Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the AudioCodesMediant 1000 and Mediant 800 Multi Service Business Gateways with Avaya Aura® Session Manager and Avaya Aura® Communication Manager in a Distributed Trunk Configuration - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the AudioCodesMediant 1000 and Mediant 800 Multi Service Business Gateways with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The AudioCodes Multi Service Business Gateways serve several functions, primarily for branch locations. First, as a bridge, offering connectivity between legacy analog endpoints at a branch location and a VoIP infrastructure at the Enterprise Core using the Session Initiation Protocol (SIP). Second, as a Stand Alone Survivable media gateway providing PSTN access for SIP endpoints when connectivity to the Enterprise Core is lost. Third, as a PSTN Gateway used for least cost routing for the enterprise when connectivity with the Enterprise Core is available.

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 the procedure for configuring the AudioCodesMediant 1000 and Mediant 800 Multi Service Business Gateways with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The AudioCodesMediant Multi Service Business Gateways serve several functions, primarily for branch locations. Both gateways that were tested had 4 FXS (analog endpoint) ports and 4 FXO (POTS trunk) ports, the Mediant 1000 series can be expanded by adding additional modules. Using these ports, PSTN trunks were configured allowing the gateway to connect calls to and from external parties. During normal conditions, calls to the analog trunk were routed to Session Manager as SIP messages, and Session Manager used routing rules to determine where to route the call. Analog endpoints were connected to FXS ports and the gateways acted as a SIP proxy to register these endpoints with Session Manager, enabling the analog endpoints to make and receive calls through Session Manager and the Enterprise Core.

As a Stand Alone Survivable media gateway, the gateways provided PSTN access for analog and SIP endpoints when connectivity to the Enterprise Core was lost. The SIP endpoints alternately registered to Session Manager and the local gateway.When the phones detected the loss of connectivity with Session Manager, they performed a soft reset enabling them to use the Audio Codes gateway as a SIP proxy. The soft reset generally occurred within a minute of loss of WAN, and the reset would also initiate when a user attempted to initiate a call while WAN connectivity was out of service. Upon restoration of the WAN, all phones re-established communications and used Session Manager for call processing, typically within a minute of the link being restored.

In this tested Distributed Trunk configuration, while WAN connectivity to the Enterprise Core was in service, calls to PSTN endpoints in the local calling area of the branch gateway were routed by Session Manager to the Audio Codes gateways. The gateways in turn routed the calls to the PSTN using the FXO ports.An alternate configuration is separately described in *Application Notes for Configuring the AudioCodesMediant 1000 and Mediant 800 Multi Service Business Gateways with Avaya Aura® Session Manager and Avaya Aura® Communication Manager in a Centralized Trunk Configuration.*

2. General Test Approach and Test Results

The general test approach was to make calls to/from the telephones at the branch site using various codec settings and exercising common PBX features.

2.1. Interoperability Compliance Testing

The testing included the analog telephones, and Avaya SIP telephones. The calls were made to/from Enterprise users located in each branch as well as in the central Enterprise Core location, to and from the PSTN and within the branch site. The same test cases, where applicable, were repeated with a simulated data WAN outage using the local analog trunks to access the PSTN.

2.2. Test Results

The AudioCodesMediant 1000 and Mediant 800 Multi Service Business Gateways successfully passed compliance testing. The following features and functionality were verified using both an analog endpoint as well as a variety of Avaya SIP endpoints when the data WAN was available.

- Calls to/from endpoints registered to the Enterprise Core
- Calls to/from the PSTN(routed by Session Manager through the local gateway FXO ports)
- Intra-branch calls
- Distributed Call Routing for calls to/from local branch endpoints
- Distributed Call Routing for calls to/from Enterprise endpoints (users in other locations)
- G.711mu, G.722 and G.729AB codec support
- Proper recognition of DTMF transmissions
- Local device support for Hold, Transfer, and Call Waiting (on analog phones)
- Call Forwarding provided by Avaya Communication Manager.
- Conferencing
- Extended telephony features using Avaya Communication Manager Feature Name Extensions such as Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls.
- Proper system recovery after a restart

The following features and functionality were verified when a simulated data WAN failure was introduced.

- Automatic routing to the POTS line to complete calls to the Enterprise Core including voicemail, and the PSTN using full 11 digit dialing. Incoming calls to the branch were limited to the single POTS number assigned to the branch.
- Intra-branch calls (i.e. calls to the POTS lines to each respective branch)
- Local device support for Hold, Transfer, Conference and Call Waiting
- Survivability of active calls (requires shuffling)

2.3. Support

For technical support, contact AudioCodes via the support link at www.audiocodes.com.

3. Reference Configuration

The lab test environment used for the AudioCodesMediant 1000 and Mediant 800 Multi Service Business Gateways solution testing is shown in **Figure 1.** This test bed included the following components:

- Branches
  - AudioCodes Multi Service Business Gatewayswith analog FXS stations and analog FXO PSTN trunks
  - 9600 and 96x1 SIP phones
- Headquarters/Datacenter
  - Avaya Aura® Communication Manager
  - Avaya Aura® Session Manager
  - Avaya G450 Media Gateway
  - HTTP Phone Configuration Server (not shown)
- PSTN
  - Simulated lab PSTN analog trunks used.

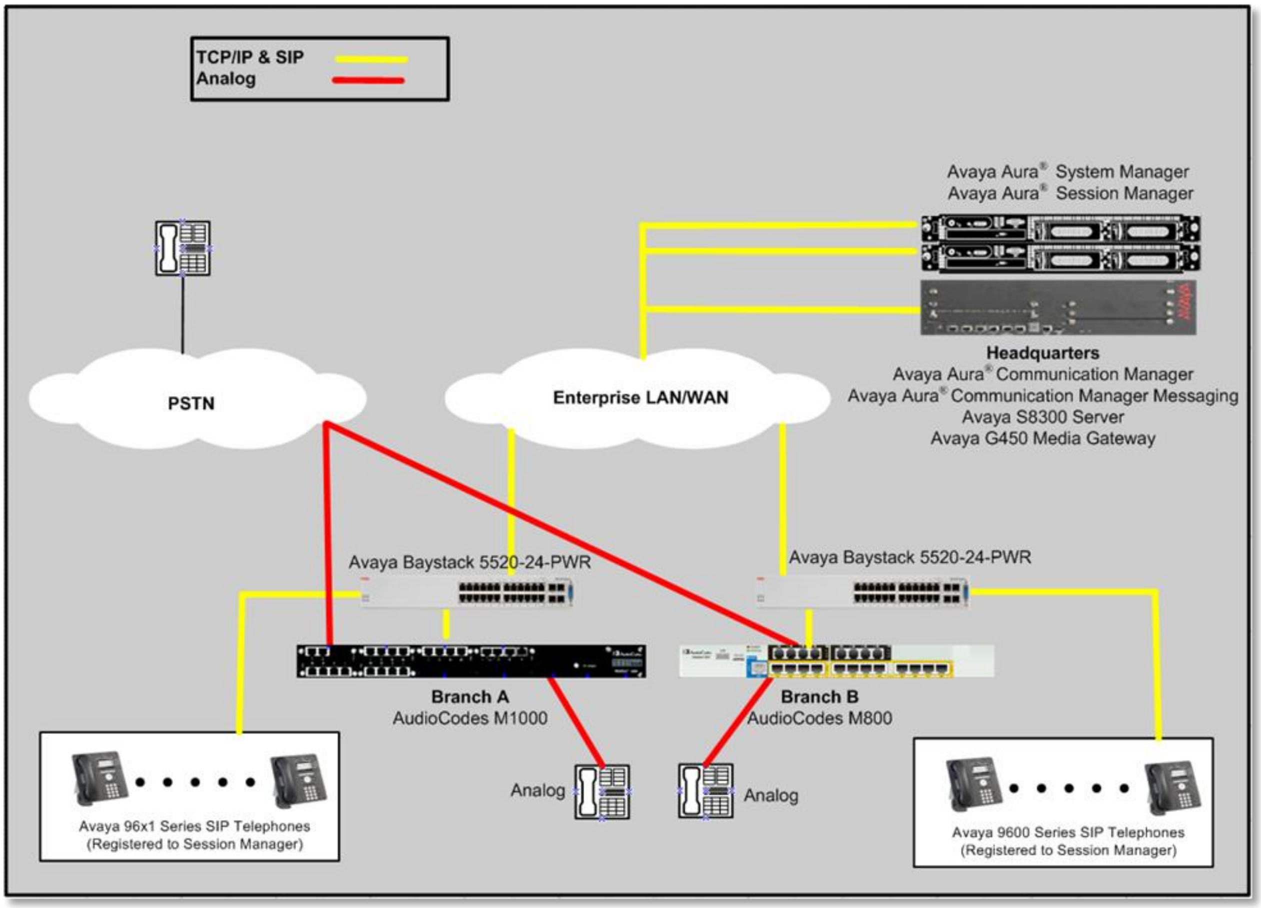


Figure 1: AudioCodes Multi Service Business Gateways Test Configuration

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300D with G450 Media Gateway	Avaya Aura® Communication Manager 6.0.1 SP3 (R016x.00.1.510.1-19009)
Avaya Aura® System Manager	6.1.0.0.7345-6.1.5.106
Avaya Aura® Session Manager	6.1.3.0.613006
Avaya 96x1 Series IP Telephones • 9611G/9621G/9641G	SIP version 6.0.1
Avaya 9600Series IP Telephones • 9620/9630	SIP version 2.6.4
Analog Telephones	-
Windows Server (HTTP Server for phone settings files)	Windows 2003
AudioCodesMediant 1000B	6.20A.032.002
AudioCodesMediant 800	6.20A.032.002

Figure 2: AudioCodesMediant 1000 Multi Service Business Gateway

Figure 2: AudioCodesMediant 800 Multi Service Business Gateway

5. Configure Avaya Aura® Communication Manager

The configuration between Avaya Aura® Communication Manager and Avaya Aura® Session Manager was via a SIP trunk group. This configuration was in place prior to this test, and followed standard configuration. Full details of this part of the configuration are not relevant to the tested solution. Only those particular configuration settings that are helpful to understanding the tested solution are provided, primarily relating to call routing.

5.1. Configuration Details for Communication Manager

The following configuration of Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

The changes made were:

- Configure IP Network Regions
- Configure IP Codecs
- Configure Signaling Group for Session Manager
- Configure SIP Trunks for Session Manager
- Configure Numbering Format for SIP Calls to Session Manager
- Create a route pattern that will use the SIP trunk to Session Manager
- Map Incoming DID Numbers to Internal Route Points
- Configure the Phone Settings File

Step	Description
1.	**Configure IP Network Regions**

Use the **change ip-network-region *n*** command, where ***n*** is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the region. In the case of the compliance test, the same IP network region that contains the S8300 Media Server and IP Telephones was selected to contain the Session Manager server. By default, the Media Server and IP telephones are in IP Network Region 1.

On the **IP Network Region** form:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is ***avaya.com***. This name will appear in the "From" header of SIP messages originating from this IP region.
- By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the G450 Media Gateway. This is true for both intra-region and inter-region IP-IP Direct Audio. Shuffling can be restricted at the trunk level on the **Signaling Group** form.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within this IP network region. If different IP network regions are used for the Avaya S8300 Media Server and the Session Manager server, then Page 3 of each **IP Network Region** form must be used to specify the codec set for inter-region communications.
- The default values can be used for all other fields.

```
changeip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       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
```

Step	Description
2.	**Configure IP Codecs** Use the **change ip-codec-set *n*** command, where ***n*** is the codec set value specified in Step 1, to enter the supported audio codecs for calls routed to Session Manager. Multiple codecs can be listed in priority order to allow the codec to be negotiated during call establishment. The list should include the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test.

```
changeip-codec-set 1                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  PerPkt  Size(ms)
 1: G.722.1-32K                 1        20
2: G.711MU           n         2        20
 3: G.729             n         2        20
```

Step	Description
3.	**Configure Signaling Group for Session Manager** Use the **add signaling group *n*** command, where ***n*** is the number of an unused signaling group, to create the SIP signaling group as follows: ▪ Set the **Group Type** field to ***sip***. ▪ The **Transport Method** field will default to ***tls*** (Transport Layer Security). ▪ Set **Peer Detection Enabled?**to***y*** ▪ Specify the S8300 Media Server (node name ***procr***) and the Session Manager (node name ***AuraSM***) as the two ends of the signaling group in the **Near-end Node Name** and the **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form (not shown). ▪ Ensure that the TLS port value of ***5061*** is configured in the **Near-endListenPort** and the **Far-endListenPort** fields. ▪ In the **Far-end Network Region** field, enter the IP network region value assigned in the **IP Network Region** form in **Step 3.** This defines which IP network region contains the Session Manager. If the **Far-end Network Region** field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the inter-region connectivity for the pair of network regions. ▪ Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is ***avaya.com***. This domain is specified in the Uniform Resource Identifier (URI) of the SIP "To" header in the INVITE message. ▪ The **Direct IP-IP Audio Connections** field is set to ***y***. ▪ The **DTMF over IP** field must be set to the default value of ***rtp-payload***for a SIP trunk. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833. ▪ The default values for the other fields may be used.

```
add signaling-group 30                                     Page   1 of   1
                                SIGNALING GROUP

 Group Number: 30             Group Type: sip
  IMS Enabled? nTransport Method: tls
Q-SIP?n                                         SIP Enabled LSP? n
     IP Video? y        Priority Video? n     Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: SM

Near-end Node Name: procr                 Far-end Node Name: AuraSM
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: avaya.com
                                        Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate             RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payloadDirect 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
```

Step	Description
4.	**Configure SIP Trunks for Session Manager**

Add a SIP trunk group by using the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group. For the compliance test, trunk group number 30 was chosen.

On Page 1, set the fields to the following values:

- Set the **Group Type** field to ***sip***.
- Choose a descriptive **Group Name**.
- Specify an available trunk access code (**TAC**) that is consistent with the existing dial plan.
- Set the **Service Type** field to ***tie***.
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously specified in **Step 3**.
- Specify the **Number of Members** supported by this SIP trunk group. 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. In this solution, each analog endpoint at the branch counts as a SIP telephone.
- The default values may be retained for the other fields.

```
change trunk-group 30                                         Page   1 of  22
                                TRUNK GROUP

Group Number: 30                   Group Type: sip          CDR Reports: n
Group Name: AuraSM                      COR: 1        TN: 1        TAC: *030
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tieAuth Code? n
                                              Member Assignment Method: auto
Signaling Group: 30
                                                     Number of Members: 23
```

Step	Description
	Configure SIP Trunks for Session Manager (continued) - Verify the **Numbering Format** field is set to ***unk-pvt***. 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.

```
change trunk-group 30                                           Page   3 of  22
TRUNK FEATURES
ACA Assignment?n            Measured: none
Maintenance Tests?y

Numbering Format: unk-pvt
                                                UUI Treatment: shared
                                              Maximum Size of UUI Contents: 128
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                Modify Tandem Calling Number: no
               Send UCID? y

 Show ANSWERED BY on Display? y
```

Step	Description
5.	**Configure Numbering Format for SIP Calls to Session Manager** Use the **change private-unknown-numbering6** command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in **Step 4**. In the example shown below, all calls originating from a 4-digit extension beginning with 60 and routed across trunk group 30 will be sent as a 4 digit calling number. This calling party number will be sent to the far-end in the SIP “From” header.

```
change private-numbering 6                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext ExtTrk        Private          Total
Len Code           Grp(s)     Prefix          Len
4  60             30                          4     Total Administered: 2
5  45000          30                          5        Maximum Entries: 540
```

Step	Description
6.	**Create a route pattern that will use the SIP trunk to Session Manager** To create a route pattern, use the **change route-pattern *n*** command, where ***n*** is the number of an unused route pattern. Enter a descriptive name for the **Pattern Name** field. Set the **Grp No** field to the trunk group number created for the SIP trunk. 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. The default values may be retained for all other fields.

```
change route-pattern 30                                         Page   1 of   3
                    Pattern Number: 30  Pattern Name: AuraSM
SCCAN?n     Secure SIP? n
GrpFRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
 NoMrkLmt List Del  Digits                               QSIG
DgtsIntw
 1: 300                                                               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  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
Subaddress
 1: y yyyyn  n            rest                                 lev0-pvt  none
 2: y yyyyn  n            rest                                           none
 3: y yyyyn  n            rest                                           none
 4: y yyyyn  n            rest                                           none
 5: y yyyyn  n            rest                                           none
 6: y yyyyn  n            rest                                           none
```

Step	Description
7.	**Map Incoming DID Numbers to Internal Route Points** To map a DID number to a station at the main or branch office, use the **change inc-call-handling-trmttrunk-group *n*** command, where ***n*** is the trunk group number connected to the PSTN from the Avaya G450 Media Gateway. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows four incoming 7-digit numbers being deleted and replaced with the extension number of the desired station. Extension 6050 was the Voicemail access number, and 6005 and 6004 were analog station ports that connected to the FXS ports on the Audio Codes Media Gateways for routing PSTN calls to and from the two branch gateways.

```
changeinc-call-handling-trmt trunk-group 2                     Page   1 of   3
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert            Per Call Night
 Feature        Len      Digits                           CPN/BN   Serv
public-ntwrk    7  5381202          all 6050
public-ntwrk    7  5381220          all 6005
public-ntwrk    7  5383512          all 6004
public-ntwrk    7  5383520          all 6004
```

Step	Description
8.	**Configure the Phone Settings File** The settings file is not actually configured in Communication Manager, but is included in this section for brevity. The goal was to use a single settings file that could be used for all endpoints, in all branches. The complete settings file is not provided as it will differ in each deployment, but the following settings were required for survivable server functionality to apply to the phones. Full details of these settings can be found in the phone documentation [4]. Note, the **SIP_CONTROLLER_LIST** setting can be expanded to include branch gateways, but is overridden by the configuration done in Session Manager for Survivability Servers (see **section 6, Step 2**). Also note that the **SIMULTANEOUS_REGISTRATIONS** parameter must be set to a value that is equal to the number of Avaya SIP servers that the phone will register with. For example, if the phones use a geo-redundant Session Manager scheme as well as a non-Avaya Survivable Branch Gateway, this setting would need to be set to ***2*** allowing the phone to simultaneously register with two Session Managers. Any additional SIP servers the phone is instructed to register with, be it via settings file or Session Manager User Configuration will be treated as "***alternate***" registrations. This is required as non-Avaya registrars are unable to provide all of the Advanced SIP Telephony (AST) and supplementary services (PPM, Presence) that Avaya AST servers are able to provide.

```
SET REGISTERWAIT "60"
SET WAIT_FOR_REGISTRATION_TIMER 32
SET WAIT_FOR_UNREGISTRATION_TIMER 32
SET TCP_KEEP_ALIVE_STATUS 1
SET TCP_KEEP_ALIVE_TIME 60
SET TCP_KEEP_ALIVE_INTERVAL 10
SET SIP_CONTROLLER_LIST 10.64.21.31:5061
SET CONTROLLER_SEARCH_INTERVAL 4
SET FAST_RESPONSE_TIMEOUT 2
SET RECOVERYREGISTERWAIT 10
SET FAILBACK_POLICY auto
SET SIPREGPROXYPOLICY alternate
SET SIMULTANEOUS_REGISTRATIONS 1
SET DISCOVER_AVAYA_ENVIRONMENT 1
```

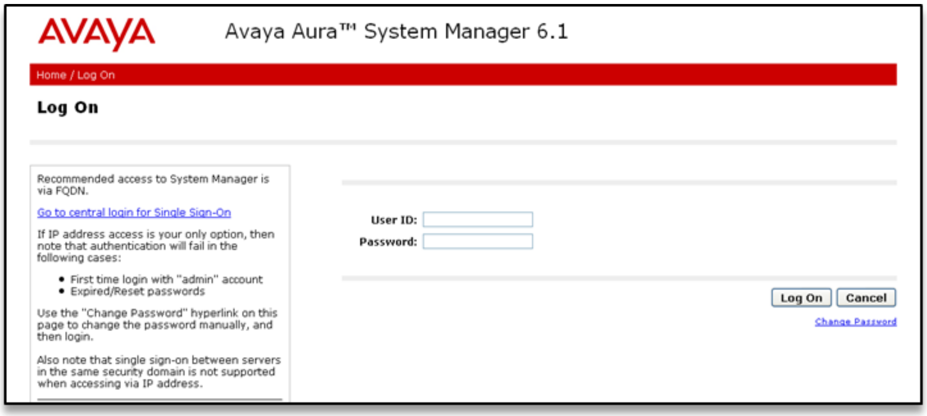
6. Configure Avaya Aura® Session Manager

This section covers the configuration of Avaya Aura® Session Manager. Session Manager is configured via Avaya Aura® System Manager using an Internet browser.

