. • Min: Minimum length of dialed number. • Max: Maximum length of dialed number. • SIP Domain: Select the SIP Domain created in Step 2 (or select –ALL– to be less restrictive). • Notes: Optional descriptive text. <p>Under Originating Locations and Routing Policies</p> <p>Click Add to select the appropriate originating Location and Routing Policy from the list (not shown).</p> <p>Under Time of Day</p> <p>Click Add to select the time range configured in Step 6.</p> <p>Default settings can be used for the remaining fields. Click Commit to save the configuration.</p>
----	--

Add Dial Patterns (continued)

The screen below shows the configuration details for the Dialed Pattern defined for routing calls to Communication Manager at the main enterprise site.

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details [Help ?](#)

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

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to CM_21_41	0	<input type="checkbox"/>	CM_21_41	

Select : All, None

Denied Originating Locations

Add Dial Patterns (continued)

The screen below shows the configuration details for the Dialed Pattern defined for routing calls to AudioCodes Mediant 1000 MSBG e-SBC (for onward routing to the 2nd site simulating a service provider service node).

AVAYA Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

[Home / Elements / Routing / Dial Patterns- Dial Pattern Details](#)

[Help ?](#)
[Commit](#) [Cancel](#)

Dial Pattern Details

General

* **Pattern:**
* **Min:**
* **Max:**
Emergency Call: ☐
SIP Domain:
Notes:

Originating Locations and Routing Policies
[Add](#) [Remove](#)
1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name ¹ ▲	Originating Location Notes	Routing Policy Name	Rank ² ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to AudioCodes	0	<input type="checkbox"/>	AudioCodes_ESBC_MSBG	

Select : All, None

Denied Originating Locations
[Add](#) [Remove](#)
0 Items [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* **Input Required** [Commit](#) [Cancel](#)

7. Configure AudioCodes Mediant 1000 MSBG e-SBC

This section provides the procedures for configuring the AudioCodes Mediant 1000 MSBG e-SBC. It is assumed that proper knowledge of the AudioCodes MSBG e-SBC usage, configuration, support in general is understood, and the craft person has experience with the product platform. The following information is derived from the product manuals and is referenced only as a general guide. Configuration of the e-SBC will vary for each specific customer environment; however, AudioCodes has provided screenshots (and called-out specific fields on each screen with “arrows”), to show the configuration used during compliance testing.

All of the configuration shown in this section can be completed using the AudioCodes Mediant 1000 MSBG e-SBC web interface. From a browser, enter the IP address of the e-SBC and log in with the appropriate credentials.

7.1. Configure Data and IP Routing Network Parameters

Ensure the IP Data Routing is set properly for support of routing for each network that is intended to interwork (these details are not shown, but they can be found in the installation manual with regards to the WAN interface setting and routing, as well as LAN side settings).

Once the administration is completed for the data segment, submit, Burn to Flash, and restart the device. Navigate to the **Maintenance Actions** page (**Management** tab > **Management Configuration** menu > **Maintenance Actions**).

- Under the **Reset Configuration** group, from the **Burn To FLASH** drop-down list, select **Yes**, and then click the **Reset** button. The Burn to flash will save the configuration and will allow the unit to recover from future resets in the configuration saved.

The device's new configuration (i.e., global IP address) is saved (burned) to the flash memory and the device performs a reset. The Web interface session terminates, as it's no longer accessible using the blade's private IP address.

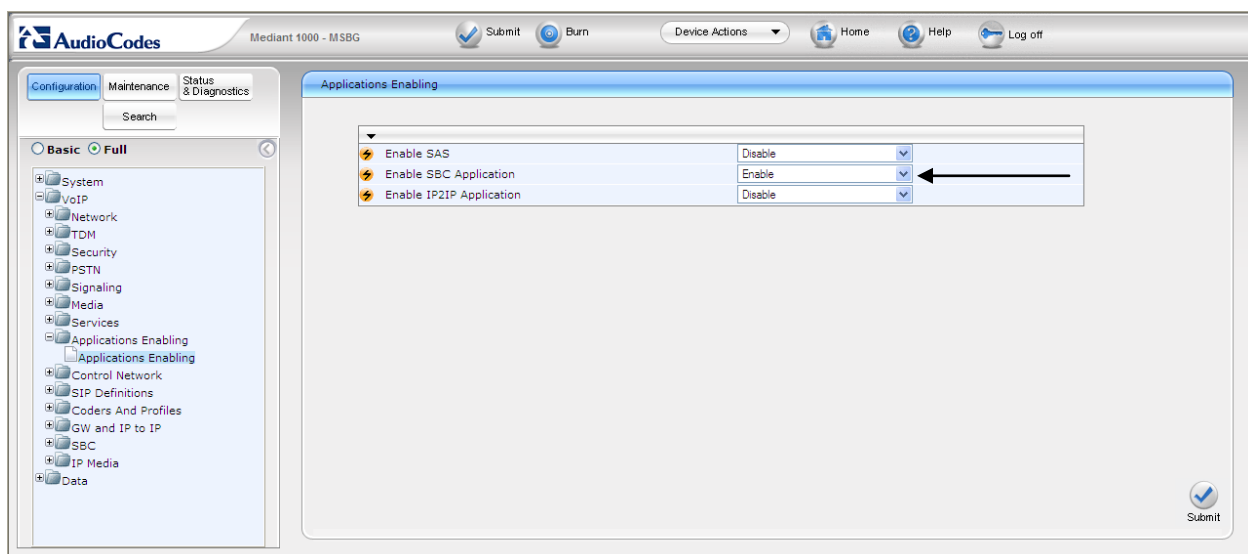
The screenshot displays the web interface for configuring the device. It is divided into three main sections:

- Reset Configuration:** Contains a "Reset Board" button, a "Burn To FLASH" dropdown menu set to "Yes", and a "Graceful Option" dropdown menu set to "No".
- LOCK / UNLOCK:** Contains a "Lock" button, a "Graceful Option" dropdown menu set to "No", and a "Current Admin State" label showing "UNLOCKED".
- Save Configuration:** Contains a "Burn To FLASH" button labeled "BURN".

