



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring Avaya Aura® Session Manager and Avaya Aura® Communication Manager with AudioCodes Mediant 3000 Gateway for E1 access - Issue 1.0

### Abstract

These Application Notes describe the procedure for configuring the AudioCodes Mediant 3000 Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunking along with E1 access to a simulated PSTN.

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

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.

## Table of Contents

1. Introduction.....	4
2. General Test Approach and Test Results.....	4
2.1. Interoperability Compliance Testing.....	4
2.2. Test Results .....	5
2.3. Support .....	5
3. Reference Configuration.....	6
4. Equipment and Software Validated .....	7
5. Configure Avaya Aura® Communication Manager .....	7
5.1. Verify Avaya Aura® Communication Manager License.....	8
5.2. Administer System Parameters Features .....	9
5.3. Administer IP Node Names.....	10
5.4. Administer IP Network Region and Codec Set.....	11
5.5. Administer SIP Trunks with Avaya Aura® Session Manager .....	13
5.5.1. Add SIP Signaling Group.....	13
5.5.2. Add Trunk Group.....	14
5.6. Configure Route Patterns .....	15
5.6.1. Route Pattern for reaching Session Manager and Simulated PSTN Endpoints.....	15
5.7. Administer Private Numbering .....	16
5.8. Administer Dial Plan and AAR analysis .....	17
5.9. Administer ARS Analysis .....	17
5.10. Administer Feature Access Code.....	18
5.11. Save Changes.....	18
6. Configure Avaya Aura® Session Manager.....	19
6.1. Specify SIP Domain .....	20
6.2. Add Locations .....	21
6.3. Add Adaptations.....	22
6.4. Add SIP Entities and SIP Entity Links .....	24
6.4.1. Adding Avaya Aura® Communication Manager SIP Entity and SIP Entity Link .....	24
6.4.2. Adding AudioCodes Mediant 3000 Gateway SIP Entity.....	26
6.5. Add Routing Policies.....	28
6.6. Add Dial Patterns .....	31
6.7. Add Users for SIP Phones .....	33
6.7.1. Identity .....	33
6.7.2. Communication Profile.....	34
7. AudioCodes Mediant 3000 Configuration.....	36
7.1. Log Into Mediant 3000.....	36
7.2. Configure Media Gateway IP Network Parameters .....	38
7.2.1. Saving Configuration and Resetting Mediant 3000.....	39
7.3. Saving Configuration .....	40
7.4. Configure Media Gateway TDM and Timing Parameters .....	42
7.4.1. Configure TDM Bus.....	42
7.4.2. Configure Digital PCM Settings .....	43

7.4.3.	Configure System Timing .....	44
7.5.	Configure Media Gateway Media Settings .....	45
7.5.1.	Configure the Voice parameters .....	45
7.5.2.	Configure the Fax Parameters .....	46
7.5.3.	Configure the RTP/RTCP Parameters .....	47
7.6.	Configure Media Gateway Telephony/PSTN Interface Parameters .....	48
7.6.1.	Configure Trunk Group Table.....	50
7.7.	Configure SIP Protocol Parameters .....	51
7.7.1.	Configure General SIP Protocol Parameters.....	51
7.7.2.	Configure DTMF and Dialing Parameters .....	52
7.7.3.	Configure Proxy & Registration Parameters .....	53
7.7.4.	Configure Device's Coders .....	54
7.7.5.	Configure Advanced General Protocol Parameters .....	55
7.7.6.	Configure Supplementary Services Parameters .....	56
7.7.7.	Configure Number Manipulation Tables.....	57
7.7.8.	Configure IP to Trunk Group Routing Rules .....	58
7.7.9.	Configure Outbound IP Routing Rules.....	59
7.7.10.	Configure Release Cause Mapping .....	61
7.7.11.	Configure Syslog Parameters for Debug Assistance.....	62
8.	Verification Steps .....	63
8.1.	Verify Avaya Aura® Communication Manager Trunk Status.....	63
8.2.	SIP Monitoring on Avaya Aura® Session Manager.....	64
8.3.	Utilizing Mediant 3000 Web Interface to Observe Status .....	65
8.3.1.	Device Status .....	65
8.3.2.	Device Information .....	66
8.3.3.	Trunks and Channels Status .....	67
9.	Conclusion .....	67
10.	Additional References.....	67
11.	Appendix.....	68

# 1. Introduction

These Application Notes describe the procedure for configuring the AudioCodes Mediant 3000 Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager using SIP trunking along with E1 access to a simulated PSTN.