6.1. Configuration Details for Session Manager

As this test used an in place, standard configuration for the core SIP elements, only those steps relevant to the configuration of the AudioCodes Multi Service Business Gateways will be described. Additional details pertaining to call routing are also provided in order to understand the functional elements of this tested solution.For additional information on these and other configuration tasks, refer to [3].

Session Manager is configured using browser access to System Manager. Enter the URL of System Manager such as **https://<*hostname*>/SMGR** where **<*hostname*>** is the ip address or qualified domain name of the System Manager. Login using appropriate credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

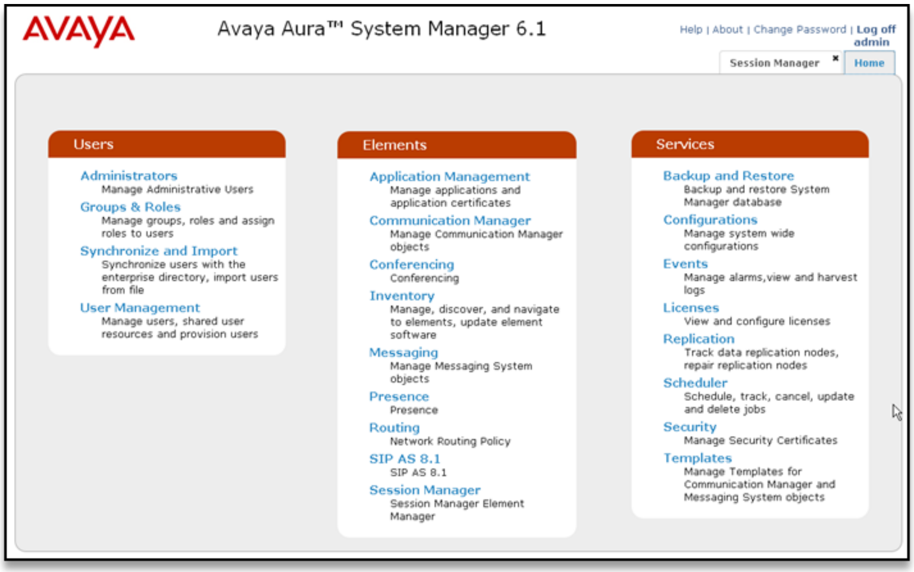
If IP address access is your only option, then note that authentication will fail in the following cases:

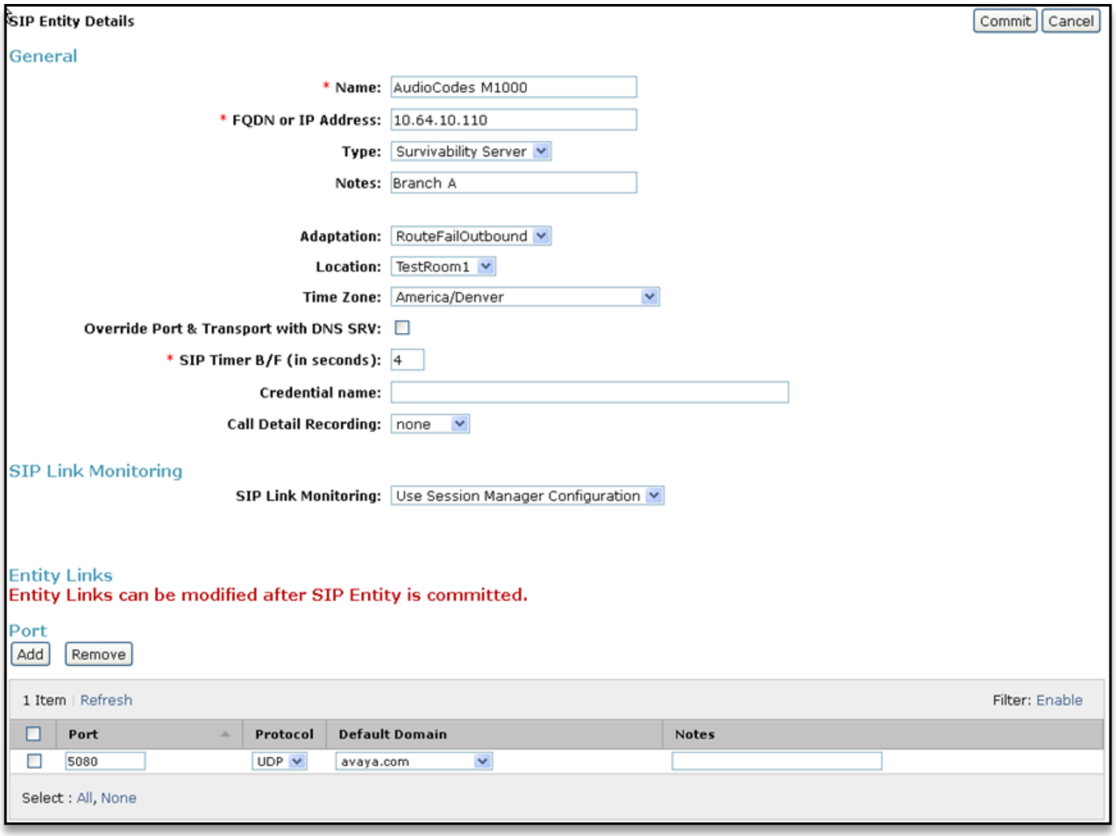
- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

The home page is a navigation screen as shown below. Each of these links will open a new tab from which to navigate to the details of the managed environment.

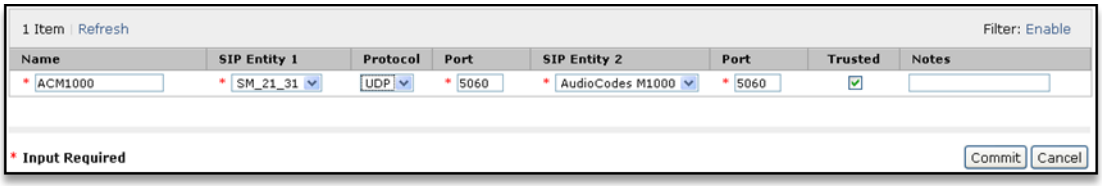


Step	Description
1.	**Add SIP Entity and Entity Links for Each Branch Gateway** Each AudioCodes Multi Service Business Gateway establishes a UDP SIP connection to Session Manager. The purpose is to establish a socket for heartbeats so the gateway knows when the WAN link is in service. Additionally, when the gateway is used by the Enterprise for call routing, an established SIP Entity Link with the SIP Peer is required in order for calls to be routed to the gateway. The Mediant 1000 was administered as a ***Survivability Server*** Entity **Type**, and was configured to use an existing **Adaptation** that added a 9 to the dialed digit string. This adaptation is described in further detail in the following step. The **Location** (***TestRoom1***) correlated to the location of **Branch A** endpoints and the Mediant 1000 gateway. This location was previously defined and can be used in routing rules as described in **Step 3** below. The **Port** settings ***5080***, ***UDP*****Protocol** and ***avaya.com*****Default Domain** are settings that push to the phones when they register with Session Manager. These entries eliminate the need for, and override these settings if administered on the phone or in phone settings files. The Audio Codes gateways listen for registration from phones on port 5080 using UDP. This step was repeated for the Mediant 800 Branch Gateway using similar settings (not shown).  SIP Entity Details General * Name: AudioCodes M1000 * FQDN or IP Address: 10.64.10.110 Type: Survivability Server Notes: Branch A Adaptation: RouteFailOutbound Location: TestRoom1 Time Zone: America/Denver Override Port & Transport with DNS SRV: ☐ * SIP Timer B/F (in seconds): 4 Credential name: Call Detail Recording: none SIP Link Monitoring SIP Link Monitoring: Use Session Manager Configuration Entity Links Entity Links can be modified after SIP Entity is committed. Port 1 Item | Refresh ☐ Port | Protocol | Default Domain | Notes ☐ 5080 | UDP | avaya.com | Select : All, None

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td></td><td>

Add SIP Entity and Entity Links for Each Branch Gateway (Continued)

Entity Links were administered after completing the **SIP Entity** above by clicking the **Entity Links** navigation link (not shown) and separately administering these settings as shown below.



1 Item | Refresh   Filter: Enable

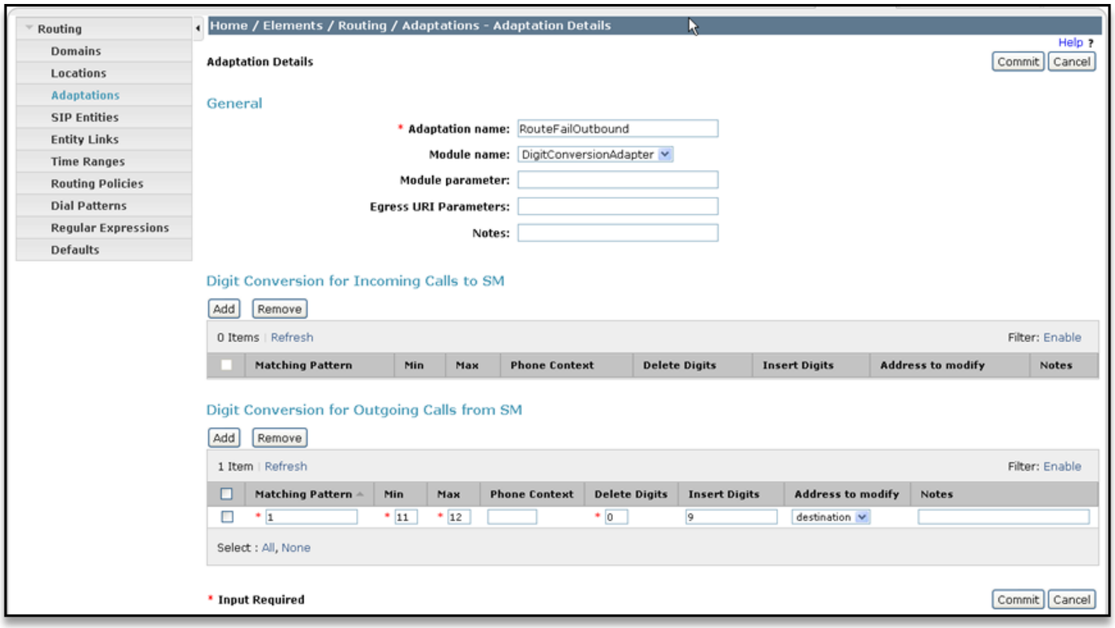
<table>
<tr><th>Name</th><th>SIP Entity 1</th><th>Protocol</th><th>Port</th><th>SIP Entity 2</th><th>Port</th><th>Trusted</th><th>Notes</th></tr>
<tr><td>* ACM1000</td><td>* SM_21_31</td><td>UDP</td><td>* 5060</td><td>* AudioCodes M1000</td><td>* 5060</td><td>☑</td><td></td></tr>
</table>

* Input Required

</td></tr>
<tr><td>2.</td><td>

Configure Adaptation Rules (Optional)

If an Adaptation Rule is applied to a SIP Entity, it is added similar to the following. This was previously defined for another purpose but was used in the tested configuration to simply prepend a 9 to the destination address of an 11 digit dial string so that Communication Manager could properly route the calls. This is an optional step as the test environment used a Communication Manager to provide Analog POTS service and required the digits string to be a 12 digit number starting with a 9 for proper routing to the PSTN. Had this been an actual service provider trunk, this step would likely not be required.



Home / Elements / Routing / Adaptations - Adaptation Details

Adaptation Details

General

* Adaptation name: RouteFailOutbound
Module name: DigitConversionAdapter
Module parameter:
Egress URI Parameters:
Notes:

Digit Conversion for Incoming Calls to SM

0 Items | Refresh   Filter: Enable

<table>
<tr><th>☐</th><th>Matching Pattern</th><th>Min</th><th>Max</th><th>Phone Context</th><th>Delete Digits</th><th>Insert Digits</th><th>Address to modify</th><th>Notes</th></tr>
</table>

Digit Conversion for Outgoing Calls from SM

1 Item | Refresh   Filter: Enable

<table>
<tr><th>☐</th><th>Matching Pattern</th><th>Min</th><th>Max</th><th>Phone Context</th><th>Delete Digits</th><th>Insert Digits</th><th>Address to modify</th><th>Notes</th></tr>
<tr><td>☐</td><td>* 1</td><td>* 11</td><td>* 12</td><td></td><td>* 0</td><td>9</td><td>destination</td><td></td></tr>
</table>

Select : All, None

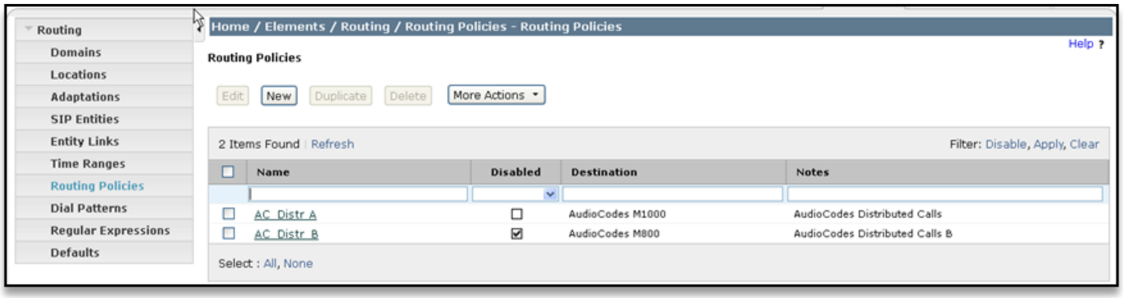
* Input Required

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Configure Routing Policies

In order for calls to be routed to the PSTN through the Audio Codes Analog FXO lines to the PSTN, a Routing Policy was created for each Branch. Below is a summary snapshot of the two Routing Policies:

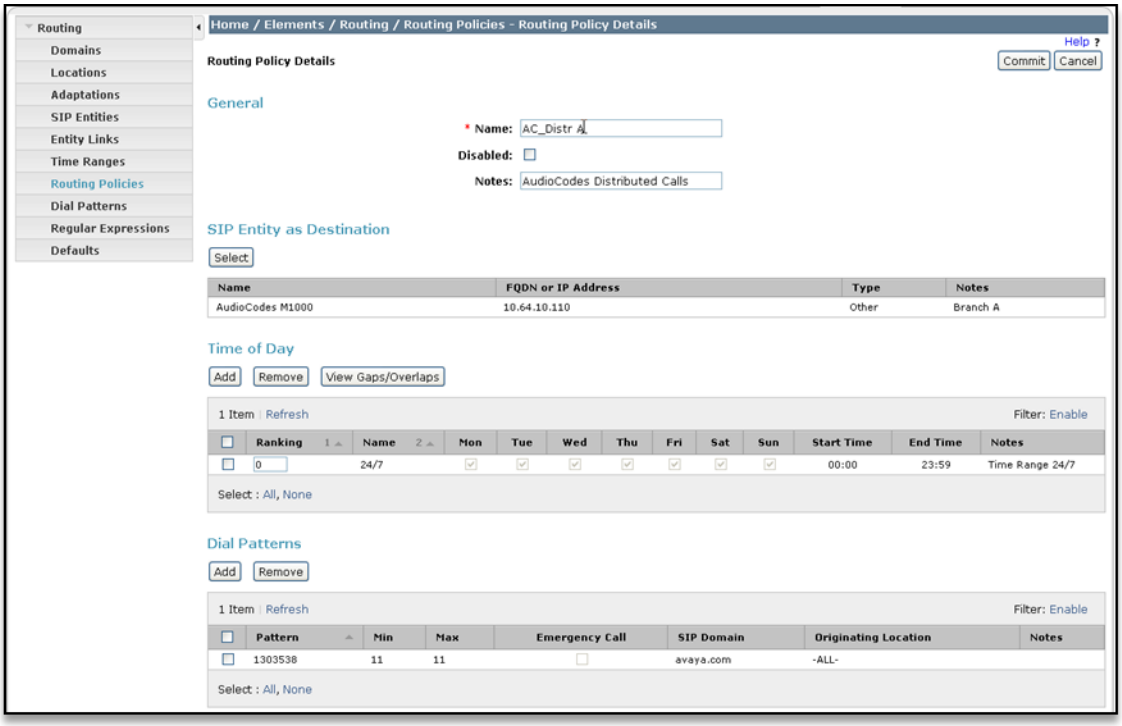


Routing Policies

2 Items Found | Refresh

<table>
<tr><th>☐</th><th>Name</th><th>Disabled</th><th>Destination</th><th>Notes</th></tr>
<tr><td>☐</td><td>AC_Distr_A</td><td>☐</td><td>AudioCodes M1000</td><td>AudioCodes Distributed Calls</td></tr>
<tr><td>☐</td><td>AC_Distr_B</td><td>☑</td><td>AudioCodes M800</td><td>AudioCodes Distributed Calls B</td></tr>
</table>

Each policy was created by clicking the New button in the above screen, and making entries as illustrated below. For calls to be routed out of the POTS line at Branch A, the <i>AudioCodes M1000</i> SIP Entity created in Step 1was selected from a list of all entities (not shown), and <i>1303538</i> was selected from a list of previously administered Dial Patterns. When this policy was enabled, calls from any Enterprise user were routed to the Mediant 1000 at Branch A for routing to the PSTN.



Routing Policy Details

General

* Name: AC_Distr A
Disabled: ☐
Notes: AudioCodes Distributed Calls

SIP Entity as Destination

<table>
<tr><th>Name</th><th>FQDN or IP Address</th><th>Type</th><th>Notes</th></tr>
<tr><td>AudioCodes M1000</td><td>10.64.10.110</td><td>Other</td><td>Branch A</td></tr>
</table>

Time of Day

1 Item | Refresh

<table>
<tr><th>☐</th><th>Ranking 1</th><th>Name 2</th><th>Mon</th><th>Tue</th><th>Wed</th><th>Thu</th><th>Fri</th><th>Sat</th><th>Sun</th><th>Start Time</th><th>End Time</th><th>Notes</th></tr>
<tr><td>☐</td><td>0</td><td>24/7</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>☑</td><td>00:00</td><td>23:59</td><td>Time Range 24/7</td></tr>
</table>

Dial Patterns

1 Item | Refresh

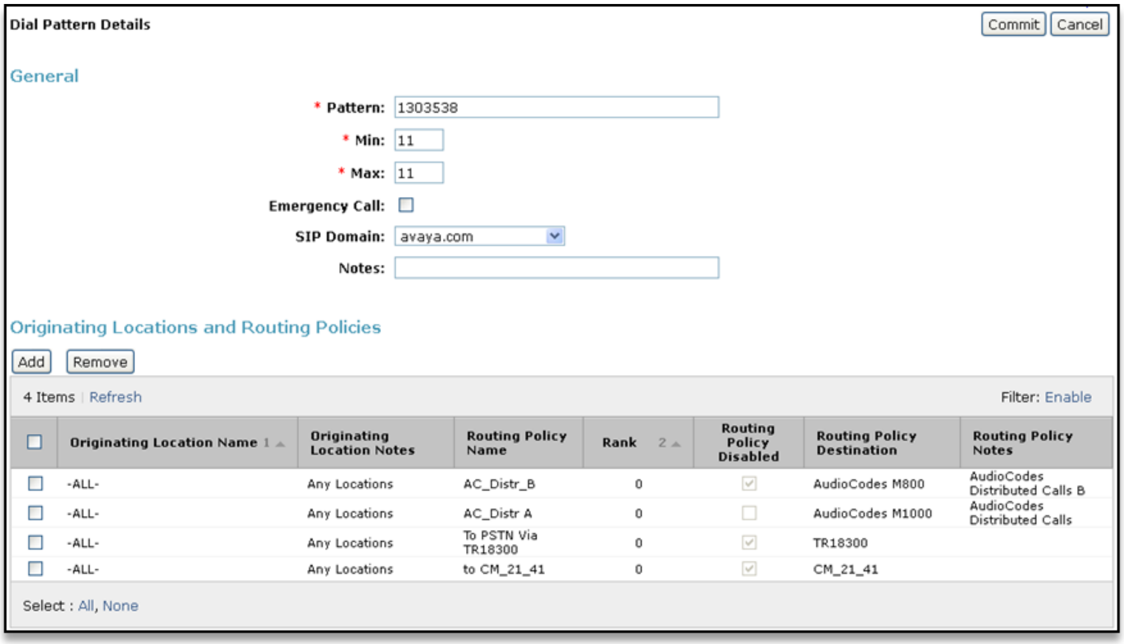
<table>
<tr><th>☐</th><th>Pattern</th><th>Min</th><th>Max</th><th>Emergency Call</th><th>SIP Domain</th><th>Originating Location</th><th>Notes</th></tr>
<tr><td>☐</td><td>1303538</td><td>11</td><td>11</td><td>☐</td><td>avaya.com</td><td>-ALL-</td><td></td></tr>
</table>

</td></tr>
</table>

Step **Description**

Configure Routing Policies (Continued)

The ***1303538*****Dial Pattern** was previously configured as follows. Note that this Dial Pattern was configured to apply to calls originating from ***ALL*** locations.However, dial patternscan also be administered to only apply to calls originating or destined to/from endpoints in the **Test Room 1** location as mentioned in **Step 1** above (not shown).