7.2. Enable SBC functionality

Open the **Applications** page (**Configuration** tab > **VoIP** menu > **Applications Enabling**) to configure the SBC functionality.

- Configure the parameter **Enable SBC Application** to **Enable**.
- Click the **Submit** button to save changes.
- Save the changes to flash memory. This is performed by selecting the **Burn** button at the top of the page. This is referred to as, "Saving Configuration", and will be referenced as such throughout this document.
- Notice the "Lightning Bolt" ⚡. All items marked with this symbol require a reset to take effect. Reset the device as noted previously in **Section 7.1**. Once the device is reset with the SBC application enabled, a submenu within VoIP menu will appear.



7.3. Configure Media Realm

Open the **Media Realm Configuration** page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration** submenu) to configure the Media Realm settings.

- Configure the parameters as required. In the configuration used for compliance testing, only the **LanRealm** was used. The **Port Range Start** field indicates first RTP port of the range defined on the SBC. After the desired **Number of Media Session Legs** is entered, the SBC automatically populates the **Port Range End**.
- Click the **Submit** button to save changes.
- Save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.

The screenshot shows the AudioCodes Mediant 1000 - MSBG configuration interface. The left sidebar contains a tree view with categories: System, VoIP, Network, TDM, Security, PSTN, Signaling, Media, Services, Applications Enabling, Control Network, SIP Definitions, Coders And Profiles, and GW and IP to IP. The 'Media' category is expanded, showing sub-items: Voice Settings, Fax/Modem/CID Settings, RTP/RTCP Settings, IPMedia Settings, General Media Settings, Media Realm Configuration (selected), and Media Security. The main content area is titled 'SIP Media Realm Table' and includes a note: 'Note: Select row index to modify the relevant row.' Below this is a table with the following data:

Index	Media Realm Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End
1	LanRealm	Voice	6000	10	6090
2	WanRealm	WAN	7000	10	7090

Below the table is a field labeled 'Default Media Realm Name' with a dropdown menu. At the bottom right of the interface is a 'Submit' button.

7.4. Configure SRD Table

Open the **SRD Table** page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SRD Table** submenu) to configure the device's Signaling Routing Domain (SRD) table. An SRD is configured with a unique name and assigned a Media Realm (defined in **Section 7.3**). Once configured, SRDs can be used to do the following:

- Associate the SRD with a SIP Interface, IP Group, and Proxy Set
- Define the SRD as a destination IP-to-IP routing rule

Therefore, an SRD is a set of definitions, together creating multiple, virtual multi-service IP gateways. Typically, one SRD is defined for each group of SIP User Agents (e.g. proxies, IP phones, application servers, gateways, soft switches, etc.) that communicate with each other. This provides these entities with VoIP services that reside on the same Layer-3 network (which must be able to communicate without traversing NAT devices and must not have overlapping IP addresses). Routing from one SRD to another is possible, whereby each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

- Select an index that is unused.
- Configure the parameters as required. During compliance testing, **SRD Index 1 (LanSRD)** was mapped to **LanRealm**.
- Click the **Submit** button to save changes.
- Save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.
- Repeat the process for the required SRD(s).
- Ensure that there is a unique SRD name which is bound to a Media Realm created previously.

The screenshot displays the AudioCodes Mediant 1000 - MSBG configuration interface. The left sidebar shows a tree view with categories like System, VoIP, Network, TDM, Security, PSTN, Signaling, Media, Services, Applications Enabling, and Control Network. Under Control Network, the 'SRD Table' is selected. The main panel is titled 'SRD Settings' and contains the following fields:

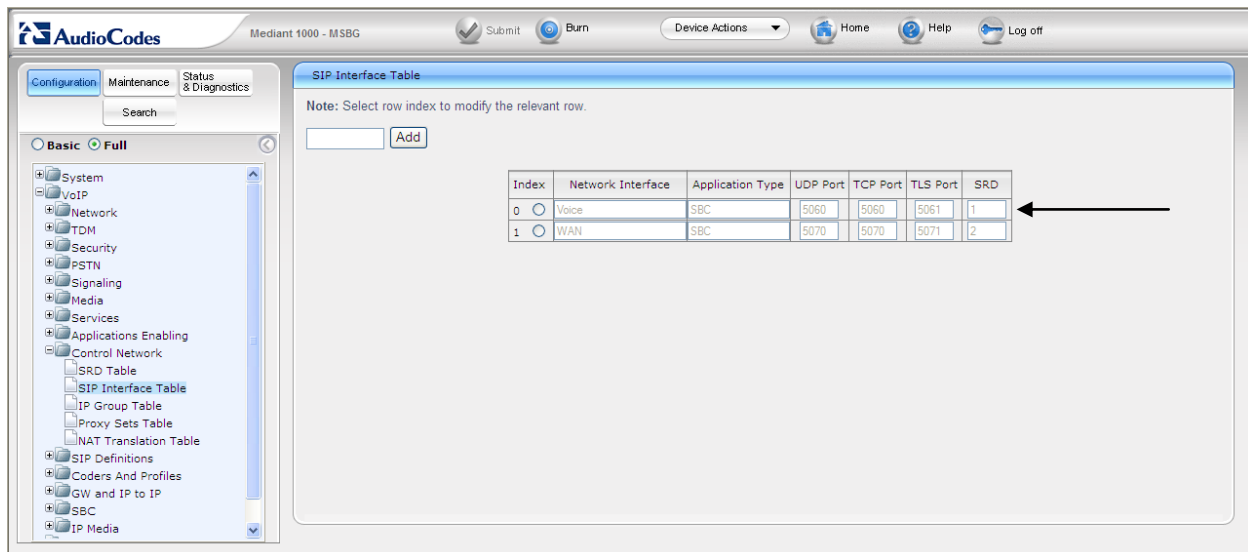
- SRD Index:** A dropdown menu showing '1 - LanSRD'.
- Common Parameters:**
 - SRD Name:** A text field containing 'LanSRD'.
 - Media Realm:** A text field containing 'LanRealm'.
- SBC Parameters:** A section with a '+' icon to expand it.
- IP Group Status Table:** A table with a '+' icon to expand it.
- Proxy Sets Status Table:** A table with a '+' icon to expand it.

At the bottom right of the 'SRD Settings' section are 'Remove' and 'Submit' buttons. Below this is the 'SIP Interface Table' section, which includes an 'Add' button and a note: 'Note: Select row button to modify the relevant row.' The table has the following columns: Network Interface, Application Type, UDP Port, TCP Port, and TLS Port. The first row is selected and shows:

Network Interface	Application Type	UDP Port	TCP Port	TLS Port
Voice	SBC	5060	5060	5061

7.5. Configure SIP Interfaces

Create an interface in the **SIP Interface Table**. Ensure the **Network Interface** name used for the new index matches the name used in the initial settings for IP Settings, in this case **Voice**. This is the interface for the SBC Application. The SIP Interface table below states that the **Network Interface** known as **Voice** is being utilized by the SBC application. It also states that port **5060** should be used for both **UDP** and TCP, and port 5061 should be used for TLS. Note, port 5060 and UDP was utilized during compliance testing for communication between Session Manager and the SBC, as defined in the Entity Link configuration in **Section 6, Step 5**. Finally, the table below states the **Voice** network interface is bound to **SRD 1**.



The screenshot shows the AudioCodes Mediant 1000 - MSBG configuration interface. The left sidebar contains a tree view with categories like System, VoIP, Network, TDM, Security, PSTN, Signalling, Media, Services, Applications Enabling, Control Network, SIP Definitions, Coders And Profiles, GW and IP to IP, SBC, and IP Media. The 'SIP Interface Table' is selected under the 'Control Network' category. The main panel displays a table with the following data:

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
0	Voice	SBC	5060	5060	5061	1
1	WAN	SBC	5070	5070	5071	2

An arrow points to the 'SRD' column of the first row (Index 0).

7.6. Configure the IP Group Table Settings

Open the **IP Group Table** page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**) to configure the IP Group(s) and their respective parameters.

- Configure an unused IP Group index and assign appropriate parameters as required. During compliance testing, two indices were created representing the public interface (**AvayaPublic**) and the private interface (**AvayaPrivate**) on the SBC. Both indices used the **LanRealm** and **SRD 1** defined in **Sections 7.3** and **7.4**, respectively.
- Click the **Submit** button to save changes.
- Repeat previous two steps for the required amount of routes needed.
- To save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.

The screenshot displays the AudioCodes Mediant 1000 - MSBG configuration interface. The left sidebar shows the navigation tree with 'IP Group Table' selected under 'Control Network'. The main panel is titled 'IP Group Table' and contains a 'Basic Parameter List' on the right. The 'Common Parameters' section is expanded, showing the following settings:

Parameter	Value
Type	SERVER
Description	AvayaPublic
Proxy Set ID	1
SIP Group Name	
Contact User	
SRD	1
Media Realm	LanRealm
IP Profile ID	0

The 'Gateway Parameters' section is also expanded, showing the following settings:

Parameter	Value
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard

Below the 'IP Group Table' section, the 'SBC Parameters' section is visible, showing the following settings:

Parameter	Value
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1

Arrows point to the 'Basic Parameter List' header, the 'Common Parameters' section, the 'Gateway Parameters' section, and the 'SBC Parameters' section.

IP Group Table

Basic Parameter List ▲

Index 2 ▼

Common Parameters

Type	SERVER ▼
Description	AvayaPrivate
Proxy Set ID	2 ▼
SIP Group Name	
Contact User	
SRD	1
Media Realm	LanRealm ▼
IP Profile ID	0 ▼

Gateway Parameters

Always Use Route Table	No ▼
Routing Mode	Not Configured ▼
SIP Re-Routing Mode	Standard ▼

Submit

SBC Parameters

Classify By Proxy Set	Enable ▼
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1

7.7. Configure Proxy Set Indices

The use of Proxy Set index is utilized for identifying the specific Proxy (or set of proxy devices) for a respective IP Group Index (reference **Section 7.6** as an example: IP Group 1 is serviced by IP Proxy Set 1). Configure an unused Proxy Set Index and identify the IP address of the proxy for which calls will be routed. Do this for each unique IP group.