These Application Notes present a sample configuration for an enterprise network consisting of Avaya Aura® Session Manager and Avaya Aura® Communication Manager, integrated with an AudioCodes Mediant 3000 Gateway using SIP and providing E1 access to a simulated PSTN. The AudioCodes Mediant 3000 is a feature-rich, highly available VoIP gateway supporting low to medium channel densities. The AudioCodes Mediant 3000 compact footprint (2U) allows high capacity and High Availability (HA) when business critical contact centers require such resilience. The AudioCodes Mediant 3000 has comprehensive PSTN access capabilities as well as SIP to SIP interworking features that enable the interconnection between enterprises and service providers. In addition to E1/T1 interfaces, the AudioCodes Mediant 3000 supports high-density PSTN interfaces, such as T3, STM-1 and OC3 to provide the enterprise with lower PSTN lease costs. The proven interoperability of the AudioCodes Mediant 3000 with different PBXs and PSTN switches facilitates smooth deployment. Even though the Mediant 3000 supports a variety of different protocols and features, only SIP and E1 access were verified in this compliance test.

## 2. General Test Approach and Test Results

The general test approach was to make calls, verify codecs, and exercise common PBX features, between endpoints located in the enterprise and the simulated PSTN.

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

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability. The feature testing focused on verifying the following:

- Simulated PSTN calls from and to Avaya endpoints
- Calling with various Avaya Deskphone models
- Support for G.711A, G.711MU and G.729 codecs
- SIP transport using UDP and TCP
- Codec negotiation
- Telephony supplementary features, such as Hold, Call Transfer, Conference Calling and Call Forwarding
- DTMF Tone Support
- Voicemail Coverage and Retrieval

- Direct IP-to-IP Media (also known as “Shuffling”) over SIP Trunk. Direct IP-to-IP media allows compatible phones to reconfigure the RTP path after call establishment directly between the Avaya phones and the AudioCodes Mediant 3000 Gateway and release media processing resources on the Avaya Media Gateway