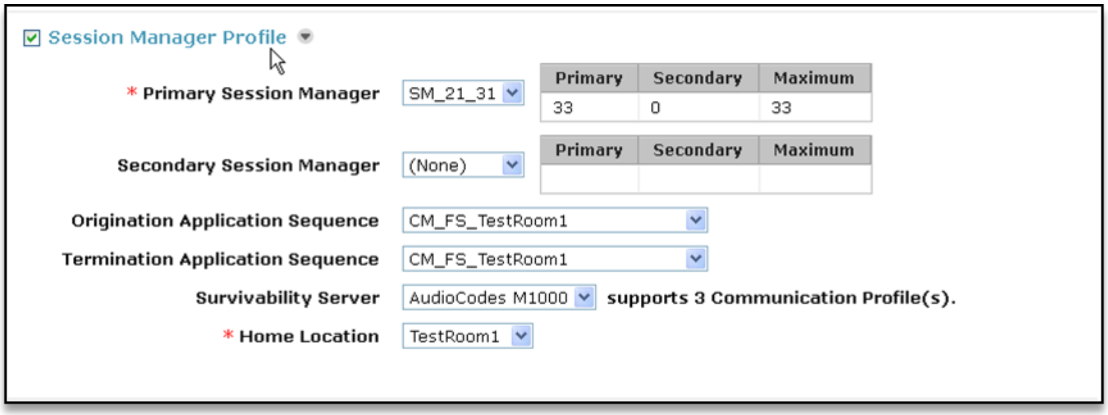
* Pattern: 1303538
* Min: 11
* Max: 11
Emergency Call: ☐
SIP Domain: avaya.com
Notes:

☐	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	-ALL-	Any Locations	AC_Distr_B	0	☑	AudioCodes M800	AudioCodes Distributed Calls B
☐	-ALL-	Any Locations	AC_Distr A	0	☐	AudioCodes M1000	AudioCodes Distributed Calls
☐	-ALL-	Any Locations	To PSTN Via TR18300	0	☑	TR18300	
☐	-ALL-	Any Locations	to CM_21_41	0	☑	CM_21_41	

4.

Modify Existing Users to add a Survivable Server

All endpoints were previously created, existing SIP accounts were used for the analog FXS ports at each branch which were previously administered as 9620 SIP set types. Configuration of these endpoints is not covered in these Application Notes as they followed standard practice. However, the one setting that is enabled on each endpoint isto assign the**Survivability Server** defined in Step 1 above.This is done by editing each User and navigating to the **Communication Profile** tab.



* Primary Session Manager: SM_21_31

Primary	Secondary	Maximum
33	0	33

Secondary Session Manager: (None)

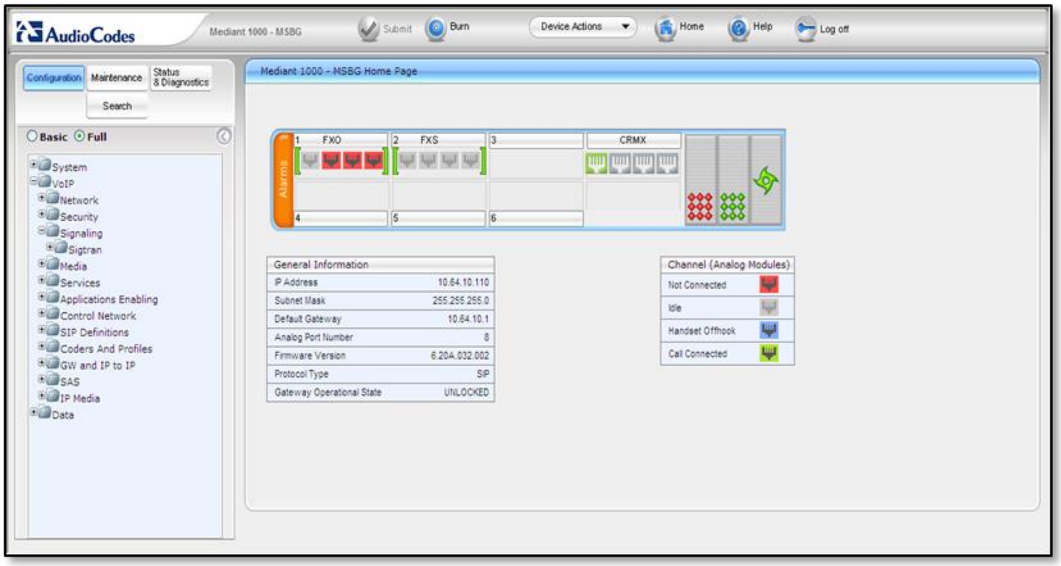
Primary	Secondary	Maximum

Origination Application Sequence: CM_FS_TestRoom1
Termination Application Sequence: CM_FS_TestRoom1
Survivability Server: AudioCodes M1000 supports 3 Communication Profile(s).
* Home Location: TestRoom1

7. AudioCodes MSBG Configuration

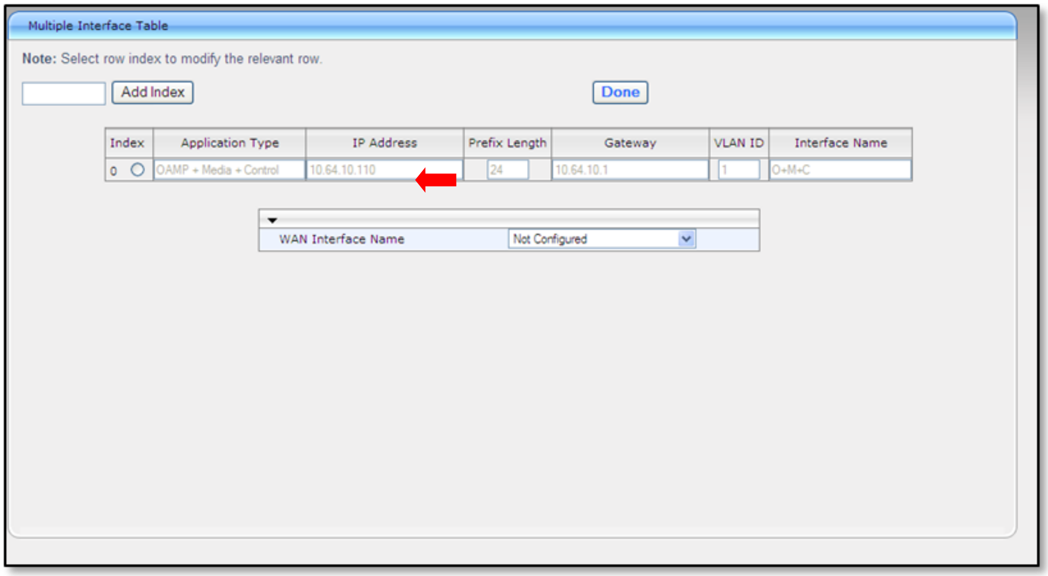
This section describes the procedures for configuring the Mediant 1000 MSBG, the Mediant 800 is administered identically using settings appropriate for the alternate location. These procedures assume the MSBG has been installed using the procedures documented in the AudioCodes Installation Manual and has been assigned an IP address for network connectivity.

Step	Description
1.	**Login to the MSBG** The configuration of the Mediant 1000 and Mediant 800 MSBG is done via a Web browser. To access the device, enter the **IP address** of the MSBG in the **Address** field of the web browser. The IP address was entered during **Installation.**  Address http://192.168.1.60/
2.	**Login credentials** The following pop-up window will appear. **Login** with the proper credentials.  This secure Web Site (at 192.168.1.60) requires you to log on. Please type the User Name and Password that you use for Realm1. User Name Password ☐ Save this password in your password list

Step	Description
3.	**MSBG Main Page at Login** The MSBG main page will appear as shown below.  Mediant 1000 - MSBG Home Page General Information IP Address 10.64.10.110 Subnet Mask 255.255.255.0 Default Gateway 10.64.10.1 Analog Port Number 8 Firmware Version 6.20A.032.002 Protocol Type SIP Gateway Operational State UNLOCKED Channel (Analog Modules) Not Connected 🟥 Idle ▨ Handset Offhook 🟦 Call Connected 🟩
4.	**Saving the MSBG Configuration** It is recommended to periodically save the configuration as the following steps of this configuration guide are completed. Return to the home web page and select **Maintenance** in the left pane. Under **Maintenance Actions c**lick the **BURN** button.  Maintenance Actions Reset Configuration Reset Board [Reset] Burn To FLASH Yes Graceful Option No LOCK / UNLOCK Lock [LOCK] Graceful Option No Gateway Operational State UNLOCKED Save Configuration Burn To FLASH [BURN] **For Reset Board :** If you choose not to save the device's configuration to flash memory, all changes made since the last time the configuration was saved will be lost after the device is reset. **For Save Configuration:** Saving configuration to flash memory may cause some temporary degradation in voice quality, therefore, it is recommended to perform this during low-traffic periods

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

View Network Settings
The network settings that were configured during installation can be viewed by selecting **Configuration** in the left pane then navigating to **VoIP>Network>IP Settings**for the **Multiple Interface Table** in the right pane. If necessary, changes can be made to the settings on this page followed by clicking **Submit**. For the compliance test, the **IP Address**, **Subnet Mask** and **Default Gateway Address** were set to values consistent with the test configuration shown in **Figure 1**.

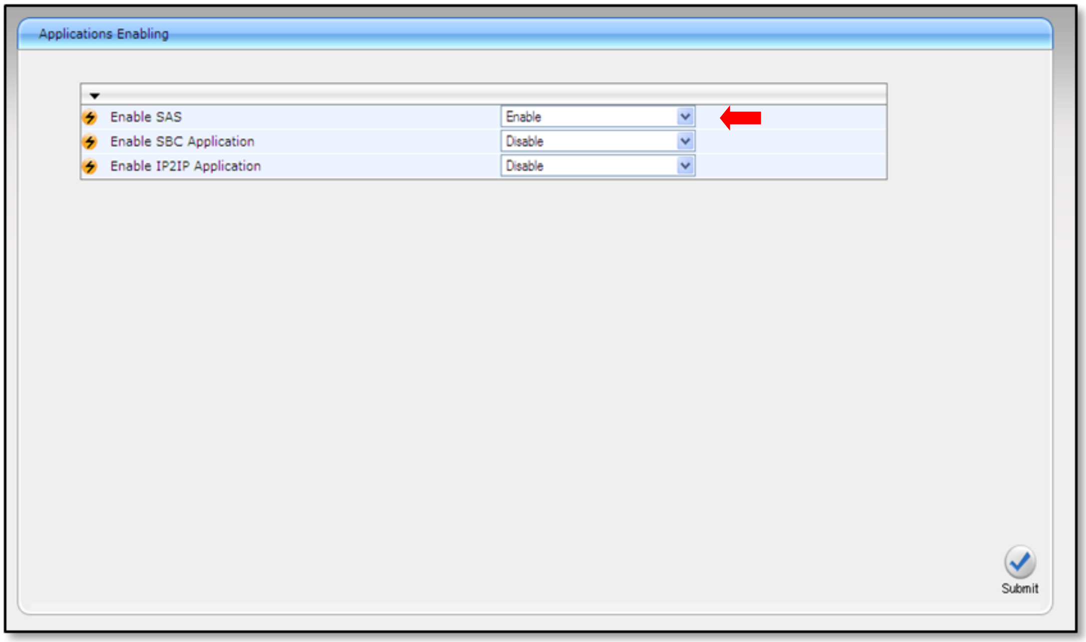
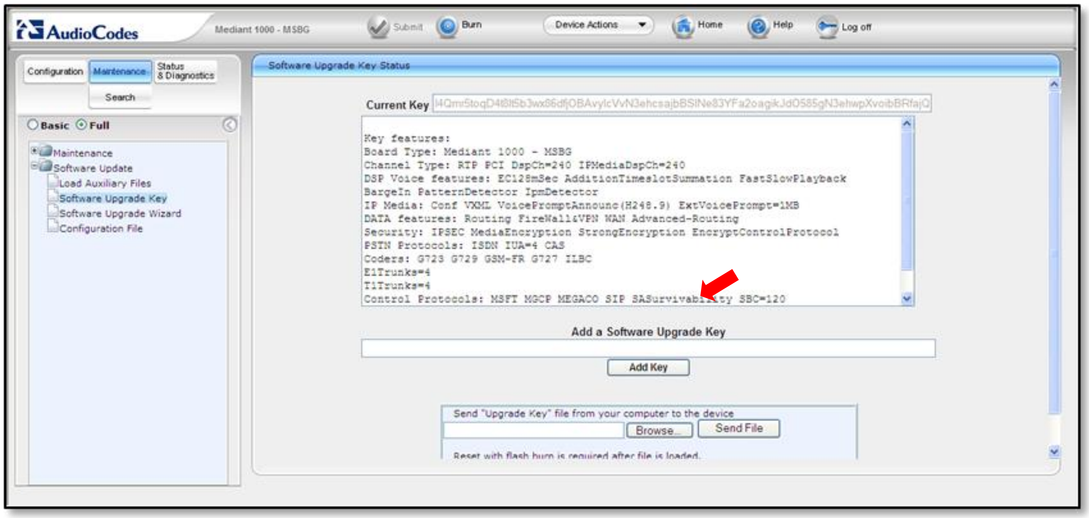


Note: Select row index to modify the relevant row.

<table>
<tr><th>Index</th><th>Application Type</th><th>IP Address</th><th>Prefix Length</th><th>Gateway</th><th>VLAN ID</th><th>Interface Name</th></tr>
<tr><td>0 ○</td><td>OAMP + Media + Control</td><td>10.64.10.110</td><td>24</td><td>10.64.10.1</td><td>1</td><td>O+M+C</td></tr>
</table>

WAN Interface Name: Not Configured

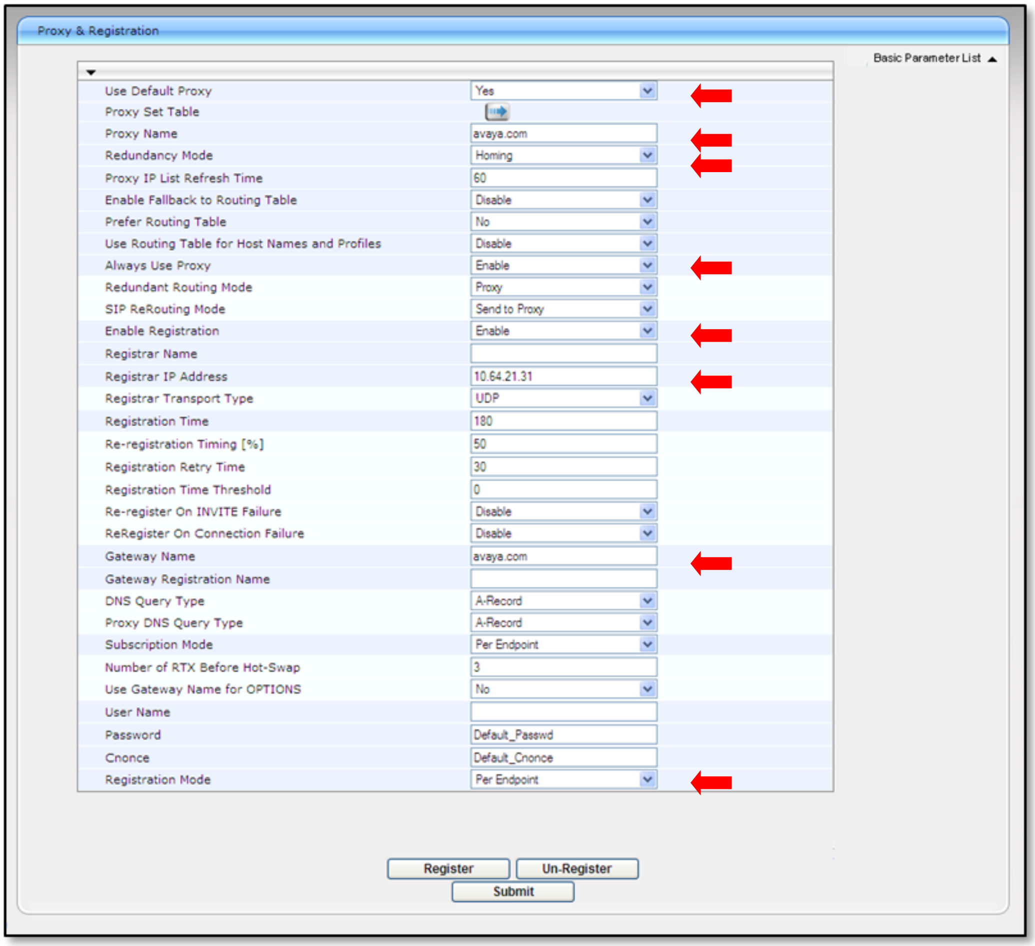
</td></tr>
</table>

Step	Description
6.	**Set Application Enabling for Stand Alone Survivability(SAS)** To access these parameters, select **VoIP>Applications Enabling** in the left pane. The pull-down choices for Applications Enabling are shown below. Note the *yellow-bolt icon* indicator requires that a “***device reset***” be performed. This alters the content of the configuration screens from this point forward.  Applications Enabling Enable SAS: Enable Enable SBC Application: Disable Enable IP2IP Application: Disable
7.	**Feature and License Key** To access the Feature Key information, go to the main **HOME** page of the MSBG GUI. Select **MAINTENANCE** menu drop-down. Then **Software Update** in the left pane and drop-down to **Software Update Key**. The features licensed and supported on the MSBG for Compliance testing aredisplayed below:  Current Key: I4QmiStoqD4t8It5b3wx86dfjOBAvylcVvN3ehcsajbBSINe83YFa2oagikJd0585gN3ehwpXvoibBRfajQ

```
Key features:
Board Type: Mediant 1000 - MSBG
Channel Type: RTP PCI DspCh=240 IPMediaDspCh=240
DSP Voice features: EC128mSec AdditionTimeslotSummation FastSlowPlayback
BargeIn PatternDetector IpmDetector
IP Media: Conf VXML VoicePromptAnnounc(H248.9) ExtVoicePrompt=1MB
DATA features: Routing FireWall&VPN WAN Advanced-Routing
Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
PSTN Protocols: ISDN IUA=4 CAS
Coders: G723 G729 GSM-FR G727 ILBC
E1Trunks=4
T1Trunks=4
Control Protocols: MSFT MGCP MEGACO SIP SASurvivability SBC=120
```

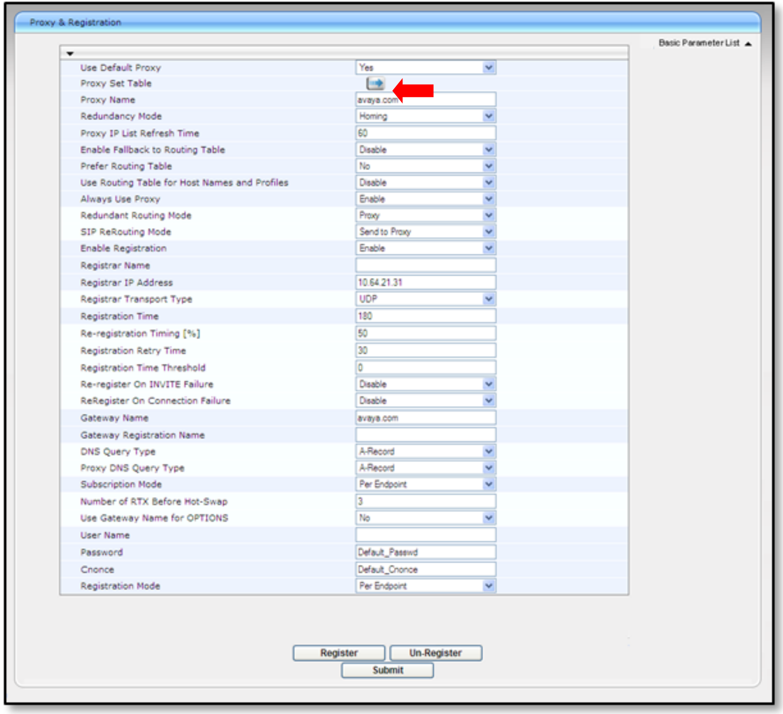
Step	Description
8.	**SIP General Parameters** To access these parameters, select **General Parameters** in the left pane and navigate to **SIP Definitions** in the right pane. From the menu shown in **Step 3** (Main Login Page), navigate to **SIP General Parameters**. Configure the parameters as described below. ▪ For the **Enable Early Media** field, select ***Enable***. If enabled, the MSBG sends Session Description Protocol (SDP) information in the 18x responses allowing the media stream to be set-up prior to answering the call. ▪ Select ***UDP*** for the **SIP Transport Type** field; Enter port ***5060*** for the **SIP UDP Local Port** ▪ Select ***No*** for the **Use user=phone in SIP URL** field. Default values may be retained for all other fields. Scroll down to the bottom of the page and click **Submit** (not shown). 

SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Disable
Channel Select Mode	By Dest Phone Number
Enable Early Media	Enable
183 Message Behavior	Alert
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
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060
Use user=phone in SIP URL	No
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	Play Local Until Remote Media A
Use Tgrp information	Disable
Enable GRUU	Disable
User-Agent Information	
SDP Session Owner	AudiocodesGW
Subject	
Multiple Packetization Time Format	None
Enable Semi-Attended Transfer	Disable
3xx Behavior	Forward
Enable P-Charging Vector	Disable
Enable VoiceMail URI	Disable
Retry-After Time	0
Enable P-Associated-URI Header	Disable
Source Number Preference	
Forking Handling Mode	Parallel handling
Enable Comfort Tone	Disable
Add Trunk Group ID as Prefix to Source	No
Fake Retry After	0
Enable Reason Header	Enable
Retransmission Parameters	
SIP T1 Retransmission Timer [msec]	500
SIP T2 Retransmission Timer [msec]	4000
SIP Maximum RTX	7

Step	Description
9.	**Proxy and Registration** From the menu shown in Step 3, navigate to **SIP Definition>Proxy & Registration**. Configure the parameters as described below. ▪ For the **Use Default Proxy** field, select ***Yes*** from the pull-down menu. ▪ Enter "***avaya.com***" for the **Proxy Name** ▪ Set **Redundancy Mode** to ***Homing*** ▪ For the **Always Use Proxy** field, select ***Enable***. ▪ For the **Enable Registration** field, select ***Enable***. This will allow the MSBG to register the FXS endpoints with the Avaya SM. ▪ In the **Registrar IP Address** field, enter the IP address of the Avaya SM. ▪ In the **Gateway Name** field, enter the domain of the Avaya SM ▪ **Registration Mode** is set to ***Per Endpoint*** Click **Submit**. *Note: Homing provides the ability to revert registrations back to AVAYA SM when connection is re-established.* Default values may be retained for all other fields. Scroll down to continue configuring parameters on the lower half of the screen. 

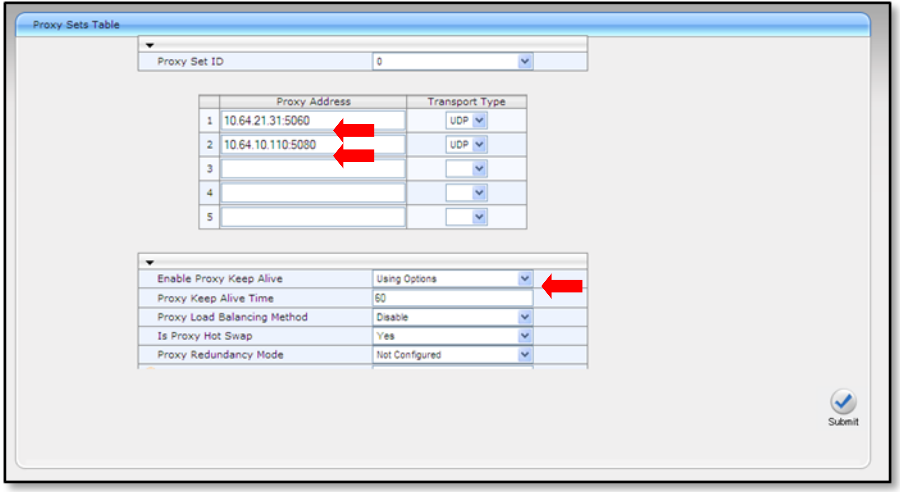
Use Default Proxy	Yes
Proxy Set Table	
Proxy Name	avaya.com
Redundancy Mode	Homing
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Enable
Redundant Routing Mode	Proxy
SIP ReRouting Mode	Send to Proxy
Enable Registration	Enable
Registrar Name	
Registrar IP Address	10.64.21.31
Registrar Transport Type	UDP
Registration Time	180
Re-registration Timing [%]	50
Registration Retry Time	30
Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	avaya.com
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Subscription Mode	Per Endpoint
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Passwd
Cnonce	Default_Cnonce
Registration Mode	Per Endpoint

Step	Description
10.	**PROXY SET TABLE** From the menu shown in **Step 3**, navigate to**SIP Definitions>Proxy & Registration.** Click on **"PROXY SET TABLE".** See the drop down menu below.



Use Default Proxy	Yes
Proxy Set Table	
Proxy Name	avaya.com
Redundancy Mode	Homing
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Enable
Redundant Routing Mode	Proxy
SIP ReRouting Mode	Send to Proxy
Enable Registration	Enable
Registrar Name	
Registrar IP Address	10.64.21.31
Registrar Transport Type	UDP
Registration Time	180
Re-registration Timing [%]	50
Registration Retry Time	30
Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	avaya.com
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Subscription Mode	Per Endpoint
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Passwd
Cnonce	Default_Cnonce
Registration Mode	Per Endpoint

Enter the **Proxy Address** for the Session Manager in Line 1 specifying ***Port 5060***. Set address transport to ***UDP***. Enter the **Proxy Address** for the MSBG SAS specifying ***Port 5080.*** Set address transport to UDP. For the **Enable Proxy Keep Alive** Select ***Using Options*** from the pull-down menu. See Notes below:



Proxy Set ID	0

	Proxy Address	Transport Type
1	10.64.21.31:5060	UDP
2	10.64.10.110:5080	UDP
3		
4		
5		

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	Yes
Proxy Redundancy Mode	Not Configured

Note: The Proxy Set table prioritizes calls based upon availability. The first line is the Proxy that calls use. The second line is the Proxy that is used if the first is not available. With SAS, the first PROXY is not available so the second proxy is the primary address. This is the SAS gateway IP Address and 5080 is the port that is typically assigned. The SAS Gateway provides routing (Hunt Group) to a FXO port for outbound calls.

Note: The MSBG will use the SIP OPTIONS message as a handshake mechanism with the Avaya SM to determine if the SIP connection is up. If the connection is down, the MSBG will failover to the SAS application which will in turn utilize the FXO ports.

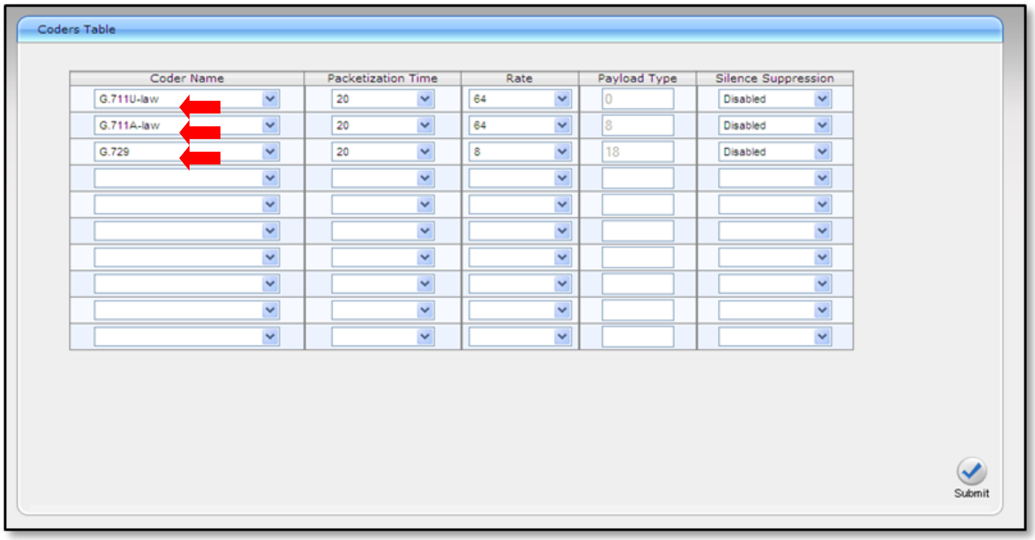
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>11.</td><td>

CODECS

From the menu shown in Step 3, navigate to **VoIP>Coders And Profiles**. In the screen below, select the list of preferred codecs to be used by the MSBG with the most preferred codec at the top and working downward to the least preferred. This list must have an overlap with the list provided on Avaya Communication Manager. The codec is selected from the pull-down menu under the **Coder Name** field.

The codec list used for the compliance test is shown in the example below. ***G.711U-law*** was selected as the most preferred followed by ***G.711A-law*** and followed by ***G.729*** as the next-preferable codec.

Click **Submit**.



Coders Table

<table>
<tr><th>Coder Name</th><th>Packetization Time</th><th>Rate</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>G.711U-law</td><td>20</td><td>64</td><td>0</td><td>Disabled</td></tr>
<tr><td>G.711A-law</td><td>20</td><td>64</td><td>8</td><td>Disabled</td></tr>
<tr><td>G.729</td><td>20</td><td>8</td><td>18</td><td>Disabled</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

</td></tr>
</table>

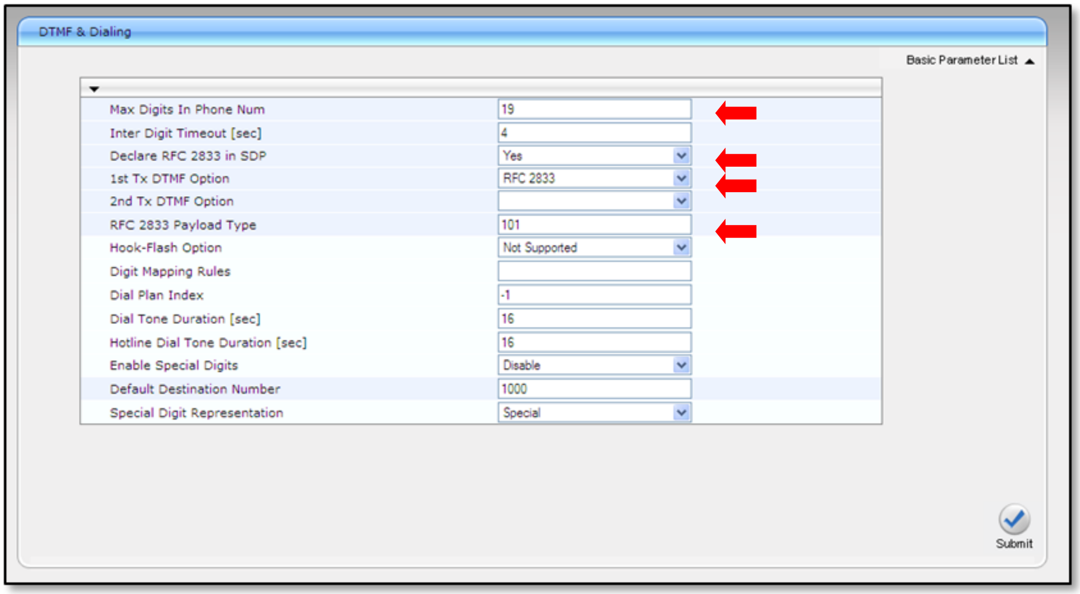
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>12.</td><td>

DTMF and Dialing

From the menu shown in **Step 3**, navigate to **SIP Definition>DTMF & Dialing**. Configure the parameters as described below.

- In the **Max Digits in Phone Num** field, enter the maximum number of digits that can be dialed.
- For the **Declare RFC 2833 in SDP** field, select ***Yes***.
- For the **1stTx DTMF Option** field, select ***RFC 2833***. This selects RFC 2833 as the preferred DTMF transmission method.
- Select ***101*** as the **RFC 2833 Payload Type** to match the value used by the Avaya SIP Telephones. Media may not be redirected (shuffled) in all scenarios from Avaya Communication Manager to the endpoints if this value is not the same as the SIP Telephones.

Default values may be retained for all other fields. Click **Submit**.

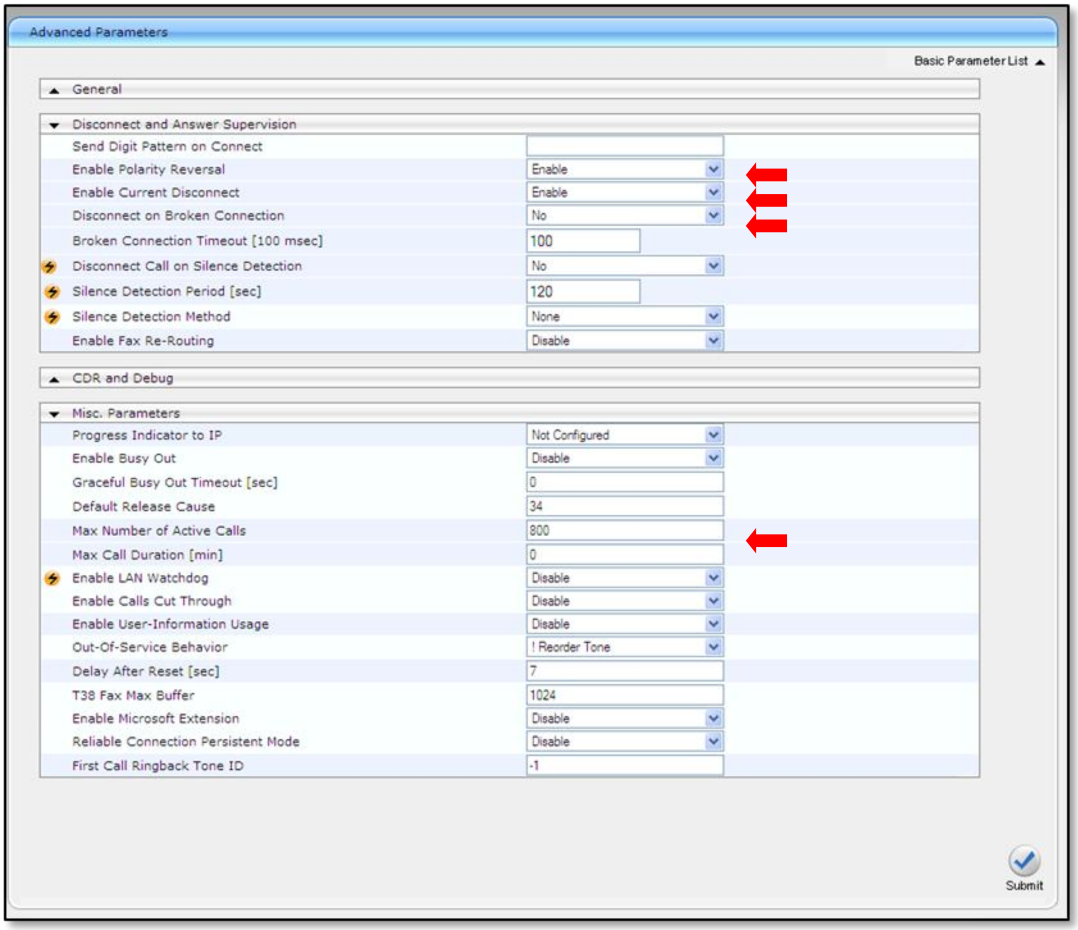


<table>
<tr><th></th><th></th></tr>
<tr><td>Max Digits In Phone Num</td><td>19</td></tr>
<tr><td>Inter Digit Timeout [sec]</td><td>4</td></tr>
<tr><td>Declare RFC 2833 in SDP</td><td>Yes</td></tr>
<tr><td>1st Tx DTMF Option</td><td>RFC 2833</td></tr>
<tr><td>2nd Tx DTMF Option</td><td></td></tr>
<tr><td>RFC 2833 Payload Type</td><td>101</td></tr>
<tr><td>Hook-Flash Option</td><td>Not Supported</td></tr>
<tr><td>Digit Mapping Rules</td><td></td></tr>
<tr><td>Dial Plan Index</td><td>-1</td></tr>
<tr><td>Dial Tone Duration [sec]</td><td>16</td></tr>
<tr><td>Hotline Dial Tone Duration [sec]</td><td>16</td></tr>
<tr><td>Enable Special Digits</td><td>Disable</td></tr>
<tr><td>Default Destination Number</td><td>1000</td></tr>
<tr><td>Special Digit Representation</td><td>Special</td></tr>
</table>

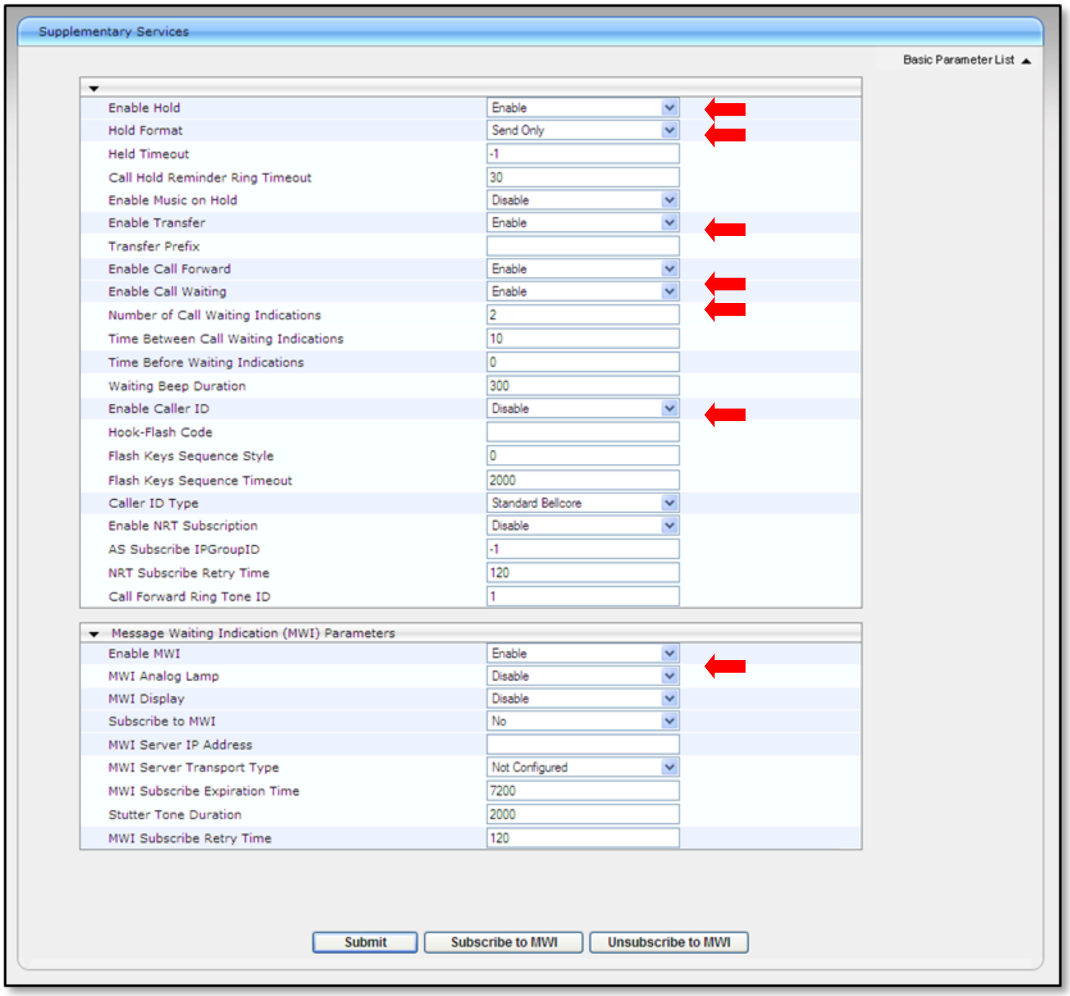
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>13.</td><td>
Advanced Parameters
From the menu shown in **Step 3**, navigate to select **SIP Definition** in the left pane and navigate to Advanced Parameters in the right pane. The pull-down choices for Advanced Parameters are shown below**.**

- Select***Enable***for the **Enable Polarity Reversal** and **Enable Current Disconnect** fields. This will allow the MSBG to provide the proper disconnect indication to various line types.
- **Disconnect on Broken Connection** fieldis set to ***No*.**
- In the **Max Number of Active Calls** field, enter a value that is equal to or greater than the maximum number of ports (FXS + FXO) available on the gateway. For the compliance test, there were 4 FXS ports and 4 FXO ports.