Open the **IP Group Table** page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**) to configure the Proxy Set(s) and their respective parameters:

- Configure an unused IP Group index and assign its appropriate parameters as required. (Note: 10.64.21.31 is the IP address of Session Manager and the Enterprise site. 10.64.20.31 is the IP address of Session Manager at the simulated 2nd site)
- Click the **Submit** button to save changes.
- Repeat previous two steps for the required amount of routes needed.
- To save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.

The screenshot shows the AudioCodes Mediant 1000 - MSBG configuration interface. The left sidebar contains a tree view with categories like VoIP, Network, TDM, Security, PSTN, Signaling, Media, Services, Applications Enabling, Control Network, SIP Definitions, Coders And Profiles, GW and IP to IP, SBC, IP Media, and Data. The 'Control Network' category is expanded, showing 'SRD Table', 'SIP Interface Table', 'IP Group Table', 'Proxy Sets Table', and 'NAT Translation Table'. The 'Proxy Sets Table' is selected, and its configuration page is displayed. The page has a 'Proxy Set ID' dropdown set to '1'. Below it is a table with 5 rows for Proxy Address and Transport Type. The first row is filled with '10.64.20.31' and a dropdown. Below this table is another section with parameters: 'Enable Proxy Keep Alive' (Disable), 'Proxy Keep Alive Time' (60), 'Proxy Load Balancing Method' (Disable), 'Is Proxy Hot Swap' (No), 'Proxy Redundancy Mode' (Not Configured), 'SRD Index' (1), and 'Classification Input' (IP only). A 'Submit' button is at the bottom right.

Proxy Address	Transport Type
1 10.64.20.31	
2	
3	
4	
5	

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

This is a close-up of the configuration parameters from the previous screenshot. It shows a table with 7 rows. The first four rows are 'Enable Proxy Keep Alive' (Disable), 'Proxy Keep Alive Time' (60), 'Proxy Load Balancing Method' (Disable), and 'Is Proxy Hot Swap' (No). The fifth row is 'Proxy Redundancy Mode' (Not Configured). The sixth row is 'SRD Index' (1) with a lightning bolt icon. The seventh row is 'Classification Input' (IP only). Arrows point to the 'SRD Index' and 'Classification Input' fields.

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

AudioCodes Mediant 1000 - MSBG

Submit Burn Device Actions Home Help Log off

Configuration Maintenance Status & Diagnostics

Search

Basic Full

- VoIP
 - Network
 - TDM
 - Security
 - PSTN
 - Signaling
 - Media
 - Services
 - Applications Enabling
 - Control Network
 - SRD Table
 - SIP Interface Table
 - IP Group Table
 - Proxy Sets Table
 - NAT Translation Table
 - SIP Definitions
 - Coders And Profiles
 - GW and IP to IP
 - SBC
 - IP Media
 - Data

Proxy Sets Table

Proxy Set ID: 2

	Proxy Address	Transport Type
1	10.64.21.31	
2		
3		
4		
5		

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No

Submit

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

7.8. Configure SIP General Parameters

Open the SIP General Parameters page (Configuration tab > VoIP menu > SIP Definitions submenu > General Parameters) to configure the general SIP protocol parameters.

- Configure the parameters as required. (Note: Transport protocol UDP and Port 5060 were used for communication with Session Manager. See the Entity Link defined in **Section 6, Step 5**).
- Click the **Submit** button to save changes.
- To save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.

AudioCodes Mediant 1000 - MSBG

Configuration Maintenance Status & Diagnostics

Search

Basic Full

System

VoIP

Network

TDM

Security

PSTN

Signaling

Media

Services

Applications Enabling

Control Network

SRD Table

SIP Interface Table

IP Group Table

Proxy Sets Table

NAT Translation Table

SIP Definitions

General Parameters

Advanced Parameters

Account Table

Proxy & Registration

SIP General Parameters

SIP General		
NAT IP Address	0.0.0.0	
PRACK Mode	Supported	
Channel Select Mode	Cyclic Ascending	
Enable Early Media	Disable	
183 Message Behavior	Progress	
Session-Expires Time	0	
Minimum Session-Expires	90	
Session Expires Method	Re-INVITE	
Asserted Identity Mode	Disabled	
Fax Signaling Method	No Fax	
Detect Fax on Answer Tone	Initiate T.38 on Preamble	
SIP Transport Type	UDP	
SIP UDP Local Port	5060	
SIP TCP Local Port	5060	
SIP TLS Local Port	5061	

Basic Parameter List

Submit

AudioCodes Mediant 1000 - MSBG

Configuration Maintenance Status & Diagnostics

Search

Basic Full

System

VoIP

Network

TDM

Security

PSTN

Signaling

Media

Services

Applications Enabling

Control Network

SRD Table

SIP Interface Table

IP Group Table

Proxy Sets Table

NAT Translation Table

SIP Definitions

General Parameters

Advanced Parameters

Account Table

Proxy & Registration

SIP General Parameters

SIP Destination Port	5060	
Use user=phone in SIP URL	Yes	
Use user=phone in From Header	No	
Use Tel URI for Asserted Identity	Disable	
Tel to IP No Answer Timeout	180	
Enable Remote Party ID	Disable	
Add Number Plan and Type to RPI Header	Yes	
Enable History-Info Header	Disable	
Use Source Number as Display Name	No	
Use Display Name as Source Number	No	
Enable Contact Restriction	Disable	
Play Ringback Tone to IP	Don't Play	
Play Ringback Tone to Tel	Prefer IP	
Use Tgrp information	Disable	
Enable GRUU	Disable	
User-Agent Information		

Basic Parameter List

Submit

7.9. Configure General Settings

Open the **General Settings** page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **General Settings**) to configure the general SBC parameters.