## **2.2. Test Results**

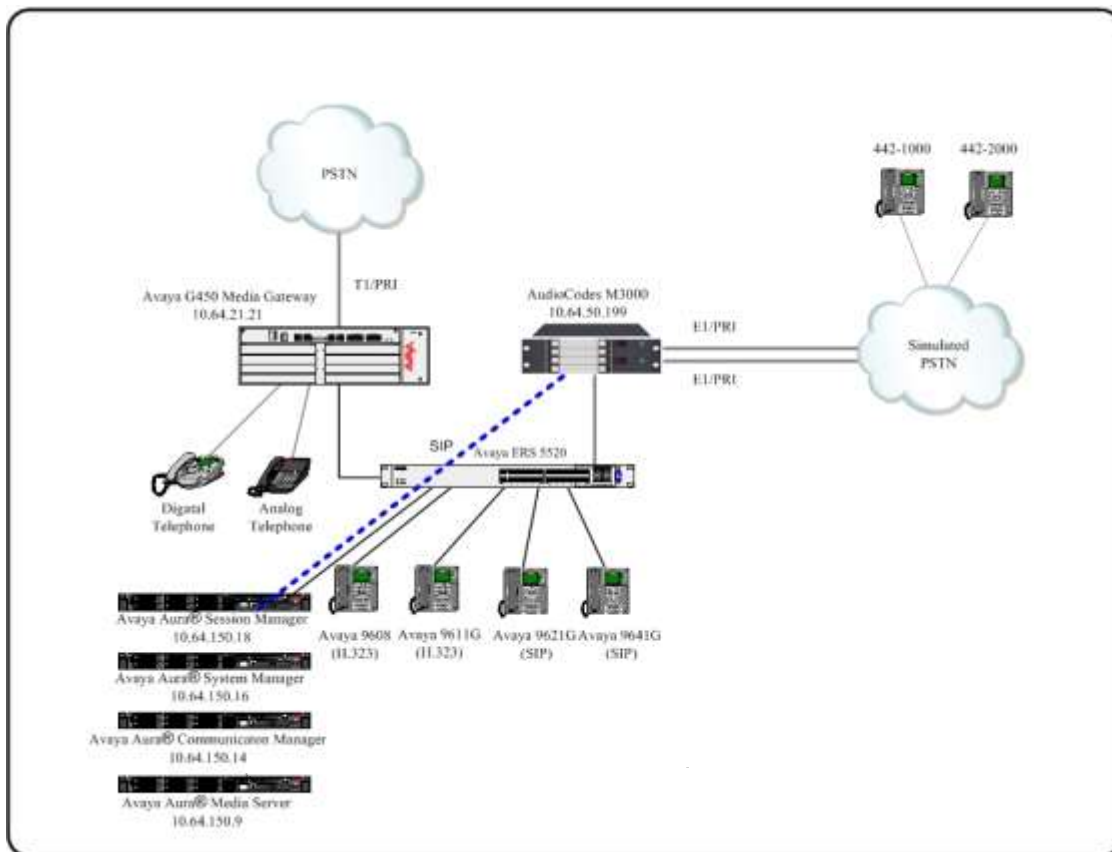
The AudioCodes Mediant 3000 passed compliance testing.

## **2.3. Support**

For technical support, contact AudioCodes via the support link at [www.audiocodes.com](http://www.audiocodes.com).

### 3. Reference Configuration

As shown in **Figure 1**, the Avaya enterprise network uses SIP trunking for call signaling internally, and with the Mediant 3000 Gateway in order to access the simulated PSTN. The Mediant 3000 is managed by using the web interface. Session Manager, with its SM-100 (Security Module) network interface, routes calls between the different entities using SIP Trunks. All inter-system calls are carried over these SIP trunks. Session Manager supports flexible inter-system call routing based on the dialed number, the calling number and the system location; it can also provide protocol adaptation to allow multi-vendor systems to interoperate. Session Manager is managed by Avaya Aura® System Manager via the management network interface.



**Figure 1: Compliance Test Reference Configuration**

For the sample configuration shown in **Figure 1**, Session Manager, System Manager, Communication Manager, and Media Server all run in a virtual environment. These Application Notes focus on the configuration of the SIP trunks and call routing.

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in a Virtual Environment	7.0 SP3
Avaya Aura® Session Manager in a Virtual Environment	7.0 SP2
Avaya Aura® System Manager in a Virtual Environment	7.0 SP2
Avaya Aura® Media Server in a Virtual Environment	7.7.0.226
Avaya 96x1 Deskphone	SIP 7.0, H.323 6.6
Avaya 6211 and 6221 Analog Phone	-
AudioCodes Mediant 3000	7.00A.049.003

## 5. Configure Avaya Aura® Communication Manager

This section shows the configuration in Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Communication Manager, please consult with **Reference [1]**. The procedures include the following areas:

- Verify Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec set
- Administer SIP Signaling Group and Trunk Group
- Administer Route Pattern
- Administer Private Numbering
- Administer Dial Plan and AAR analysis
- Administer ARS analysis
- Administer Feature Access Codes
- Save Changes

## 5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameter customer options** command to verify whether the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

**Note:** The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	4000	10	
Maximum Concurrently Registered IP Stations:	2400	1	
Maximum Administered Remote Office Trunks:	4000	0	
Maximum Concurrently Registered Remote Office Stations:	2400	0	
Maximum Concurrently Registered IP eCons:	68	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	2400	2	
Maximum Video Capable IP Softphones:	2400	4	
<b>Maximum Administered SIP Trunks:</b>	<b>4000</b>	<b>22</b>	
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0	
Maximum Number of DS1 Boards with Echo Cancellation:	80	0	
Maximum TN2501 VAL Boards:	10	0	
Maximum Media Gateway VAL Sources:	50	1	
Maximum TN2602 Boards with 80 VoIP Channels:	128	0	
Maximum TN2602 Boards with 320 VoIP Channels:	128	0	
Maximum Number of Expanded Meet-me Conference Ports:	300	0	