Default values may be retained for all other fields. Click **Submit**.


<table>
<tr><th colspan="2">Disconnect and Answer Supervision</th></tr>
<tr><td>Send Digit Pattern on Connect</td><td></td></tr>
<tr><td>Enable Polarity Reversal</td><td>Enable</td></tr>
<tr><td>Enable Current Disconnect</td><td>Enable</td></tr>
<tr><td>Disconnect on Broken Connection</td><td>No</td></tr>
<tr><td>Broken Connection Timeout [100 msec]</td><td>100</td></tr>
<tr><td>Disconnect Call on Silence Detection</td><td>No</td></tr>
<tr><td>Silence Detection Period [sec]</td><td>120</td></tr>
<tr><td>Silence Detection Method</td><td>None</td></tr>
<tr><td>Enable Fax Re-Routing</td><td>Disable</td></tr>
<tr><th colspan="2">Misc. Parameters</th></tr>
<tr><td>Progress Indicator to IP</td><td>Not Configured</td></tr>
<tr><td>Enable Busy Out</td><td>Disable</td></tr>
<tr><td>Graceful Busy Out Timeout [sec]</td><td>0</td></tr>
<tr><td>Default Release Cause</td><td>34</td></tr>
<tr><td>Max Number of Active Calls</td><td>800</td></tr>
<tr><td>Max Call Duration [min]</td><td>0</td></tr>
<tr><td>Enable LAN Watchdog</td><td>Disable</td></tr>
<tr><td>Enable Calls Cut Through</td><td>Disable</td></tr>
<tr><td>Enable User-Information Usage</td><td>Disable</td></tr>
<tr><td>Out-Of-Service Behavior</td><td>! Reorder Tone</td></tr>
<tr><td>Delay After Reset [sec]</td><td>7</td></tr>
<tr><td>T38 Fax Max Buffer</td><td>1024</td></tr>
<tr><td>Enable Microsoft Extension</td><td>Disable</td></tr>
<tr><td>Reliable Connection Persistent Mode</td><td>Disable</td></tr>
<tr><td>First Call Ringback Tone ID</td><td>-1</td></tr>
</table>
</td></tr>
</table>

Step	Description
14.	**Supplementary Services** From the menu shown in **Step 3**, navigate to **DTMF and SupplementarySupplementary Services**. Configure the parameters as described below. ■ If the analog phones connected to the MSBG support Caller ID then set the **Enable Caller ID** field to ***Enable***. For the compliance test, this field was set to ***Disable*** since none of the analog phones used had a Caller ID display. ■ **Hold Format** field is set to **Send Only.** ■ Select ***Enabled*** for the **Enable MWI** field if the analog phones support a visual MWI indicator. For the compliance test, even though these fields were enabled, MWI was only tested for stutter dial tone. ■ Hold, Transfer, Call Forwarding and Call Waiting are enabled by default. Default values may be retained for all other fields. Scroll down to the bottom of the page and click **Submit** (not shown).  Enable Hold: Enable Hold Format: Send Only Held Timeout: -1 Call Hold Reminder Ring Timeout: 30 Enable Music on Hold: Disable Enable Transfer: Enable Transfer Prefix: Enable Call Forward: Enable Enable Call Waiting: Enable Number of Call Waiting Indications: 2 Time Between Call Waiting Indications: 10 Time Before Waiting Indications: 0 Waiting Beep Duration: 300 Enable Caller ID: Disable Hook-Flash Code: Flash Keys Sequence Style: 0 Flash Keys Sequence Timeout: 2000 Caller ID Type: Standard Bellcore Enable NRT Subscription: Disable AS Subscribe IPGroupID: -1 NRT Subscribe Retry Time: 120 Call Forward Ring Tone ID: 1 Message Waiting Indication (MWI) Parameters Enable MWI: Enable MWI Analog Lamp: Disable MWI Display: Disable Subscribe to MWI: No MWI Server IP Address: MWI Server Transport Type: Not Configured MWI Subscribe Expiration Time: 7200 Stutter Tone Duration: 2000 MWI Subscribe Retry Time: 120
15.	**Manipulation Tables**. Digit Manipulation was not included during testing but can be added and configured per the applicable AudioCodes User's Manual available on the Audiocodes website.

Step	Description
16.	**Routing Tables**

From the menu shown in **Step 3**, navigate to **Routing** in the left pane and navigate to **IP to Trunk Group Routing** in the right pane. The pull-down choices for the **Routing Tables** are shown below.

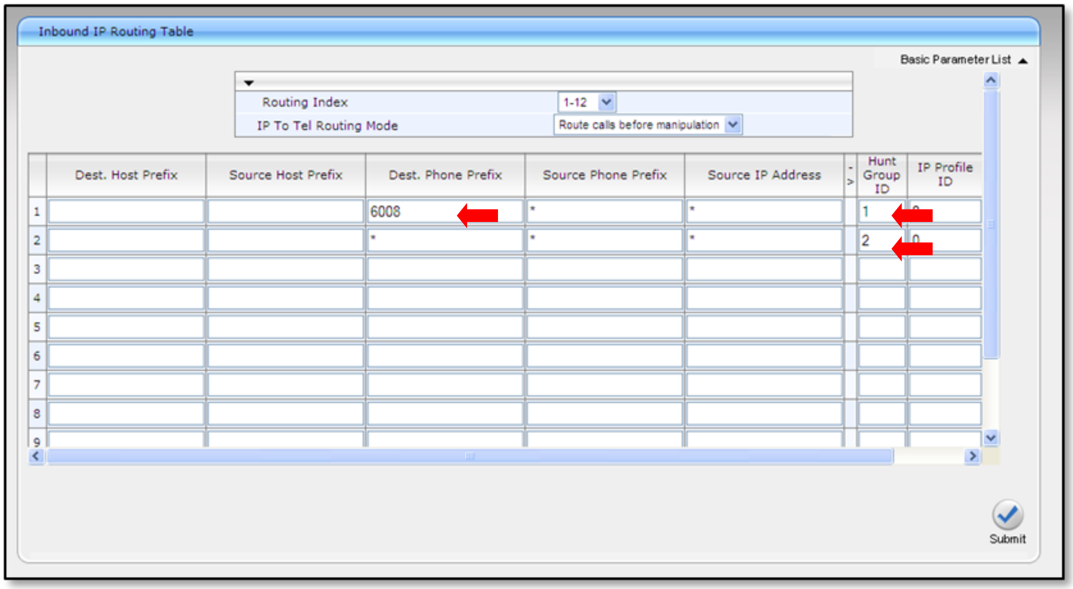
This table defines the mapping of IP calls to a group of channels or "hunt group". In **Step 18**, the **FXS ports** are assigned to **hunt group 1** and the **FXO ports** are assigned to **hunt group 2**.

*NOTE: **Trunk Group** and **Hunt Group** are interchangeable terminology**.** A **Hunt Group** refers to analog functionality. A **Trunk Group** is a more generic terminology and is also applicable to digital trunks.*

The **Dest. Phone Prefix**, **Source Phone Prefix** and **Source IP Address** columns define which calls are mapped to the hunt group in the **Hunt Group ID** column. In the first entry in the example below, all calls to **extension 6008** from any source extension and source IP will be routed to **hunt group 1**. Thus, the dialed number must be an exact match.

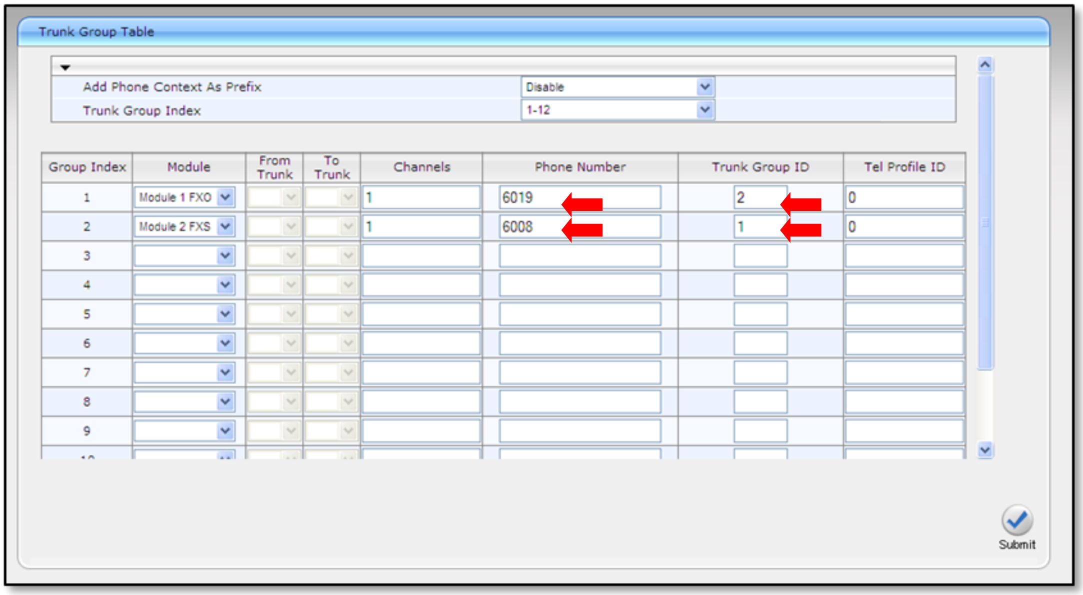
The second entry routes any other call to **hunt group 2**. Even though Avaya Communication Manager will not route any other calls to the MSBG except calls to **extension6008**, this entry is needed for the failover case. If a user dials an outbound number and it cannot reach the main site, this table will direct the call to **hunt group 2** which contains the FXO ports for access to the PSTN.

Click **Submit**.



Routing Index: 1-12
IP To Tel Routing Mode: Route calls before manipulation

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Hunt Group ID	IP Profile ID
1			6008	*	*		1	0
2			*	*	*		2	0
3								
4								
5								
6								
7								
8								
9								

Step	Description
17.	**Endpoint Phone Numbers** From the menu shown in **Step 3**, navigate to **Hunt Group** in the left pane and navigate to **Hunt Group** in the right pane. The Hunt Group maps a particular channel/port to a phone number and hunt group. In the **Channels** column, enter a range of channels to be assigned. In the **Phone Number** column, enter the starting extension for the range of extensions. In the **Trunk Group ID** column, enter the hunt group that contains these extensions. In the example below, the first entry assigns **FXO** channel ***1*** (the first FXO port) with extension ***6019*** to Trunk Group ID ***2***. The second entry assigns **FXS** channel ***1*** (the first FXS port) with extension **6008** to Trunk Group ID ***1***. Since only the first FXO port was connected to the PSTN, only channel 1 was enter in this table. Click **Submit**. 

Trunk Group Table

Add Phone Context As Prefix: Disable

Trunk Group Index: 1-12

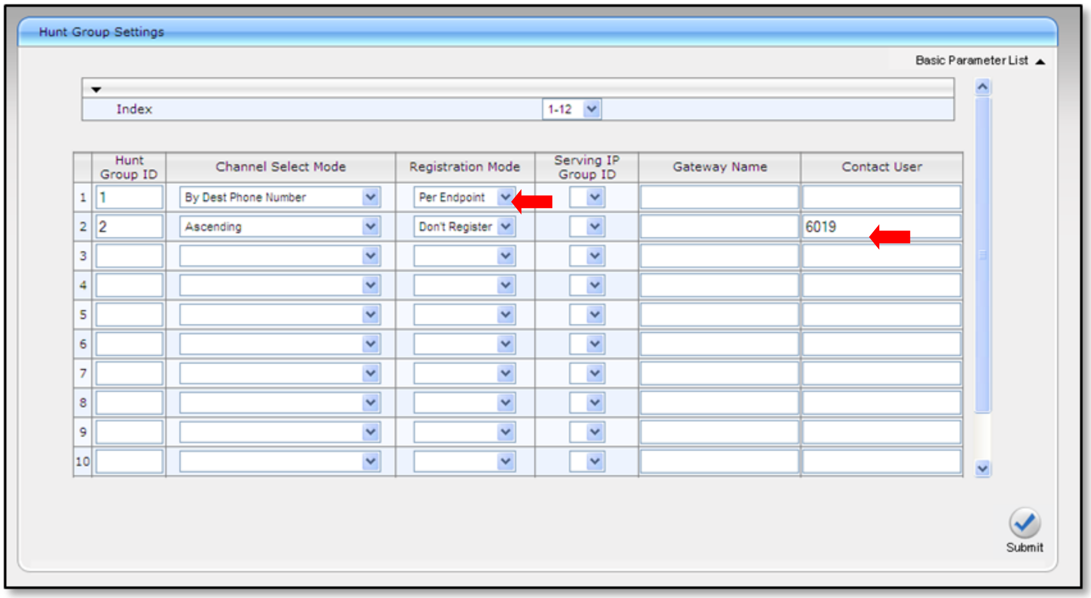
Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 FXO			1	6019	2	0
2	Module 2 FXS			1	6008	1	0
3							
4							
5							
6							
7							
8							
9							

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>18.</td><td>
Hunt Group Settings
From the menu shown in Step 3, navigate to Hunt Group in the left pane and navigate to Hunt Group Settings in the right pane.

Configure the parameters described below.

For Hunt Group ID1 which contain the FXS (endpoint) ports, select the Channel Select Mode as <i>By Dest Phone Number</i>. Thus, each port in this hunt group will only be selected if its destination phone number is dialed. Select the Registration Mode to be <i>Per Endpoint.</i>
For Hunt Group ID2 which contain the FXO (POTS) ports, select the Channel Select Mode as <i>Ascending</i>. The ports in this hunt group are treated as a pool, and each will be selected in ascending order. Select the Registration Mode to be <i>Don't Register</i>. Set the Contact User as 6019 for Caller ID.
This allows the MSBG to register per endpoint for all the FXS ports using the gateway extension entered in Step 17.The MSBG requires that only the FXS ports be registered since registration was enabled in Step 9.

Click Submit.



Index: 1-12
<table>
<tr><th></th><th>Hunt Group ID</th><th>Channel Select Mode</th><th>Registration Mode</th><th>Serving IP Group ID</th><th>Gateway Name</th><th>Contact User</th></tr>
<tr><td>1</td><td>1</td><td>By Dest Phone Number</td><td>Per Endpoint</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>2</td><td>Ascending</td><td>Don't Register</td><td></td><td></td><td>6019</td></tr>
<tr><td>3</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>7</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>8</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>9</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>10</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>19.</td><td>
Analog Gateway Settings
From the menu shown in Step 3, navigate to Analog Gateway in the left pane and navigate to the submenu below in the right pane.

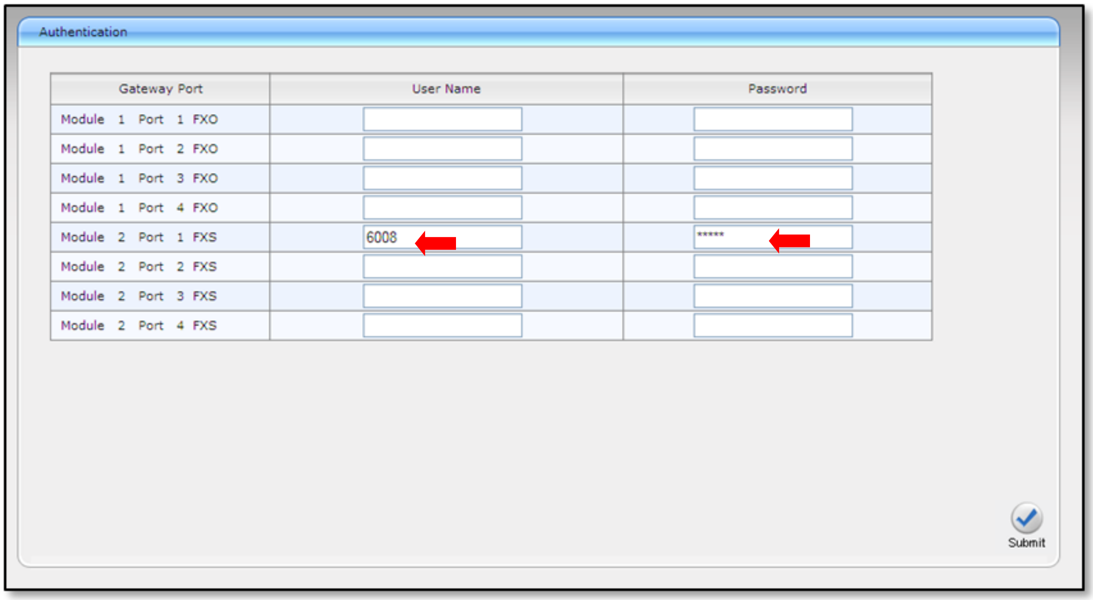
Continue with the following steps:
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>20.</td><td>

Authentication

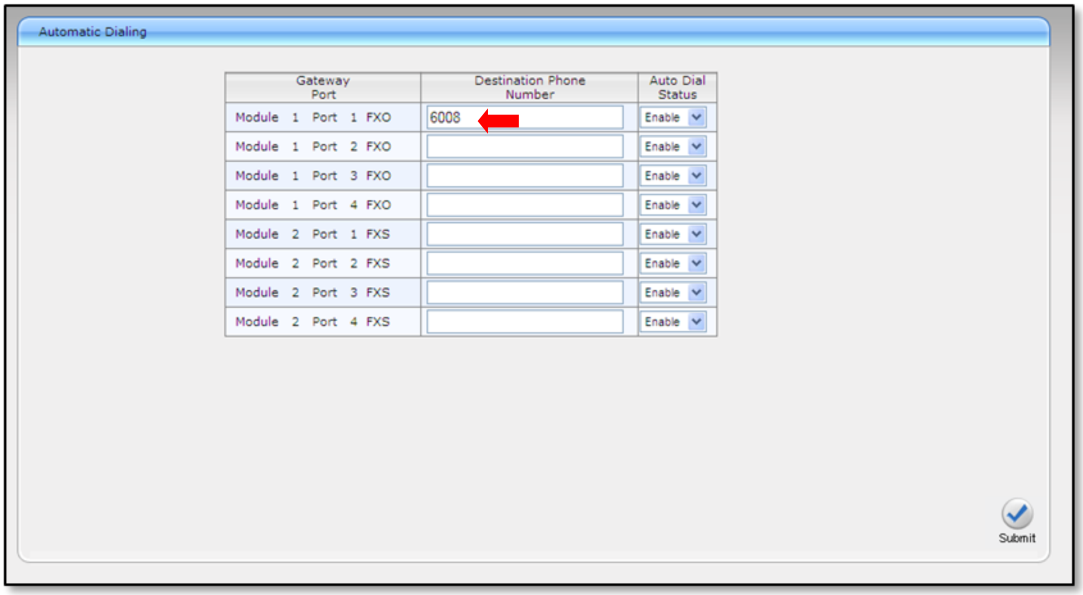
From the menu shown in **Step 3**, navigate to **Analog Gateway>Authentication**.

The Authentication page defines a username and password combination for authentication of each MSBG port with the Avaya Session Manager. Enter a **User Name** and **Password**for a valid user account.
Click **Submit**.



<table>
<tr><th>Gateway Port</th><th>User Name</th><th>Password</th></tr>
<tr><td>Module 1 Port 1 FXO</td><td></td><td></td></tr>
<tr><td>Module 1 Port 2 FXO</td><td></td><td></td></tr>
<tr><td>Module 1 Port 3 FXO</td><td></td><td></td></tr>
<tr><td>Module 1 Port 4 FXO</td><td></td><td></td></tr>
<tr><td>Module 2 Port 1 FXS</td><td>6008</td><td>*****</td></tr>
<tr><td>Module 2 Port 2 FXS</td><td></td><td></td></tr>
<tr><td>Module 2 Port 3 FXS</td><td></td><td></td></tr>
<tr><td>Module 2 Port 4 FXS</td><td></td><td></td></tr>
</table>

</td></tr>
</table>

Step	Description
21.	**Automatic Dialing** From the menu shown in **Step 3**, navigate to **Analog Gateway>Automatic Dialing**. The Automatic Dialing page provides the mapping of incoming calls on the FXO ports to a branch extension when the data WAN is unavailable. In the example below, each FXO port is mapped to a different extension at the branch location. All ports were mapped even though only one FXO port was connected. The destination extension is placed in the **Destination Phone Number** column. Click **Submit**. 