- Configure the parameters as required. Note, the **WAN IP Address** below was not used for the compliance tested configuration.
- Allowing of Unclassified calls is optional. All calls were classified by IP Group Index.
- Click the **Submit** button to save changes.
- To save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.

The screenshot shows the AudioCodes Mediant 1000 - MSBG configuration interface. The left sidebar contains a tree view with the following structure:

- Configuration
- Maintenance
- Status & Diagnostics
- Basic
- Full
- General Parameters
- Advanced Parameters
- Account Table
- Proxy & Registration
- Coders And Profiles
- Coders
- Coders Group Settings
- Tel Profile Settings
- IP Profile Settings
- GW and IP to IP
- SBC
 - General Settings
 - Admission Control
 - Allowed Coders Group
 - Routing SBC
 - Classification Table
 - IP to IP Routing Table
 - Alternative Routing Reasons
 - Manipulations SBC
 - IP Media
 - Data

The main area displays the 'General Settings' page for SBC. The parameters are listed in a table:

Basic Parameter List	
WAN IP Address	172.22.201.25
Transcoding Mode	Only if Required
SBC Registration Time	0
SBC No Answer Timeout	600
SBC GRUU Mode	AsProxy
Minimum Session-Expires [sec]	0
Allow Unclassified Calls	Reject

A black arrow points to the 'Only if Required' value in the 'Transcoding Mode' row. A 'Submit' button is located at the bottom right of the main area.

7.10. Configure Coders

Open the **Coders** page for the SBC application (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Allowed Coders Group**) to configure the device's SBC Allowed coders.

- From the **Coder Name** drop-down list, select the required coder. (Note: G.711A-law, G.711U-law, and G.729 were compliance tested)
- Repeat steps for the next optional coders.
- Click the **Submit** button to save changes.
- To save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.

The screenshot shows the AudioCodes Mediant 1000 - MSBG configuration interface. The top navigation bar includes the AudioCodes logo, the device name 'Mediant 1000 - MSBG', and buttons for 'Submit', 'Burn', 'Device Actions', 'Home', 'Help', and 'Log off'. The left sidebar contains a tree view with categories: Configuration, Maintenance, and Status & Diagnostics. Under Configuration, there are sub-categories: Basic and Full. The 'Full' category is selected, and the 'Allowed Coders Group' option is highlighted. The main content area is titled 'Allowed Coders Group' and features a search bar for 'Allowed Coders Group ID' with a value of '0'. Below this is a table with a single column 'Coder Name' containing several drop-down menus. The first three drop-downs are set to 'G.711A-law', 'G.711U-law', and 'G.729'. A 'Submit' button is located at the bottom right of the configuration area.

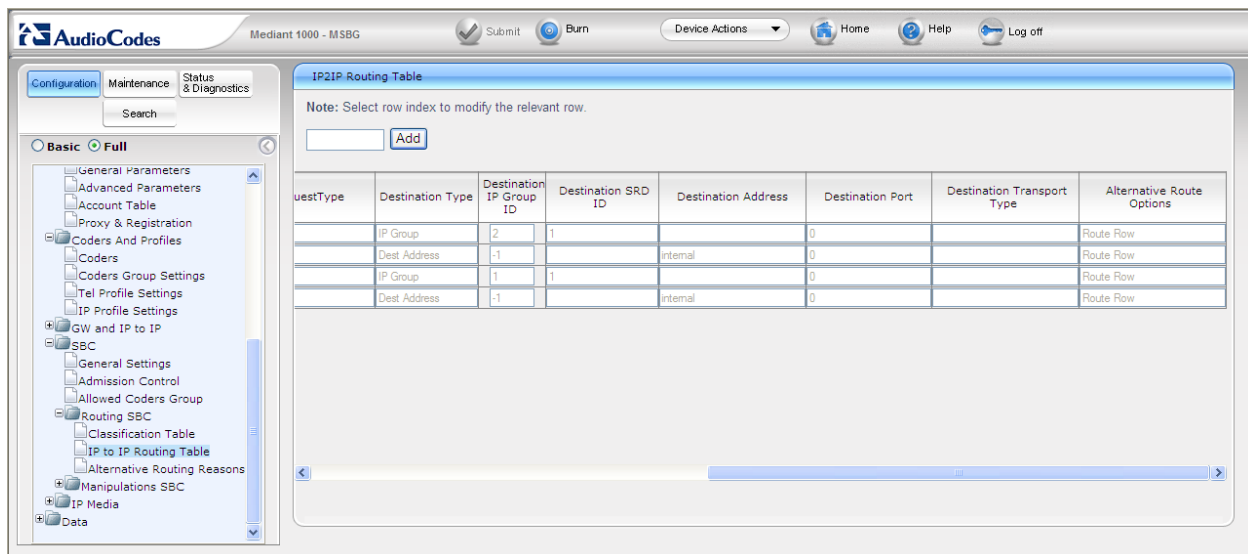
7.11. Configure IP to IP Routing Table

Open the **IP to IP Routing Table** page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **IP to IP Routing Table**) to configure IP2IP routing rules.