## 5.2. Administer System Parameters Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from/to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable all trunk-to-trunk transfers on a system wide basis.

```
change system-parameters features                               Page 1 of 20
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? no
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? n
```

### 5.3. Administer IP Node Names

Use the **change node-names ip** command to add entries for Communication Manager and Session Manager that will be used for connectivity. In the sample network, the processor Ethernet interface **procr** and **10.64.150.14** are entered as **Name** and **IP Address** for the signaling in Communication Manager running in a virtual environment. In addition, **sm15018** and **10.64.150.18** are entered for Session Manager.

change node-names ip		Page 1 of 2	
		IP NODE NAMES	
Name	IP Address		
procr	10.64.150.14		
sm15018	10.64.150.18		

## 5.4. Administer IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number, to configure the network region being used. In the sample network ip-network-region **1** is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: avaya.com
        Name: CM Local      Stub Network Region: n
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
    Codec Set: 1          Inter-region IP-IP Direct Audio: yes
        UDP Port Min: 40000      IP Audio Hairpinning? y
        UDP Port Max: 65535
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
H.323 IP ENDPOINTS          AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 Link Bounce Recovery? y      RSVP Enabled? n
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
        Keep-Alive Count: 5
```

Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. The codecs used in the compliance test are shown here. Configure the IP Codec Set as shown in the screen below.

Retain the default values for the remaining fields.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP CODEC SET

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size (ms)
1: G.711A      n           2         20
2: G.711MU     n           2         20
3: G.729       n           2         20
4:
5:
6:
7:

Media Encryption
1: none
2:
3:
```

## 5.5. Administer SIP Trunks with Avaya Aura® Session Manager

In the test configuration, a SIP trunk was configured between Communication Manager and Session Manager for enterprise calling between Communication Manager and Session Manager registered endpoints. Additionally a SIP trunk was configured between Session Manager and the Mediant 3000 in order to communicate between the enterprise and the simulated PSTN. To administer a SIP Trunk on Communication Manager, two steps are required: the creation of a signaling group and a trunk group.

### 5.5.1. Add SIP Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** sip
- **Transport Method:** tls
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name from **Section 5.3**  
i.e., **sm15018**
- **Near-end Listen Port:** 5061
- **Far-end Listen Port:** 5061
- **Far-end Network Region:** 1
- **DTMF over IP:** rtp-payload
- **Direct IP-IP Audio Connections:** y

```
add signaling-group 2                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 2                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
Q-SIP? n
IP Video? y                        Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr              Far-end Node Name: sm15018
Near-end Listen Port: 5061             Far-end Listen Port: 5061
                                     Far-end Network Region: 1

Far-end Domain:

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
                                     RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3 IP Audio Hairpinning? n
Enable Layer 3 Test? y              Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

## 5.5.2. Add Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** sip
- **Group Name:** A descriptive name (i.e., **sm15018**)
- **TAC:** An available trunk access code (i.e., **102**)
- **Service Type:** tie
- **Signaling Group:** The number of the signaling group associated (i.e., **2**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total trunks available from license verified in **Section 5.1**)

```
add trunk-group 2                                     Page 1 of 21
TRUNK GROUP
Group Number: 2                                     Group Type: sip          CDR Reports: y
Group Name: sm15018                                COR: 1                  TN: 1          TAC: 102
Direction: two-way                                Outgoing Display? n
Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                  Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 2
                                                Number of Members: 20
```

Navigate to **Page 3** and change **Numbering Format** to **private**. Use default values for all other fields.