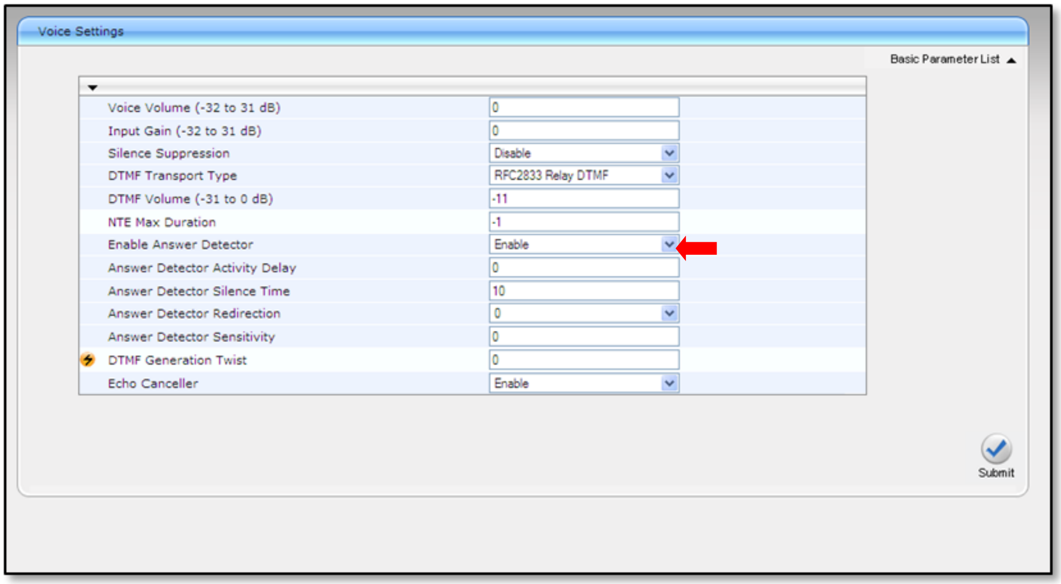
Gateway Port	Destination Phone Number	Auto Dial Status
Module 1 Port 1 FXO	6008	Enable
Module 1 Port 2 FXO		Enable
Module 1 Port 3 FXO		Enable
Module 1 Port 4 FXO		Enable
Module 2 Port 1 FXS		Enable
Module 2 Port 2 FXS		Enable
Module 2 Port 3 FXS		Enable
Module 2 Port 4 FXS		Enable

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>22.</td><td>

FXO Voice Settings

From the menu shown in **Step 3**, navigate to **Analog gateway** in the left pane and navigate to **Voice Settings** in the right pane. The pull-down choices for **Voice Settings** are shown below. **Answer Detector** is set to ***Enable***.

Note: This can be used if Polarity Reversal is <u>not</u>provided by the PSTN for answer detection.



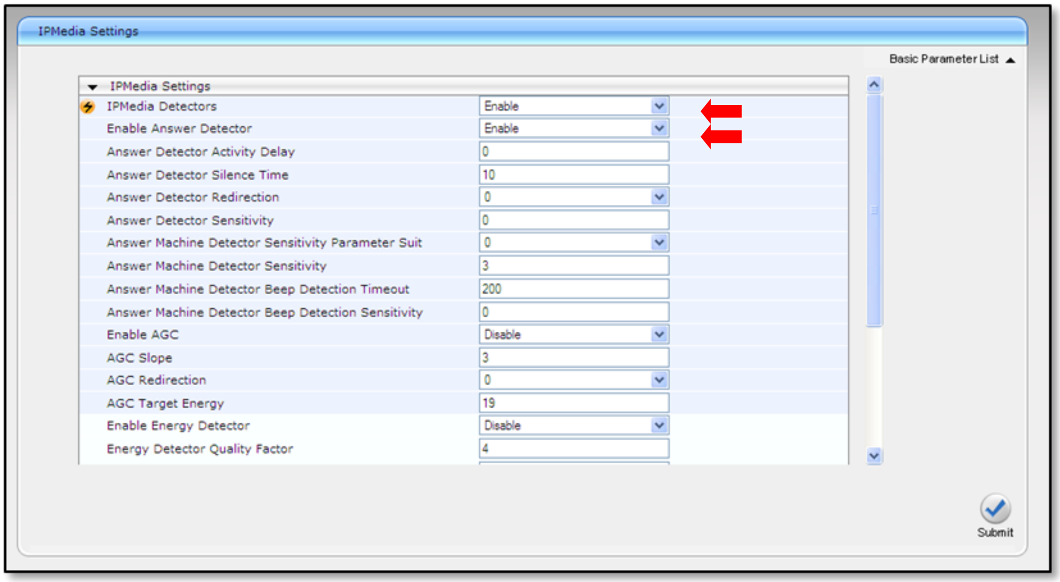
<table>
<tr><td>Voice Volume (-32 to 31 dB)</td><td>0</td></tr>
<tr><td>Input Gain (-32 to 31 dB)</td><td>0</td></tr>
<tr><td>Silence Suppression</td><td>Disable</td></tr>
<tr><td>DTMF Transport Type</td><td>RFC2833 Relay DTMF</td></tr>
<tr><td>DTMF Volume (-31 to 0 dB)</td><td>-11</td></tr>
<tr><td>NTE Max Duration</td><td>-1</td></tr>
<tr><td>Enable Answer Detector</td><td>Enable</td></tr>
<tr><td>Answer Detector Activity Delay</td><td>0</td></tr>
<tr><td>Answer Detector Silence Time</td><td>10</td></tr>
<tr><td>Answer Detector Redirection</td><td>0</td></tr>
<tr><td>Answer Detector Sensitivity</td><td>0</td></tr>
<tr><td>DTMF Generation Twist</td><td>0</td></tr>
<tr><td>Echo Canceller</td><td>Enable</td></tr>
</table>

</td></tr>
<tr><td>23.</td><td>

IP Media Settings for FXO

From the menu shown in **Step 3**, navigate to **IP Media>IP Media Settings**. Enable the parameters as illustrated below.

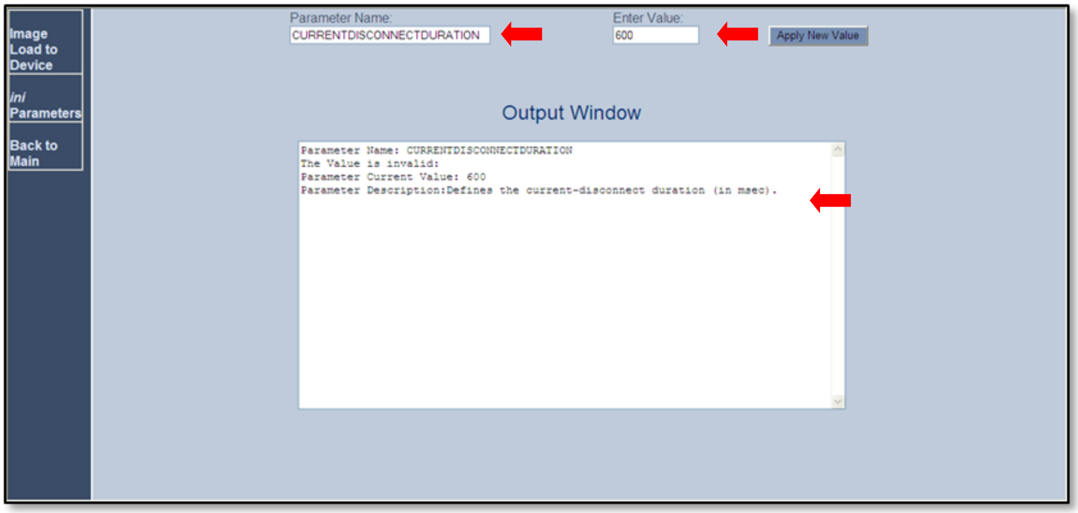
Default values may be retained for all other fields. Click **Submit**.



<table>
<tr><td>IPMedia Detectors</td><td>Enable</td></tr>
<tr><td>Enable Answer Detector</td><td>Enable</td></tr>
<tr><td>Answer Detector Activity Delay</td><td>0</td></tr>
<tr><td>Answer Detector Silence Time</td><td>10</td></tr>
<tr><td>Answer Detector Redirection</td><td>0</td></tr>
<tr><td>Answer Detector Sensitivity</td><td>0</td></tr>
<tr><td>Answer Machine Detector Sensitivity Parameter Suit</td><td>0</td></tr>
<tr><td>Answer Machine Detector Sensitivity</td><td>3</td></tr>
<tr><td>Answer Machine Detector Beep Detection Timeout</td><td>200</td></tr>
<tr><td>Answer Machine Detector Beep Detection Sensitivity</td><td>0</td></tr>
<tr><td>Enable AGC</td><td>Disable</td></tr>
<tr><td>AGC Slope</td><td>3</td></tr>
<tr><td>AGC Redirection</td><td>0</td></tr>
<tr><td>AGC Target Energy</td><td>19</td></tr>
<tr><td>Enable Energy Detector</td><td>Disable</td></tr>
<tr><td>Energy Detector Quality Factor</td><td>4</td></tr>
</table>

</td></tr>
</table>

Step	Description
24.	**Fax/Modem/CID Settings** Fax was not included in testing but can be added and configured per the applicable AudioCodes User's Manual available on the AudioCodes website.

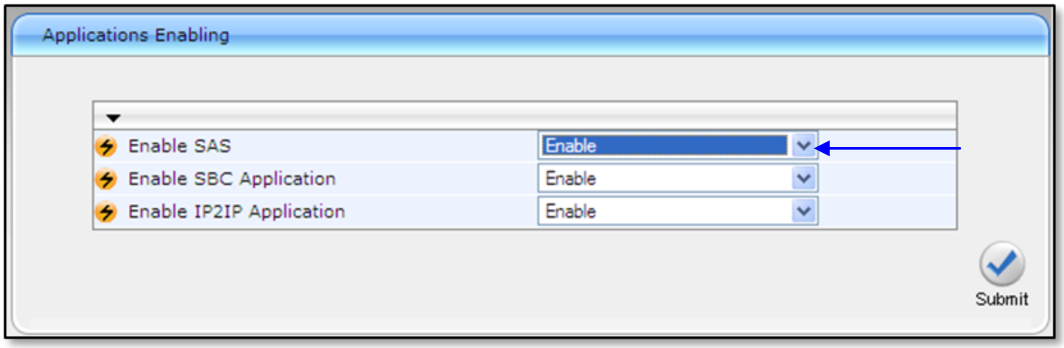
25.	**Disconnect Timer Setting**
	For setting the disconnect detection time for Current Disconnect of talk-battery to signal a media disconnect event, an additional parameter must be changed in the ini file. From a web browser, enter **<*ip_address*>/*AdminPage*** in the **Address** field where **<*ip_address*>**is the IP address of the MSBG. The main page will appear as shown below. In this instance, the detection is reported as a disconnect at 600ms of no talk-battery. Enter parameter name: **CURRENTDISCONNECTDURATION** and Enter Value: **600**.
	
	
	Parameter Name: CURRENTDISCONNECTDURATION
	Enter Value: 600
	`Parameter Name: CURRENTDISCONNECTDURATION`
	`The Value is invalid:`
	`Parameter Current Value: 600`
	`Parameter Description:Defines the current-disconnect duration (in msec).`

7.1. SAS Configuration for MSBG

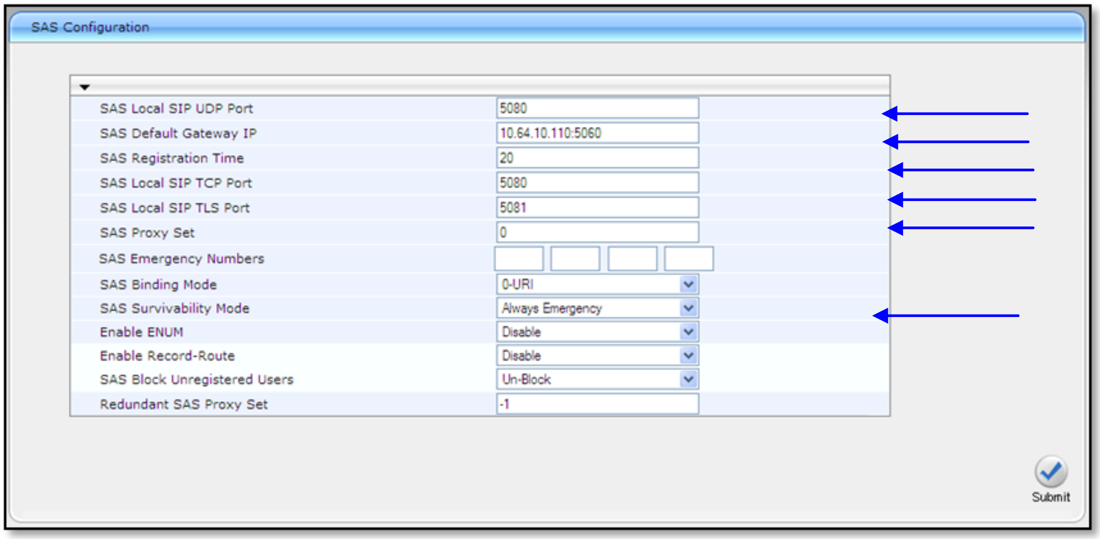
SAS supports various configuration possibilities, depending on how the device is deployed in the network and the network architecture requirements. This section provides step-by-step procedures on configuring the SAS application, using the device's Web interface.

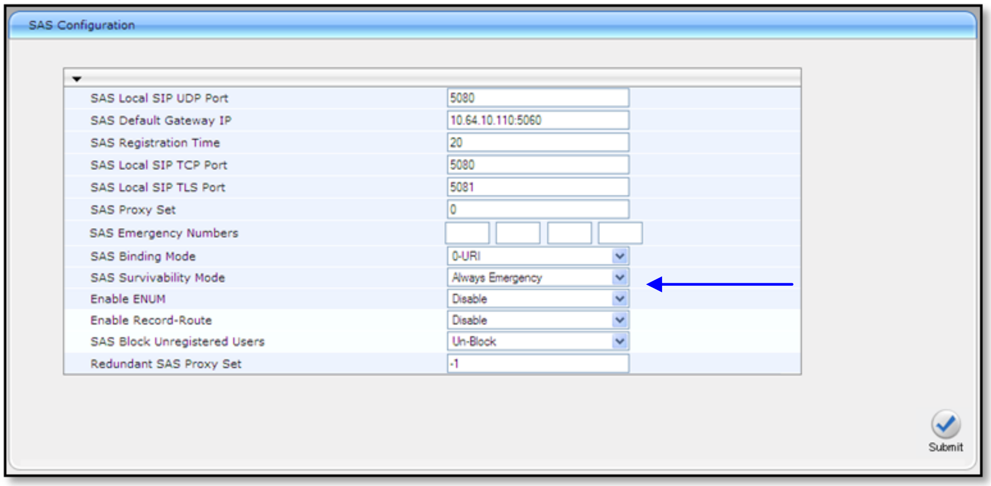
The SAS configuration includes the following:

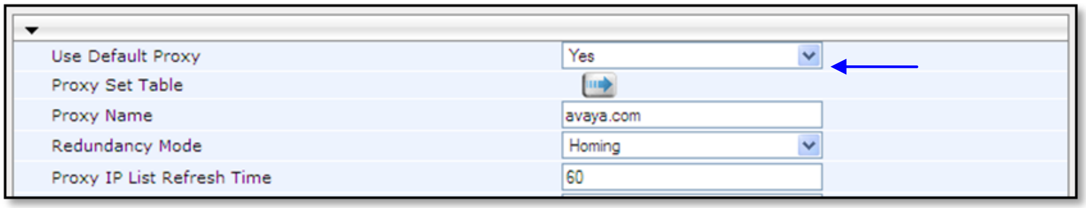
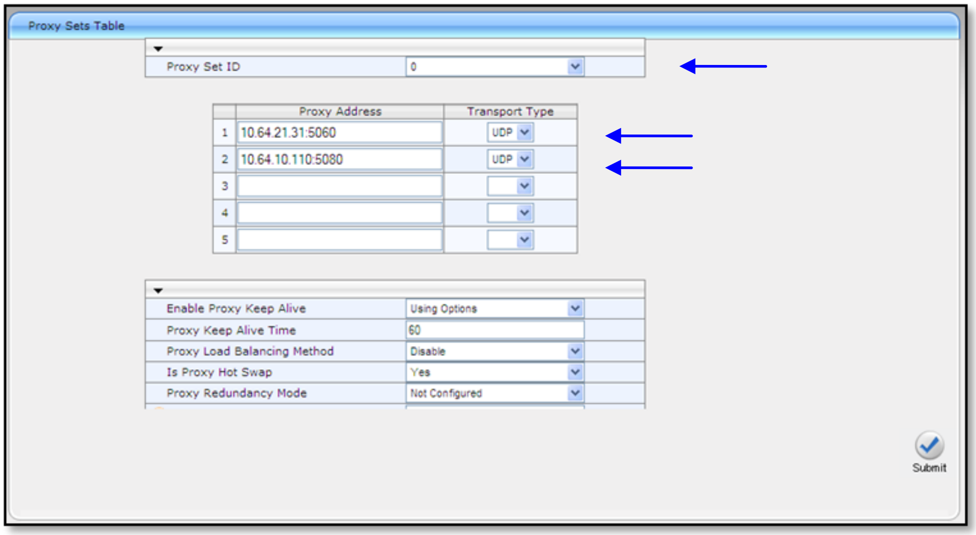
- Enabling the SAS Application on the MSBG
- Defining MSBGSAS Settings - common to all deployment types
- Configuring SAS Redundant Mode
- Configuring MSBG Gateway Application with SAS

Step	Description
1.	**Enabling the SAS Application on the MSBG** Before beginning to configure SAS, the SAS application must be enabled on the device. Once enabled, the device's Web interface provides the SAS pages for configuring SAS. *Note: The SAS application is available only if the device is installed with the SAS Software Upgrade Key. If the device is not installed with the SAS feature, please contact anAudioCodes representative* To enable the SAS application(Configured in**Section 7,Step 6**)open the **Applications Enabling page (**Configuration>VoIP>Applications Enabling>Applications Enabling**). From the** Enable SAS **drop-down list, select** *Enable***.**  Applications Enabling Enable SAS: Enable Enable SBC Application: Enable Enable IP2IP Application: Enable Click **Submit**.Save the changes to the flash memory with a device reset; after the device resets, the **SAS** menu re-appears.

Step	Description
2.	**Defining MSBG SAS Settings** The common SAS settings include configuring the various SAS parameters and defining the Proxy Set ID for the SAS proxy. This configuration was not included in **Section 7** and must be completed to replicate the test scenarios.The procedure below describes how to configure SAS settings that are common to all SAS modes. To configure common SAS settings: ▪ Open the **SAS Configuration** page **Configuration tab>VoIP menu>SAS>Stand Alone Survivability**. ▪ Define the port used for sending and receiving SAS messages. This can be any of the following port types: o UDP port - defined in the **SAS Local SIP UDP Port** field. o TCP port - defined in the **SAS Local SIP TCP Port** field. o TLS port - defined in the **SAS Local SIP TLS Port** field. *Note:This SAS port must be different to the device's local gateway port (i.e., that defined for the 'SIP UDP/TCP/TLS Local Port' parameter in the SIP General Parameters page - **Configuration>VoIP>SIP Definitions> General Parameters**).* In the **SAS Default Gateway IP** field, define the IP address and port (in the format x.x.x.x:port) of the device (i.e., Gateway application). Note that the port of the device is defined by the parameter **SIP UDP Local Port** (refer to the note above). In the **SAS Registration Time** field, define the value for the SIP Expires header that is sent in the 200 OK response to an incoming REGISTER message when SAS is in emergency state. From the **SAS Binding Mode** drop-down list, select the database binding mode: ▪ ***0-URI***: If the incoming AOR in the REGISTER request uses a 'tel:' URI or 'user=phone', the binding is done according to the Request-URI user part only. Otherwise, the binding is done according to the entire Request-URI (i.e., user and host parts - user@host). ▪ ***1-User Part Only***: Binding is done according to the user part only. Select '1-User Part Only' in cases where the UA sends REGISTER messages as SIP URI, but the INVITE messages sent to this UA include a Tel URI. For example, when the AOR of an incoming REGISTER is sip:3200@domain.com, SAS adds the entire SIP URI (e.g., sip:3200@domain.com) to its database (when the parameter is set to '0-URI'). However, if a subsequent Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS searches its database for "3200", which it does not find. Alternatively, when this parameter is set to '1-User Part Only', then upon receiving a REGISTER message with sip:3200@domain.com, SAS adds only the user part (i.e., "3200") to its database. Therefore, if a Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS can successfully locate the UA in its database.