The figures below shows the following configured outbound IP routing rules:

- **Rule 1:** If the incoming message originates from Source IP Group “1” and is associated with a call (Invite) then the call will be routed to a Destination IP Group of “2” and an SRD of “1”.
 - **Rule 2:** If the incoming message is not associated with a call, and originates from Source IP Group “1”, then terminate the message to the internal device. This is set to enable the Avaya method of Heartbeat interworking for the product to return a 200 OK rather than send the received “Options” message to the terminating route.
 - **Rule 3:** If the incoming message originates from Source IP Group “2” and is associated with a call (Invite) then the call will be routed to a Destination IP Group of “1” and an SRD of “1”.
 - **Rule 4:** If the incoming message is not associated with a call, and originates from Source IP Group “2”, then terminate the message to the internal device. This is set to enable the Avaya method of Heartbeat interworking for the product to return a 200 OK rather than send the received “Options” message to the terminating route.
- From the **Routing Index** drop-down list, select the range of entries that you want to add.
 - Configure the outbound IP routing rules according to the table below.
 - Click the **Submit** button to apply changes.
 - To save the changes to flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.

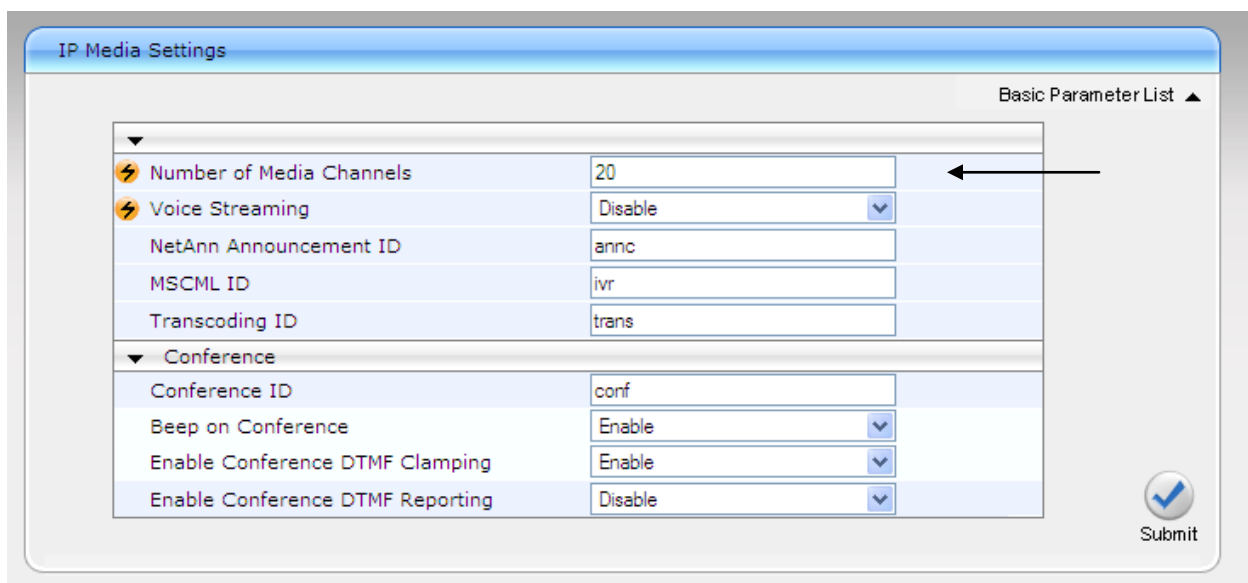
Index	Source IP Group	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	RequestType	Destination Type	De IF
1	1	*	*	*	*	INVITE	IP Group	1
2	1	*	*	*	*	All	Dest Address	1
3	2	*	*	*	*	INVITE	IP Group	1
4	2	*	*	*	*	All	Dest Address	1



7.12. Configure IP Media Settings

Open the **IP Media Settings** page (**Configuration** tab > **VoIP** menu > **IP Media** submenu > **IP Media Settings**) to configure the IP Media Settings.

- Configure the IP Media Settings according to the required amount of supported sessions.
- Click the **Submit** button to save changes.
- To save the changes to the flash memory, refer to “Saving Configuration” as shown in **Section 7.2**.
- Reset the device to ensure the media resources are properly reserved.



7.13. Configure SRD Table

Open the **SRD Table** page (**Configuration** tab > **VoIP** menu > **Control Network submenu** > **SRD Table submenu**) to view and confirm the device's intended SRD tables and respective routing interdependencies:

- Select the index that was created earlier.
- Insure the configured parameters are set as required.
- Click the IP Group Status and Proxy Sets Status sections to expand.
- Ensure the entries match that of the data previously entered.

Ensure the Network Interface name used for the new index matches the name used in the initial settings for IP Settings. This is the interface for the SBC Application.