```
add trunk-group 2                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment? n                                Measured: none
                                                Maintenance Tests? y

Numbering Format: private
                                                UI Treatment: service-provider
                                                Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                Hold/Unhold Notifications? Y
Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

## 5.6. Configure Route Patterns

Configure route patterns to correspond to the newly added SIP trunk group. Use the **change route pattern n** command, where **n** is an available route pattern.

The route pattern, as shown below, was configured to route calls to Session Manager and simulated PSTN endpoints.

### 5.6.1. Route Pattern for reaching Session Manager and Simulated PSTN Endpoints

When changing the route pattern, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name (i.e., **sm15018**)
- **Grp No:** The trunk group number from **Section 5.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive
- **No. Del Dgts:** **0** was entered to delete zero digits
- **Numbering Format:** This was set to **lev0-pvt** in the tested configuration

change route-pattern 2															Page 1 of 3		
Pattern Number: 2 Pattern Name: sm15018																	
SCCAN? n Secure SIP? n Used for SIP stations? n																	
Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC																	
No Mrk Lmt List Del Digits QSIG																	
Dgts Intw																	
1:	2	0													n	user	
2:															n	user	
3:															n	user	
4:															n	user	
5:															n	user	
6:															n	user	
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM Sub Numbering LAR																	
0 1 2 M 4 W Request Dgts Format																	
1:	y	y	y	y	y	n	n									lev0-pvt	none
2:	y	y	y	y	y	n	n										none
3:	y	y	y	y	y	n	n										none
4:	y	y	y	y	y	n	n										none
5:	y	y	y	y	y	n	n										none
6:	y	y	y	y	y	n	n										none

## 5.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration below, all calls originating from a **5**-digit extension (**Ext Len**) beginning with **5** (**Ext Code**) and routed through any trunk will result in a **5**-digit calling number (**Total Len**). The calling party number will be in the SIP “From” header.

change private-numbering 0					Page	1 of	2
NUMBERING - PRIVATE FORMAT							
Ext	Ext	Trk	Private	Total			
Len	Code	Grp(s)	Prefix	Len			
5	5			5	Total Administered: 1		
					Maximum Entries: 540		



## 5.8. Administer Dial Plan and AAR analysis

Configure the dial plan for dialing 5-digit extensions beginning with **5** to stations registered with Session Manager.

Use the **change aar analysis n** command, where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 5** (Extensions on Session Manager) to use **Route Pattern 2** (defined in Section 5.6). The **Call Type** was set to **lev0**.

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

## 5.9. Administer ARS Analysis

This section provides sample Auto Route Selection (ARS) used for routing calls with dialed digits beginning with **1303442** which correspond to numbers accessible via the Mediant 3000. Use the **change ars analysis 1303442** command and add an entry to specify how to route calls. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed digits to match on
- **Total Min:** Minimum number of digits, in this case **11**
- **Total Max:** Maximum number of digits, in this case **11**
- **Route Pattern:** The route pattern number from **Section 5.6**, i.e., **2**
- **Call Type:** hnpa

**Note:** The additional entries may be added for different number destinations.

change ars analysis 1303442							Page	1	of	2
ARS DIGIT ANALYSIS TABLE							Percent Full: 2			
Location: all										
	Dialed	Total		Route	Call	Node	ANI			
	String	Min	Max	Pattern	Type	Num	Reqd			
1303442		11	11	2	hnpa					

## 5.10. Administer Feature Access Code

Configure a feature access code to use for AAR and ARS routing. Use the **change feature access code** command to define **Access Code** for **Auto Alternate Routing (AAR)** and for **Auto Route Selection (ARS)**. In the test configuration, **8** and **9** were used respectively.

```
change feature-access-codes                                     Page 1 of 10
                                FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code:
Answer Back Access Code:
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
Automatic Callback Activation:                      Deactivation:
```