Step	Description
	Defining MSBG SAS Settings (Continued)  SAS Local SIP UDP Port: 5080 SAS Default Gateway IP: 10.64.10.110:5060 SAS Registration Time: 20 SAS Local SIP TCP Port: 5080 SAS Local SIP TLS Port: 5081 SAS Proxy Set: 0 SAS Emergency Numbers: SAS Binding Mode: 0-URI SAS Survivability Mode: Always Emergency Enable ENUM: Disable Enable Record-Route: Disable SAS Block Unregistered Users: Un-Block Redundant SAS Proxy Set: -1 Click **Submit** to apply settings.

Step	Description
3.	**Configuring MSBG SAS Redundant Mode** This section describes how to configure the SAS redundant mode. This configuration was not included in Section 7 and must be completed to replicate the test scenarios. These settings are in addition to the ones described previously. *Note: The VoIP CPEs (such as IP phones or residential gateways) need to be defined so that their primary proxy is the external proxy and the* ***redundant*** *proxy destination addresses and port is the same as that configured for the device's SAS IP address and SAS SIP port.* To configure SAS redundant mode: ▪ Open the **SAS Configuration**page (**Configuration**>**VoIP>SAS**>**Stand Alone Survivability**). ▪ From the **SAS Survivability Mode** drop-down list, select one of the following depending on whether the UAs support homing (i.e., they always attempt to operate with the primary proxy, and if using the redundant proxy, they switch back to the primary proxy whenever it's available): **UAs support homing:** Select ***Always Emergency***. This is because SAS does not need to communicate with the primary proxy of the UAs; SAS serves only as the redundant proxy of the UAs. When the UAs detect that their primary proxy is available, they automatically resume communication with it instead of with SAS.  SAS Local SIP UDP Port: 5080 SAS Default Gateway IP: 10.64.10.110:5060 SAS Registration Time: 20 SAS Local SIP TCP Port: 5080 SAS Local SIP TLS Port: 5081 SAS Proxy Set: 0 SAS Emergency Numbers: SAS Binding Mode: 0-URI SAS Survivability Mode: Always Emergency Enable ENUM: Disable Enable Record-Route: Disable SAS Block Unregistered Users: Un-Block Redundant SAS Proxy Set: -1 Click **Submit**.

Step	Description
4.	**Configuring MSBG Gateway Application with SAS** If the device willrun both the Gateway and SAS applications, the configuration described in this section is required. The configuration steps apply only to SAS in redundant mode. These configurations were included in Section 7 to configure MSBG testing. *Note:The Gateway application must use the same SAS operation mode as the SIP UAs. For example, if the UAs use the SAS application as a redundant proxy (i.e., SAS redundancy mode), then the Gateway application must do the same.* To configure Gateway application with SAS redundant mode: Define the proxy servers for the Gateway application: ▪ Open the **Proxy & Registration** page (**Configuration**>**VoIP**>**SIPDefinitions**>**Proxy & Registration**). ▪ From the **Use Default Proxy** drop-down list, select ***Yes***.  Use Default Proxy: Yes Proxy Set Table Proxy Name: avaya.com Redundancy Mode: Homing Proxy IP List Refresh Time: 60 Click **Submit**. Open the **Proxy Sets Table** page (**Configuration**>**VoIP>Control Network>Proxy Sets Table**). From the **Proxy Set ID** drop-down list, select ***0***. In the first **Proxy Address** field, enter the IP address of the external proxy server. In the second **Proxy Address** field, enter the IP address and port of the device (in the format *x.x.x.x:port*).  Proxy Sets Table Proxy Set ID: 0 Proxy Address / Transport Type 1 10.64.21.31:5060 UDP 2 10.64.10.110:5080 UDP 3 4 5 Enable Proxy Keep Alive: Using Options Proxy Keep Alive Time: 60 Proxy Load Balancing Method: Disable Is Proxy Hot Swap: Yes Proxy Redundancy Mode: Not Configured Click **Submit**.

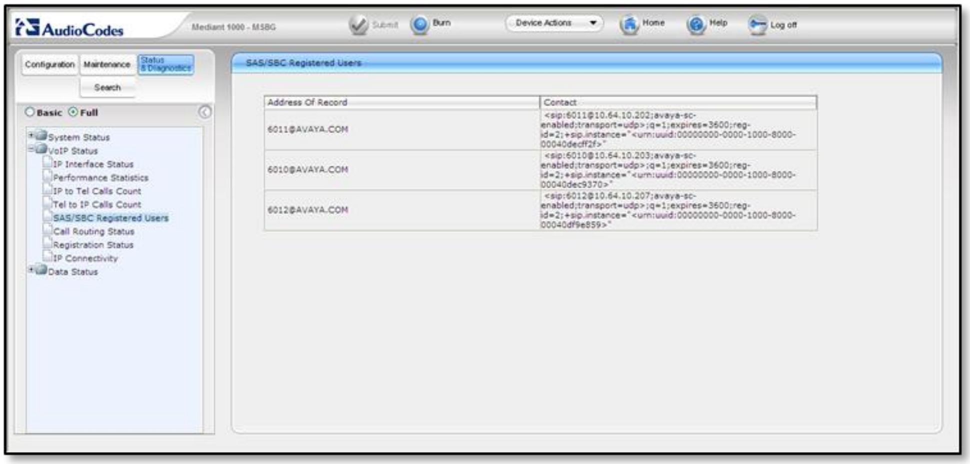
8. Verification Steps

The following steps may be used to verify the configuration from the Avaya side:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya Aura® System Manager web administration interface, verify that all branch endpoints are registered with the Avaya Aura® Session Manager.
- Verify that calls can be placed to/from the analog endpoints behind the branch gateways from Enterprise and Branch SIP users.
- Verify that calls can be placed to/from the analog endpoints and the PSTN.
- Verify that calls can be placed from the analog and SIP endpoints behind the branch gateways when a simulated data WAN failure is introduced.

The following steps may be used to verify the configuration from the Audio Codes side:

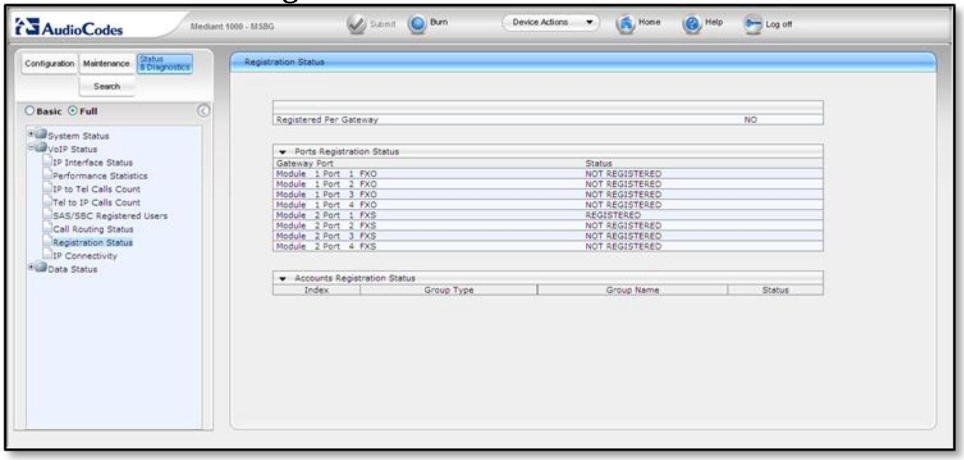
- To view SAS registered users, open the**SAS/SBC Registered Users** page (**Status & Diagnostics>VoIPStatus>SAS/SBC Registered Users**).



SAS/SBC Registered Users

Address Of Record	Contact
6011@AVAYA.COM	<sip:6011@10.64.10.202;avaya-sc-enabled;transport=udp>;q=1;expires=3600;reg-id=2;+sip.instance="<urn:uuid:00000000-0000-1000-8000-00040decff2f>"
6010@AVAYA.COM	<sip:6010@10.64.10.203;avaya-sc-enabled;transport=udp>;q=1;expires=3600;reg-id=2;+sip.instance="<urn:uuid:00000000-0000-1000-8000-00040dec9370>"
6012@AVAYA.COM	<sip:6012@10.64.10.207;avaya-sc-enabled;transport=udp>;q=1;expires=3600;reg-id=2;+sip.instance="<urn:uuid:00000000-0000-1000-8000-00040df9e859>"

- To view FXS Port Registration Status, open the **Registration Status** page (**Status & Diagnostics>VoIPStatus>Registration Status**).



Registration Status

Registered Per Gateway	NO

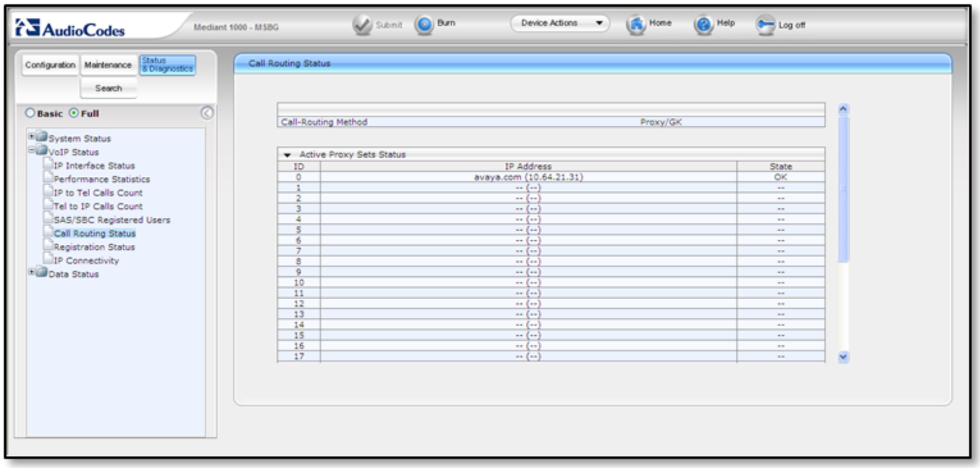
Ports Registration Status

Gateway Port	Status
Module 1 Port 1 FXO	NOT REGISTERED
Module 1 Port 2 FXO	NOT REGISTERED
Module 1 Port 3 FXO	NOT REGISTERED
Module 1 Port 4 FXO	NOT REGISTERED
Module 2 Port 1 FXS	REGISTERED
Module 2 Port 2 FXS	NOT REGISTERED
Module 2 Port 3 FXS	NOT REGISTERED
Module 2 Port 4 FXS	NOT REGISTERED

Accounts Registration Status

Index	Group Type	Group Name	Status

- To view call routing status, open the **Call Routing Status** page (**Status & Diagnostics>VoIPStatus>Call Routing Status**).



Call-Routing Method	Proxy/GK

Active Proxy Sets Status

ID	IP Address	State
0	avaya.com (10.64.21.31)	OK
1	-- (--)	--
2	-- (--)	--
3	-- (--)	--
4	-- (--)	--
5	-- (--)	--
6	-- (--)	--
7	-- (--)	--
8	-- (--)	--
9	-- (--)	--
10	-- (--)	--
11	-- (--)	--
12	-- (--)	--
13	-- (--)	--
14	-- (--)	--
15	-- (--)	--
16	-- (--)	--
17	-- (--)	--

9. Conclusion

These Application Notes describe the procedures required to configure the AudioCodesMediant 1000 and Mediant 800 Multi Service Business Gateways to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The AudioCodes Multi Service Business Gateways successfully passed compliance testing.

10. Additional References

Avaya

[1] *Administering Avaya Aura® Communication Manager Server Options*, Doc # 03-603479, Release 6.0.1, Issue 2.2, April 2011.

[2] *Administering AvayaAura™ Communication Manager*, Doc # 03-300509, Release 6.0, Issue 6.0, June 2010

[3] *Administering Avaya Aura® Session Manager*, Doc # 03-3603324, Release 6.1, Issue 1, November 2010

[4] *Avaya one-X™ Deskphone SIP for 9600 Series IP Telephones Administrator Guide Release 2.6*, Doc# 16-601944, Issue 6, June 2010

Audio Codes

[5] *LTRT-52307 SIP CPE Product Reference Manual, Version 6.2*

[6] *LTRT-40810 Mediant 1000 MSBG Installation Manual, Version 6.2*

[7] *LTRT-27001 Mediant 1000 MSBG User's Manual, Version 6.2*

[8] *LTRT-10205 Mediant 800 MSBG Installation Manual, Version 6.2*

[9] *LTRT-12804 Mediant 800 MSBG SIP User's Manual, Version 6.2*

[10] *LTRT-29802 SAS Technical Note, Version 6.2*

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

Product documentation for AudioCodes products may be found at http://www.audiocodes.com.

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.

Appendix - MSBG Advanced SAS Settings

This section describes the configuration of advanced SAS features that can be optionally implemented in an SAS deployment. *These configurations were not included in the current testing:*

- Manipulating incoming SAS Request-URI user part of REGISTER message
- Manipulating destination number of incoming SAS INVITE messages
- Defining SAS routing rules based on the SAS Routing table
- Blocking unregistered SAS UA's
- Defining SAS emergency calls

Step	Description
1.	**Manipulating URI user part of Incoming REGISTER** There are scenarios in which the UAs register to the proxy server with their full phone number (for example, "976653434"), but can receive two types of INVITE messages (calls): ▪ INVITEs whose destination is the UAs' full number (when the call arrives from outside the enterprise) ▪ INVITES whose destination is the last four digits of the UAs' phone number ("3434" in the example) when it is an internal call within the enterprise Therefore, it is important that the device registers the UAs in the SAS registered database with their extension numbers (for example, "3434") in addition to their full numbers. To do this, define a manipulation rule to manipulate the SIP Request-URI user part of the AOR (in the To header) in incoming REGISTER requests. Once manipulated, it is saved in this manipulated format in the SAS registered users database in addition to the original (un-manipulated) AOR. For example: Assume the following incoming REGISTER message is received and that the requirement is to register in the SAS database the UA's full number as well as the last four digits from the right of the SIP URI user part:

```
REGISTER sip:10.33.38.2 SIP/2.0
Via: SIP/2.0/UDP 10.33.4.226:5050;branch=z9hG4bKac10827
Max-Forwards: 70
From: <sip: 976653434@10.33.4.226>;tag=1c30219
To: <sip: 976653434@10.33.4.226>
Call-ID: 16844@10.33.4.226
CSeq: 1 REGISTER
Contact: <sip: 976653434@10.10.10.10:5050>;expires=180
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,
UPDATE
Expires: 180
User-Agent: Audiocodes-Sip-Gateway-/v.
Content-Length: 0
```

Step	Description

Manipulating URI user part of Incoming REGISTER (Continued)

After manipulation, the SAS registers the user in its database as follows:

AOR: 976653434@10.33.4.226

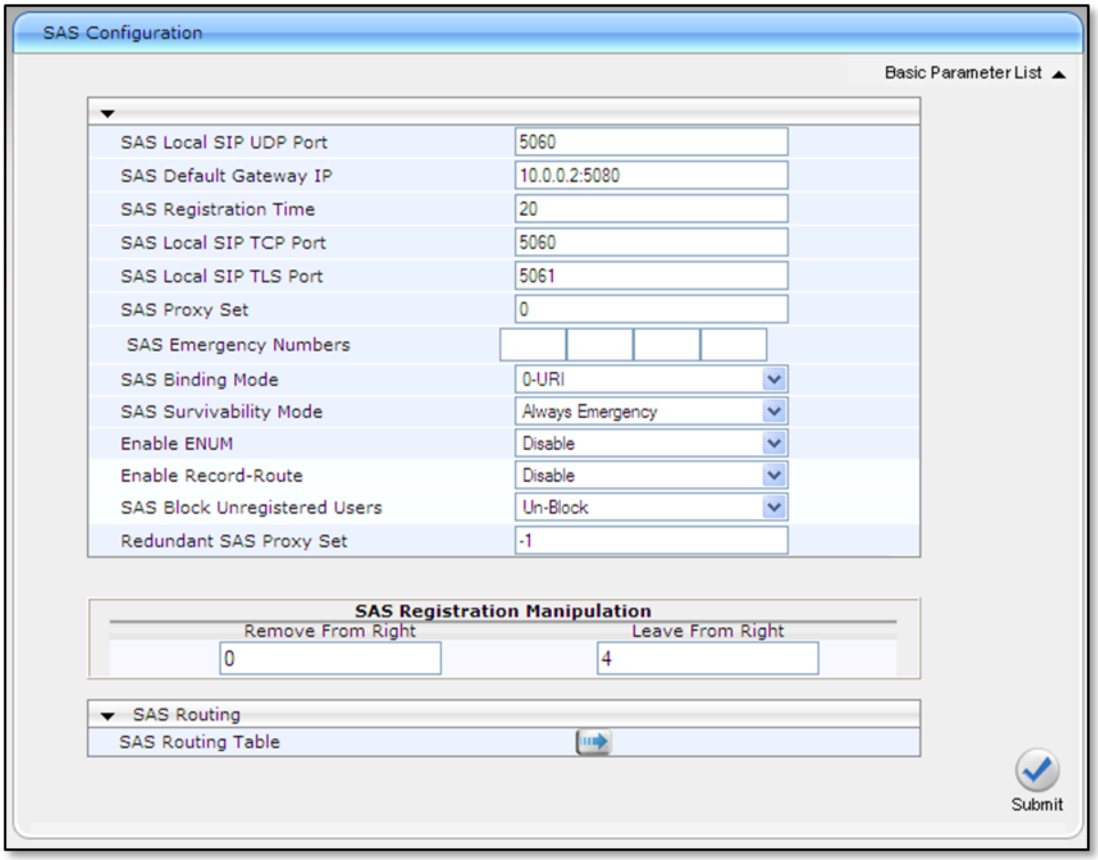
Associated AOR: 3434@10.33.4.226 (after manipulation, in which only the four digits from the right of the URI user part are retained)

Contact: 976653434@10.10.10.10

The procedure below describes how to configure the manipulation example scenario above (relevant ini parameter is SASRegistrationManipulation):

To manipulate incoming Request-URI user part of REGISTER message:

- Open the 'SAS Configuration' page (Configuration tabVoIP menuSASStand Alone Survivability).
- In the SAS Registration Manipulation table, in the 'Leave From Right' field, enter the number of digits (e.g., 4) to leave from the right side of the user part. (The 'Leave From Right' field defines the number of digits to retain from the right side of the user part; all other digits in the user part are removed.)



SAS Configuration

SAS Local SIP UDP Port	5060
SAS Default Gateway IP	10.0.0.2:5080
SAS Registration Time	20
SAS Local SIP TCP Port	5060
SAS Local SIP TLS Port	5061
SAS Proxy Set	0
SAS Emergency Numbers	
SAS Binding Mode	0-URI
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Un-Block
Redundant SAS Proxy Set	-1

SAS Registration Manipulation

Remove From Right	Leave From Right
0	4

Click **Submit**.

Step	Description
2.	**Manipulating Destination Number of Incoming INVITE**

One can define a manipulation rule to manipulate the destination number in the Request-URI of incoming INVITE messages when SAS is in emergency state. This is required, for example, if the call is destined to a registered user but the destination number in the received INVITE is not the number assigned to the registered user in the SAS registration database. To overcome this and successfully route the call, define manipulation rules to change the INVITE's destination number so that it matches that of the registered user in the database. This is done using the IP to IP Inbound Manipulation table.

For example, in SAS emergency state, assume an incoming INVITE has a destination number "7001234" which is destined to a user whose registered in the SAS database as "552155551234". In this scenario, the received destination number needs to be manipulated to the number "552155551234". The outgoing INVITE sent by the device will also then contain this number in the Request-URI user part.

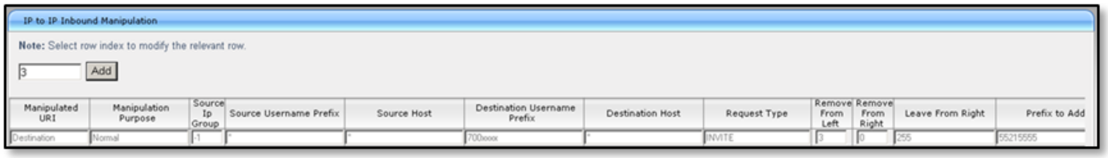
In normal state, the numbers are not manipulated. In this state, SAS searches the number 552155551234 in its database and if found, it sends the INVITE containing this number to the UA.