The screenshot shows the AudioCodes Mediant 1000 - MSBG configuration interface. The left sidebar contains a tree view with categories like System, VoIP, Network, TDM, Security, PSTN, Signaling, Media, Services, Applications Enabling, Control Network, and SIP Definitions. The 'Control Network' category is expanded, showing 'SRD Table' as the selected item. The main content area is titled 'SRD Settings' and contains several sections: 'SRD Index' with a dropdown set to '1 - LanSRD', 'Common Parameters' with 'SRD Name' set to 'LanSRD' and 'Media Realm' set to 'LanRealm', and 'SBC Parameters'. Below these are two expandable sections: 'IP Group Status Table' and 'Proxy Sets Status Table'. At the bottom right of the 'SRD Settings' section are 'Remove' and 'Submit' buttons. Below the 'SRD Settings' section is the 'SIP Interface Table' with an 'Add' button and a note: 'Note: Select row button to modify the relevant row.' The table has columns for 'Network Interface', 'Application Type', 'UDP Port', 'TCP Port', and 'TLS Port'. The first row is selected, showing 'Voice' for Network Interface, 'SBC' for Application Type, and ports 5060 for UDP, TCP, and TLS.

IP Group Status Table				
Index	Type	Description	Proxy set ID	SIP group name
1	SERVER	AvayaPublic	1	0
2	SERVER	AvayaPrivate	2	0

- If Heart beating is required by the device, ensure that the value is set accordingly in the Proxy Set Indices.
- Ensure that there is a unique SRD name which is bound to a Media Realm created previously.

▼ Proxy Sets Status Table	
Index	Enable Proxy Keep Alive
1	Disable
2	Disable

8. Verification Steps

The following steps may be used to verify the configuration:

- Using System Manager, navigate to **Session Manager→System Status→SIP Entity Monitoring**, and click on the appropriate SIP Entities to verify that the Entity Links to the Mediant 1000 MSBG e-SBC and Communication Manager are up.
- From the Communication Manager SAT, use the **status signaling-group x** command to verify that the SIP signaling group is in-service (where **x** is the signaling group number associated with the trunk between Communication Manager and Session Manager).
- From the Communication Manager SAT, use the **status trunk-group y** command to verify that the SIP trunk group is in-service (where **y** is the trunk group number for the trunk between Communication Manager and Session Manager).
- Verify that calls can be placed from both SIP and non-SIP endpoints between sites.

9. Conclusion

The AudioCodes Mediant 1000 MSBG e-SBC passed compliance testing. These Application Notes describe the procedures required to configure the AudioCodes Mediant 1000 MSBG e-SBC to interoperate with Session Manager and Communication Manager to support the network shown in **Figure 1** where Session Manager connects the Mediant 1000 MSBG e-SBC to Communication Manager using SIP trunking interface.

10. Additional References

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

- [1] *Avaya AuraTM Communication Manager Feature Description and Implementation*, Doc # 555-245-205, August 2010.
- [2] *Administering Avaya AuraTM Communication Manager*, Doc # 03-300509, August 2010.
- [3] *Administering Avaya AuraTM Session Manager*, Doc # 03-603324, December 2010.
- [4] *Installing and Configuring Avaya AuraTM Session Manager*, Doc # 03-603472, January 2011.

Product documentation for the AudioCodes Mediant 1000 MSBG e-SBC can be found at <http://www.audiocodes.com/support>.

- [5] *LTTRT-26901_SIP_CPE_Release_Notes_Ver._6.2.pdf*
- [6] *LTTRT-52306_SIP_CPE_Product_Reference_Manual_Ver_6.2.pdf*
- [7] *LTTRT-83508_Mediant_1000_SIP_Installation_Manual_Ver._6.2.pdf*
- [8] *LTTRT-83307_Mediant_600_and_Mediant_1000_SIP_User's_Manual_v6.2.pdf*

11. Appendix – AudioCodes .ini file

For completeness, the AudioCodes Mediant 1000 MSBG e-SBC ini configuration file (with its appropriate parameters) that was used during compliance testing is shown below:

```
.*****  
,  
** Ini File **  
,  
*****
```

[SYSTEM Params]

```
SyslogServerIP = 10.64.21.100  
EnableSyslog = 1  
PM_VEDSPUtil = '1,43,48,15'
```

[BSP Params]

```
PCMLawSelect = 3  
RoutingTableDestinationsColumn = 128.0.0.0  
RoutingTableDestinationPrefixLensColumn = 1  
RoutingTableGatewaysColumn = 10.33.0.1  
WANIPAddress = 172.22.201.25  
WanInterfaceName = 'GigabitEthernet 0/0'
```

[Analog Params]

```
FXSLoopCharacteristicsFilename = 'M1K13-1-fxs16khz.dat'
```

[ControlProtocols Params]

```
AdminStateLockControl = 0
```

[MGCP Params]

[MEGACO Params]

```
EP_Num_0 = 0  
EP_Num_1 = 1
```

EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

CNGDetectorMode = 1
CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
WanMgmtHttpPort = 80

[SIP Params]

GWDEBUGLEVEL = 5
FAXCNGMODE = 1
ENABLESBCAPPLICATION = 1
SBCMAXFORWARDSLIMIT = 70

[SCTP Params]