## 5.11. Save Changes

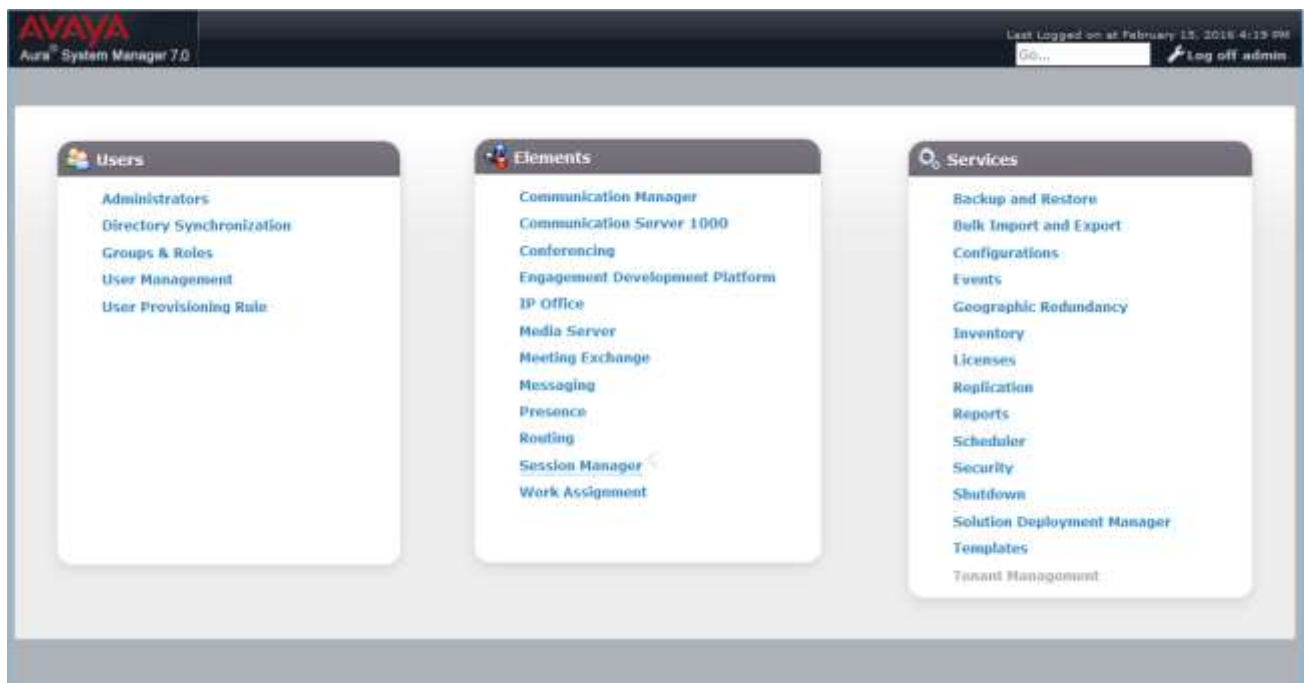
Use the **save translation** command to save all changes.

## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, assuming it has been installed and licensed as described in **Reference [2]**. The procedures include adding the following items:

- Specify SIP Domain
- Add Locations
- Add Adaptations
- Add SIP Entities and Entity Links
- Add Routing Policies
- Add Dial Patterns
- Add Users for SIP Phones

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. The home screen as shown below is displayed. Expand the **Routing** Link under **Elements**.



## 6.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Domains** on the left and clicking the **New** button on the right (not shown). The following screen will then be shown. Fill in the following fields and click **Commit**.

- **Name:** The authoritative domain name (e.g., **avaya.com**)
- **Type** Select **sip**
- **Notes:** Descriptive text (optional)

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', and a 'Log off admin' button. The left sidebar contains a menu with 'Routing' selected, and sub-items: 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Domain Management' and shows a table with one item: 'avaya.com' of type 'sip'. The table has columns for 'Name', 'Type', and 'Notes'. Below the table are 'Commit' and 'Cancel' buttons. The breadcrumb trail at the top of the main area reads 'Home / Elements / Routing / Domains'.

Name	Type	Notes
avaya.com	sip	

## 6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management. A single location is added to the configuration for Communication Manager and the Mediant 3000 Gateway. To add a location, select **Locations** on the left and click on the **New** button on the right (not shown). The following screen will then be shown. Fill in the following:

Under **General**:

- **Name:** A descriptive name

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location (optional). In these Application Notes, no pattern was defined.