To manipulate destination number in SAS emergency state:

- Load an ini file to the device with the following setting to enable inbound manipulation:

  SASInboundManipulationMode = 1
- Open the 'SAS Configuration' page (**Configuration>VoIP>SAS>Stand Alone Survivability**).
  - Click the IP to IP Inbound Manipulation Table button to open the 'IP to IP Inbound Manipulation' page.
  - Enter an table index number, and then click Add.
  - Define the rules as required, and then click Apply.

The figure below displays a manipulation rule for the example scenario described above whereby the destination number "7001234" is changed to "552155551234".



IP to IP Inbound Manipulation

Note: Select row index to modify the relevant row.

3

Manipulated URI	Manipulation Purpose	Source Ip Group	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Remove From Left	Remove From Right	Leave From Right	Prefix to Add
Destination	Normal	-1	*	*	700xxxx	*	INVITE	3	0	255	55215555

Notes: The 'Source IP Group' field must not be configured; leave it at '-1'.

The 'Manipulation Purpose' field must be set to 'Normal'.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

SAS Routing Based on SAS Routing Table Rules

SAS routing based on the SAS Routing table is applicable for:

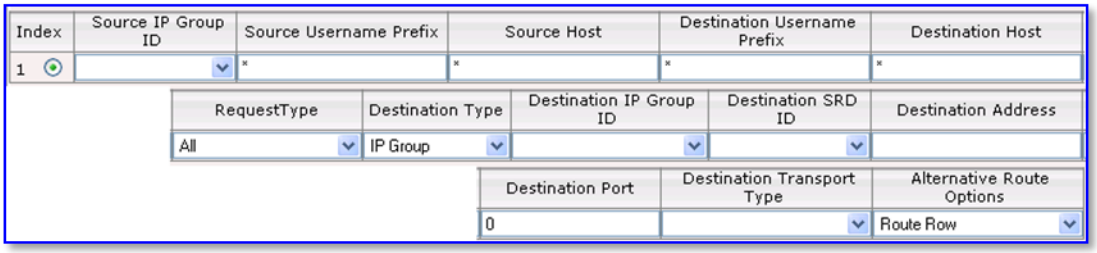
SAS in normal state, if the SASSurvivabilityMode parameter is set to 4

SAS in emergency state, if the SASSurvivabilityMode parameter is not set to 4

The SAS routing rule destination can be an IP Group, IP address, Request-URI, or ENUM query.

To configure SAS routing rules in the SAS Routing table:

- Open the 'SAS Configuration' page (**Configuration>VoIP>SAS>Stand Alone Survivability**).
- In the 'Redundant SAS Proxy Set' field, enter the Proxy Set ID of the redundant SAS (not shown).
- Click the SAS Routing Table button to define SAS IP-to-IP routing rules.



<table>
<tr><th>Index</th><th>Source IP Group ID</th><th>Source Username Prefix</th><th>Source Host</th><th>Destination Username Prefix</th><th>Destination Host</th></tr>
<tr><td>1 ●</td><td></td><td>*</td><td>*</td><td>*</td><td>*</td></tr>
</table>

<table>
<tr><th>RequestType</th><th>Destination Type</th><th>Destination IP Group ID</th><th>Destination SRD ID</th><th>Destination Address</th></tr>
<tr><td>All</td><td>IP Group</td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th>Destination Port</th><th>Destination Transport Type</th><th>Alternative Route Options</th></tr>
<tr><td>0</td><td></td><td>Route Row</td></tr>
</table>

Add an entry and then configure it according to the table below.

Click the Apply button to save changes
to flash memory.

Note: The following fields are not applicable to SAS: Source IP Group ID, Request Type, Destination SRD ID, and Alternative Route Options.

</td></tr>
</table>

Step	Description
	SAS Routing Based on SAS Routing Table Rules (Continued) SAS IP2IP Routing Table Parameters:

Parameter	Description
Matching Characteristics	
Source Username Prefix **[IP2IPRouting_SrcUsernamePrefix]**	The prefix of the user part of the incoming INVITE's source URI (usually the From URI). The default is "*".
Source Host **[IP2IPRouting_SrcHost]**	The host part of the incoming SIP INVITE's source URI (usually the From URI). If this rule is not required, leave the field empty. To denote any host name, use the asterisk (*) symbol. The default is "*".
Destination Username Prefix **[IP2IPRouting_DestUsernamePrefix]**	The prefix of the incoming SIP INVITE's destination URI (usually the Request URI) user part. If this rule is not required, leave the field empty. To denote any prefix, use the asterisk (*) symbol. The default is "*".
Destination Host **[IP2IPRouting_DestHost]**	The host part of the incoming SIP INVITE's destination URI (usually the Request URI). If this rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any destination host. The default is "*".
Operation Routing Rule (performed when match found in above characteristics)	
Destination Type **[IP2IPRouting_DestType]**	Determines the destination type to which the outgoing INVITE is sent. **[0]** IP Group (default) = The INVITE is sent to the IP Group's Proxy Set (if the IP Group is of SERVER type) \ registered contact from the database (if USER type). **[1]**Dest Address = The INVITE is sent to the address configured in the following fields: 'Destination Address', 'Destination Port', and 'Destination Transport Type'. **[2]** Request URI = The INVITE is sent to the address indicated in the incoming Request-URI. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence. **[3]** ENUM = An ENUM query is sent to conclude the destination address. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request URI parameters are overridden and these fields take precedence.

Step	Description
	SAS Routing Based on SAS Routing Table Rules (Continued)

Parameter	Description
Destination IP Group ID **[IP2IPRouting_DestIPGroupID]**	The IP Group ID to where you want to route the call. The INVITE messages are sent to the IP address(es) defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, the IP Group takes precedence. If the destination IP Group is of USER type, the device searches for a match between the Request-URI (of the received INVITE) to an AOR registration record in the device's database. The INVITE is then sent to the IP address of the registered contact. The default is -1. **Note:** This parameter is only relevant if the parameter 'Destination Type' is set to 'IP Group'. However, regardless of the settings of the parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile
Destination Address **[IP2IPRouting_DestAddress]**	The destination IP address (or domain name, e.g., domain.com) to where the call is sent. **Notes:** This parameter is applicable only if the parameter 'Destination Type' is set to 'Dest Address'**[1].** When using domain names, enter a DNS server IP address or alternatively, define these names in the 'Internal DNS Table'.
Destination Port **[IP2IPRouting_DestPort]**	The destination port to where the call is sent.
Destination Transport Type **[IP2IPRouting_DestTransportType]**	The transport layer type for sending the call: **[-1]** Not Configured (default) **[0]** UDP **[1]** TCP **[2]** TLS **Note:** When this parameter is set to -1, the transport type is determined by the parameter SIPTransportType.

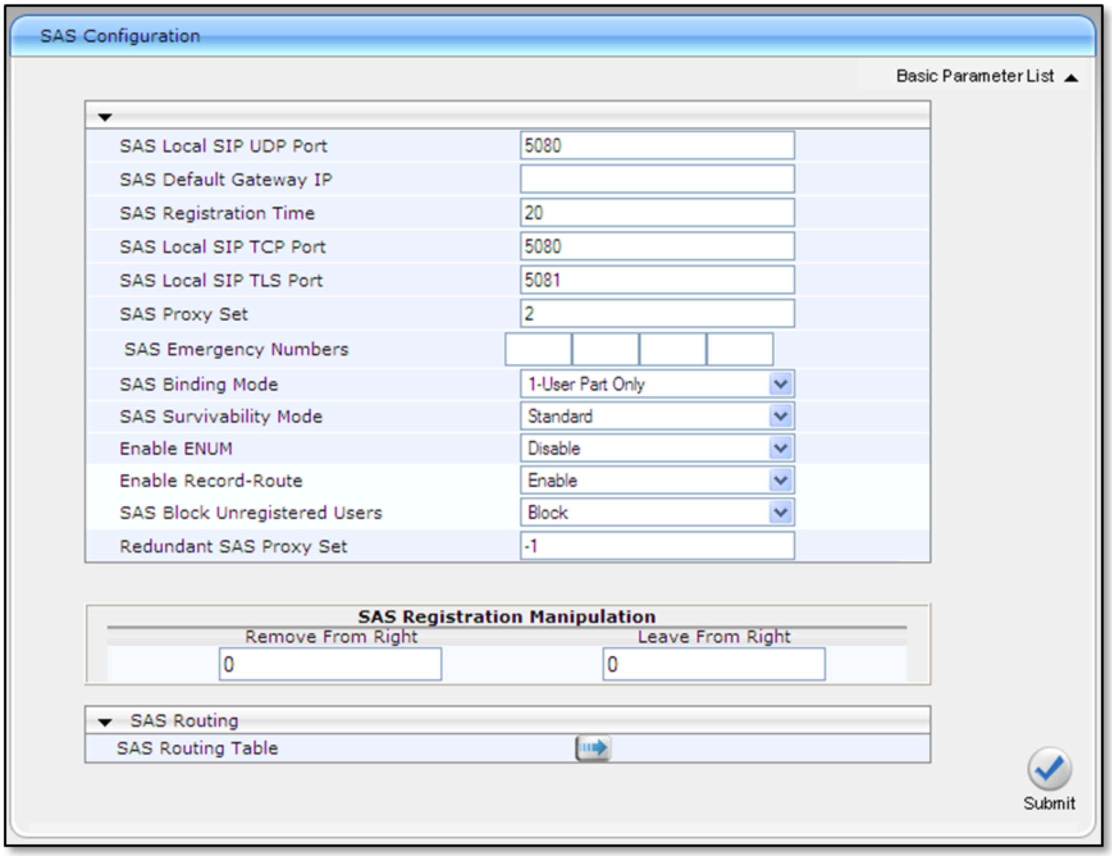
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

Blocking Calls from Unregistered SAS Users

To prevent malicious calls (for example, Service Theft), it is recommended to configure the feature for blocking SIP INVITE messages received from SAS users that are not registered in the SAS database. This applies to SAS in normal and emergency states.

To block calls from unregistered SAS users:

- Open the 'SAS Configuration' page (**Configuration>VoIP>SAS>Stand Alone Survivability**).
- From the **SAS Block Unregistered Users** drop-down list, select ***Block***.



<table>
<tr><th></th><th></th></tr>
<tr><td>SAS Local SIP UDP Port</td><td>5080</td></tr>
<tr><td>SAS Default Gateway IP</td><td></td></tr>
<tr><td>SAS Registration Time</td><td>20</td></tr>
<tr><td>SAS Local SIP TCP Port</td><td>5080</td></tr>
<tr><td>SAS Local SIP TLS Port</td><td>5081</td></tr>
<tr><td>SAS Proxy Set</td><td>2</td></tr>
<tr><td>SAS Emergency Numbers</td><td></td></tr>
<tr><td>SAS Binding Mode</td><td>1-User Part Only</td></tr>
<tr><td>SAS Survivability Mode</td><td>Standard</td></tr>
<tr><td>Enable ENUM</td><td>Disable</td></tr>
<tr><td>Enable Record-Route</td><td>Enable</td></tr>
<tr><td>SAS Block Unregistered Users</td><td>Block</td></tr>
<tr><td>Redundant SAS Proxy Set</td><td>-1</td></tr>
</table>

SAS Registration Manipulation

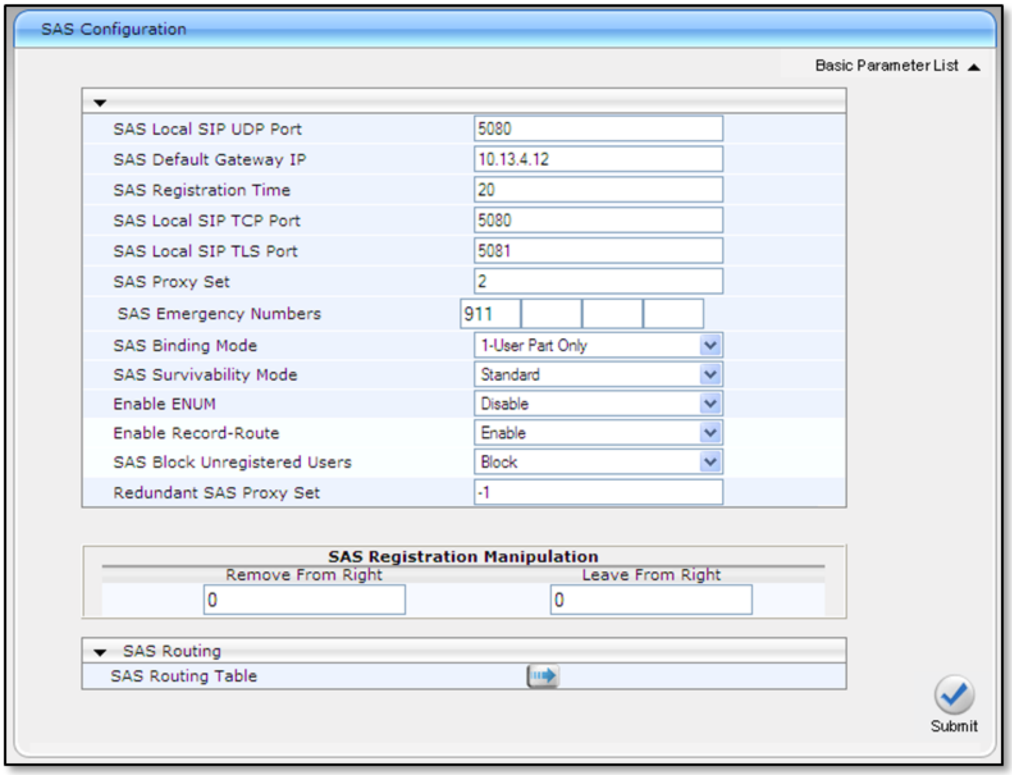
<table>
<tr><th>Remove From Right</th><th>Leave From Right</th></tr>
<tr><td>0</td><td>0</td></tr>
</table>

SAS Routing

SAS Routing Table

Click **Submit.**

</td></tr>
</table>

Step	Description
5.	**Configuring SAS Emergency Calls** One can configure SAS to route emergency calls (such as 911 in North America) directly to the PSTN (through its FXO interface or E1/T1 trunk interface). Therefore, even during a communication failure with the external proxy, enterprise UAs can still make emergency calls. Define up to four emergency numbers, where each number can include up to four digits. When SAS receives a SIP INVITE (from a UA) that includes one of the user-defined emergency numbers in the SIP user part, it forwards the INVITE directly to the default gateway. The default gateway is defined in the 'SAS Default Gateway IP' field, and this is the device itself. The device then sends the call directly to the PSTN. This feature is applicable to SAS in normal and emergency states. To configure SAS emergency numbers: ▪ Open the 'SAS Configuration' page (**Configuration>VoIP>SAS>Stand Alone Survivability**). ▪ In the **'SAS Default Gateway IP'** field, define the IP address and port (in the format x.x.x.x:port) of the device (Gateway application which will access the PSTN). ▪ In the **'SAS Emergency Numbers'** fields, enter an emergency number in each field box.  SAS Configuration SAS Local SIP UDP Port: 5080 SAS Default Gateway IP: 10.13.4.12 SAS Registration Time: 20 SAS Local SIP TCP Port: 5080 SAS Local SIP TLS Port: 5081 SAS Proxy Set: 2 SAS Emergency Numbers: 911 SAS Binding Mode: 1-User Part Only SAS Survivability Mode: Standard Enable ENUM: Disable Enable Record-Route: Enable SAS Block Unregistered Users: Block Redundant SAS Proxy Set: -1 SAS Registration Manipulation Remove From Right: 0 Leave From Right: 0 SAS Routing SAS Routing Table Click **Submit**. *Note: The port of the device is defined in the 'SIP UDP/TCP/TLS Local Port' field in the 'SIP General Parameters' page (**Configuration>VoIP>SIP Definitions>General Parameters**).*

Step	Description
6.	**Maximum SAS Registered Users**

The table below lists the maximum number of SAS users that can be registered in the SAS registration database per product:

Product	Maximum SAS Registered Users
Mediant 800 MSBG	200
Mediant 1000 MSBG	600

Note: Despite the maximum number of SAS users, this capacity can be increased by implementing the SAS Cascading feature, as described below:

The SAS Cascading feature allows one to increase the number of SAS users above the maximum supported by the SAS gateway. This is achieved by deploying multiple SAS gateways in the network. For example, if the SAS gateway supports up to 600 users, but the enterprise has 1,500 users, deploy three SAS gateways to accommodate all users: the first SAS gateway can service 600 registered users, the second SAS gateway the next 600 registered users, and the third SAS gateway the rest (i.e., 300 registered users).

In SAS Cascading, the SAS gateway first attempts to locate the called user in its SAS registration database. Only if the user is not located, does the SAS gateway send it on to the next SAS gateway according to the SAS Cascading configuration.

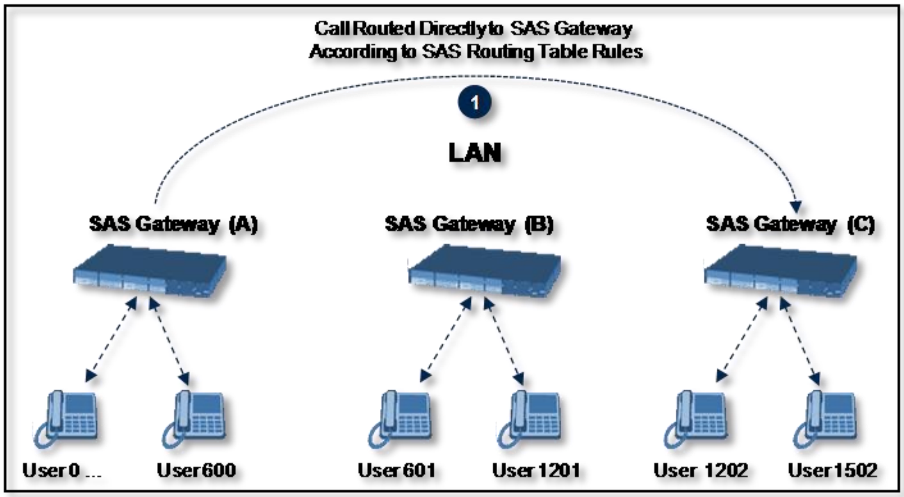
There are two methods for configuring SAS Cascading. This depends on whether the users can be identified according to their phone extension numbers:

- SAS Routing Table: If users can be identified with unique phone extension numbers, then the SAS Routing table is used to configure SAS Cascading. This SAS Cascading method routes calls directly to the SAS Gateway (defined by IP address) to which the called SAS user is registered.

  The following is an example of a SAS Cascading deployment of users with unique phone extension numbers:

  - users registered to the first SAS gateway start with extension number “40”
  - users registered to the second SAS gateway start with extension number “20”
  - users registered to the third SAS gateway start with extension number “30”

  The SAS Routing table rules for SAS Cascading are created using the destination (called) extension number prefix (e.g., “30”) and the destination IP address of the SAS gateway to which the called user is registered. Such SAS routing rules must be configured at each SAS gateway to allow routing between the SAS users. The routing logic for SAS Cascading is similar to SAS routing in Emergency state.

Step	Description
	Maximum SAS Registered Users (Continued) The figure below illustrates an example of a SAS Cascading call flow configured using the SAS Routing table. In this example, a call is routed from SAS Gateway (A) user to a user on SAS Gateway (C).  ▪ SAS Redundancy mode: If users cannot be distinguished (i.e., associated to a specific SAS gateway), then the SAS Redundancy feature is used to configure SAS Cascading. This mode routes the call in a loop fashion, from one SAS gateway to the next, until the user is located. Each SAS gateway serves as the redundant SAS gateway (“redundant SAS proxy server”) for the previous SAS gateway (in a one-way direction). For example, if a user calls a user that is not registered on the same SAS gateway, the call is routed to the second SAS gateway, and if not located, it is sent to the third SAS gateway. If the called user is not located on the third (or last) SAS gateway, it is then routed back to the initial SAS gateway, which then routes the call to the default gateway (i.e., to the PSTN). Each SAS gateway adds its IP address to the SIP via header in the INVITE message before sending it to the next (“redundant”) SAS gateway. If the SAS gateway receives an INVITE and its IP address appears in the SIP via header, it sends it to the default gateway (and not to the next SAS gateway), as defined by the SASDefaultGatewayIP parameter. Therefore, this mode of operation prevents looping between SAS gateways when a user is not located on any of the SAS gateways.

Step	Description
	Maximum SAS Registered Users (Continued) The figure below illustrates an example of a SAS Cascading call flow when configured using the SAS Redundancy feature. In this example, a call is initiated from a SAS Gateway (A) user to a user that is not located on any SAS gateway. The call is subsequently routed to the PSTN.