[VXML Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

.
;
; *** TABLE InterfaceTable ***
;
;
;

```
[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode,
InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName;
InterfaceTable 0 = 6, 10, 10.64.21.95, 24, 10.64.21.1, 1, Voice;
InterfaceTable 15 = 11, 10, 10.64.2.60, 16, 10.64.1.1, 1, Data;
```

```
[ \InterfaceTable ]
```

```
.
;
; *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts
;
```

```
.
;
; *** TABLE CpMediaRealm ***
;
;
;
```

```
[ CpMediaRealm ]
FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF,
CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg,
CpMediaRealm_PortRangeEnd;
CpMediaRealm 1 = LanRealm, Voice, , 6000, 10, 6090;
CpMediaRealm 2 = WanRealm, WAN, , 7000, 10, 7090;
```

```
[ \CpMediaRealm ]
```

```
.
;
; *** TABLE ProxyIp ***
;
;
;
```

```
[ ProxyIp ]
FORMAT ProxyIp_Index = ProxyIp_IPAddress, ProxyIp_TransportType, ProxyIp_ProxySetId;
ProxyIp 0 = 10.64.20.31, -1, 1;
ProxyIp 1 = 10.64.21.31, -1, 2;
ProxyIp 2 = 172.22.201.21, -1, 3;
```

```
[ \ProxyIp ]
```

```
.
;
; *** TABLE IpProfile ***
;
;
;
```

```
[ IpProfile ]
```

```

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay,
IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort, IpProfile_CNGmode,
IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupID, IpProfile_MediaIPVersionPreference,
IpProfile_TranscodingMode, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedCodersMode, IpProfile_SBCMediaSecurityBehaviour,
IpProfile_SBCRFC2833Behavior, IpProfile_SBCAlternativeDTMFMethod,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionsMode,
IpProfile_SBCHistoryInfoMode;
IpProfile 1 = , 1, 0, 1, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, , -1, 0, 0,
-1, 0, 0, 0, 0, -1, 0, 8, 300, 400, -1, -1;

```

[\IpProfile]

```

;
;
; *** TABLE ProxySet ***
;
;
;

```

[ProxySet]

```

FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode;
ProxySet 0 = 0, 60, 0, 0, 0, 0, -1;
ProxySet 1 = 0, 60, 0, 0, 1, 0, -1;
ProxySet 2 = 0, 60, 0, 0, 1, 0, -1;
ProxySet 3 = 0, 60, 0, 0, 2, 0, -1;

```

[\ProxySet]

```

;
;
; *** TABLE IPGroup ***
;
;
;

```

[IPGroup]

```

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability,
IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,

```

```

IPGroup_RoutingMode, IGroup_SRD, IGroup_MediaRealm, IGroup_ClassifyByProxySet,
IPGroup_ProfileId, IGroup_MaxNumOfRegUsers, IGroup_InboundManSet,
IPGroup_OutboundManSet, IGroup_ContactName;
IPGroup 1 = 0, AvayaPublic, 1, , , 0, -1, 0, 0, -1, 1, LanRealm, 1, 0, -1, -1, -1, ;
IPGroup 2 = 0, AvayaPrivate, 2, , , 0, -1, 0, 0, -1, 1, LanRealm, 1, 0, -1, -1, -1, ;
IPGroup 3 = 0, WANMP21, 3, , , 0, -1, 0, 0, -1, 2, WanRealm, 1, 0, -1, -1, -1, ;

```

[\IPGroup]

```

.
;
; *** TABLE IP2IPRouting ***
;
;
;

```

[IP2IPRouting]

```

FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix,
IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,
IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions;
IP2IPRouting 1 = 1, *, *, *, *, 1, 0, 2, 1, , 0, -1, 0;
IP2IPRouting 2 = 1, *, *, *, *, 0, 1, -1, -1, internal, 0, -1, 0;
IP2IPRouting 3 = 2, *, *, *, *, 1, 0, 1, 1, , 0, -1, 0;
IP2IPRouting 4 = 2, *, *, *, *, 0, 1, -1, -1, internal, 0, -1, 0;
IP2IPRouting 5 = 3, *, *, 30x, *, 0, 0, 1, 1, , 0, -1, 0;
IP2IPRouting 6 = 3, *, *, 50x, *, 0, 0, 2, 1, , 0, -1, 0;

```

[\IP2IPRouting]

```

.
;
; *** TABLE SIPInterface ***
;
;
;

```

[SIPInterface]

```

FORMAT SIPInterface_Index = SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD;
SIPInterface 0 = Voice, 2, 5060, 5060, 5061, 1;
SIPInterface 1 = WAN, 2, 5070, 5070, 5071, 2;

```

[\SIPInterface]

```

.
;
; *** TABLE SRD ***
;
;
;

```

[SRD]

```
FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring,  
SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;  
SRD 1 = LanSRD, LanRealm, 0, 0, -1, 1;  
SRD 2 = WanSRD, WanRealm, 0, 0, -1, 1;
```

```
[ \SRD ]
```

```
;  
;  
; *** TABLE CodersGroup0 ***  
;  
;  
;
```

```
[ CodersGroup0 ]  
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,  
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;  
CodersGroup0 0 = g711Alaw64k, 20, 0, -1, 0;  
CodersGroup0 1 = g711Ulaw64k, 20, 0, -1, 0;  
CodersGroup0 2 = g729, 20, 0, -1, 0;
```

```
[ \CodersGroup0 ]
```

©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.