Defaults can be used for the remaining fields. The screen below shows addition of the **Lab** location, which includes all the components of the compliance test environment. Click **Commit** to save.

The screenshot shows the Avaya System Manager 7.0 interface for configuring a location. The 'Location Details' page includes the following sections and fields:

- General:**
  - Name:** Lab
  - Notes:**
- Dual Plan Transparency in Survivable Mode:**
  - Enabled:** ☐
  - Listed Directory Number:**
  - Associated CM SIP Entity:**
- Overall Managed Bandwidth:**
  - Managed Bandwidth Units:** Kbit/sec
  - Total Bandwidth:**
  - Multimedia Bandwidth:**
  - Audio Calls Can Take Multimedia Bandwidth:** ☐
- Per-Call Bandwidth Parameters:**
  - Maximum Multimedia Bandwidth (Intra-Location):** 2000 Kbit/Sec
  - Maximum Multimedia Bandwidth (Inter-Location):** 2000 Kbit/Sec
  - Minimum Multimedia Bandwidth:** 64 Kbit/Sec
  - Default Audio Bandwidth:** 80 Kbit/Sec
- Alarm Threshold:**
  - Overall Alarm Threshold:** 30 %
  - Multimedia Alarm Threshold:** 80 %
  - Latency before Overall Alarm Trigger:** 5 Minutes
  - Latency before Multimedia Alarm Trigger:** 5 Minutes
- Location Pattern:**
  - Add** button
  - Remove** button
  - IP Address Pattern** table with **Notes** column

## 6.3. Add Adaptations

In order to maintain digit manipulation centrally on Session Manager, an adaptation module can be configured with a numbering plan offered from the PSTN Service Provider. To add an adaptation, select **Adaptations** on the left and click on the **New** button on the right. The following screen will then be shown. Fill in the following:

Under **General**:

- **Adaptation Name:** A descriptive name i.e., **ACM3000**
- **Module Name:** From the dropdown list select **DigitConversionAdapter**
- **Module Parameter Type:** Leave it blank

Under **Digit Conversion for Outgoing Calls From SM:**

- **Matching Pattern:** The dialed number to the simulated PSTN
- **Min/Max:** Minimum/Maximum number of digits
- **Delete Digits:** Digits to be deleted In this test the leading 4 digits for dialed numbers beginning with 1303442 were removed by Session Manager and sent to the Mediant 3000 to reach phone numbers that match 442xxxx.
- **Insert Digits:** Digit to be added
- **Address to modify:** Select **destination**

The screen below is the Adaptation detail page. Click **Commit** to save the changes.

The screenshot displays the 'Adaptation Details' page in the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options like Routing, Domains, Locations, Adaptations, SIP Trunks, Entity Links, Hunt Groups, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Adaptation Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Adaptation Name' is set to 'ACM3000', the 'Module Name' is 'DigitConversionAdapter', and the 'Module Parameter Type' is blank. Below this, there are sections for 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM'. The 'Outgoing Calls' section features a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. A single row is shown with Matching Pattern '1303442', Min '7', Max '12', and Address to modify set to 'destination'. The page also includes a 'Filter: Enable' button and a 'Select: All, None' option at the bottom.

Additionally an Adaptation was used between Session Manager and Communication Manager to replace the domain in various SIP Headers with avaya.com when communicating with Communication Manager.

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations (selected), SIP Endpoints, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Adaptation Details' and includes a 'General' tab. The 'Adaptation Name' is 'CM Adapter' and the 'Module Name' is 'DigitConversionAdapter'. The 'Module Parameter Type' is 'Name-Value Parameter'. Below this, there is a table with columns 'Name' and 'Value'. The table contains two entries: 'local' with value 'avaya.com' and 'remote' with value 'testlab.com'. Below the table, there are fields for 'Egress URI Parameters' and 'Notes'. At the bottom, there are two sections for 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM', each with a table for 'Matching Patterns' and columns for 'Min', 'Max', 'Phone Context', 'Delete Digits', 'Insert Digits', 'Addresses to modify', 'Adaptation Data', and 'Notes'. The interface also includes 'Commit' and 'Cancel' buttons at the top right and bottom right.

## 6.4. Add SIP Entities and SIP Entity Links

A SIP Entity is required for each SIP-based telephony system wishing to communicate with Session Manager for call routing. In the sample configuration, a SIP Entity and SIP Entity Link is added for Communication Manager, and the Mediant 3000.

### 6.4.1. Adding Avaya Aura® Communication Manager SIP Entity and SIP Entity Link

Navigate to **Network Routing Policy → SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name, i.e., **cm15014**
- **FQDN or IP Address:** IP address of the Communication Manager i.e., **10.64.150.14**
- **Type:** Select **CM**
- **Adaptation:** Select **CM Adapter**
- **Location:** Select one of the locations defined previously
- **Time Zone:** Time zone for this entity

Add Entity Links. Under **Entity Links**, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Name:** Will be populated automatically
- **SIP Entity 2:** Will be populated automatically with the name of this SIP Entity.
- **SIP Entity 1:** Select Session Manager from the pull down box
- **Protocol:** Select the desired Protocol from the pull down box
- **Port:** Enter the desired port number for the Entity Link
- **Policy:** Select the appropriate Connection Policy from the pull down box

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the addition of the SIP Entity for Communication Manager.



25 of 79  
AC\_M3KE1\_CMSM70

### 6.4.2. Adding AudioCodes Mediant 3000 Gateway SIP Entity

Navigate to **Network Routing Policy** → **SIP Entities** on the left and click on the **New** button on the right (not shown).

Under **General**:

- **Name:** A descriptive name, i.e., **ACM3000**
- **FQDN or IP Address:** IP address of the Mediant 3000 i.e., **10.64.50.199**
- **Type:** Select **Gateway**
- **Adaptation:** Select **ACM3000**. This was configured in **Section 6.3**
- **Location:** Select one of the locations defined previously
- **Time Zone:** Time zone for this entity
- **SIP Link Monitoring:** Use **Session Manager Configuration**

Add Entity Links. Under **Entity Links**, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Name:** Will be populated automatically
- **SIP Entity 2:** Will be populated automatically with the name of this SIP Entity.
- **SIP Entity 1:** Select Session Manager from the pull down box
- **Protocol:** Select the desired Protocol from the pull down box
- **Port:** Enter the desired port number for the Entity Link
- **Policy:** Select the appropriate Connection Policy from the pull down box

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition. The following screen shows the addition of the SIP Entity for Mediant 3000.



## 6.5. Add Routing Policies

Routing policies describe the condition under which calls will be routed to the SIP Entities specified in **Section 6.4**. A routing policy must be added for Communication Manager and the Mediant 3000 Gateway. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

### Under **General**

- Enter a descriptive **Name**

### Under **SIP Entity as Destination**

- Click **Select**, and then select the appropriate SIP entity to which this routing policy applies

### Under **Time of Day:**

- Click **Add**, and select the time range configured. In these Application Notes, the predefined **24/7** Time Range is used

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screens show the Routing Policies for Communication Manager and the Mediant 3000. Note that **Dial Patterns** (to be configured in **Section 6.6**), when configured, will be automatically displayed in the **Routing Policy Details** page.





## 6.6. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration numbers beginning with **5** with 5-digit length reside in the Enterprise network. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right (not shown). Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Communication Manager.

Under **General**:

- **Pattern:** Dialed number or prefix i.e., **5**
- **Min:** Minimum length of dialed number i.e., **5**
- **Max:** Maximum length of dialed number i.e., **5**
- **SIP Domain:** Select **ALL**

Under **Originating Locations and Routing Policies**, click **Add**, and then select the appropriate location and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.

The following screen shows the dial pattern definition for calls within the Enterprise.

The screenshot displays the Avaya Aura System Manager 7.0 interface for defining a dial pattern. The left sidebar shows the navigation menu with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and contains two sections: 'General' and 'Originating Locations and Routing Policies'. The 'General' section includes fields for Pattern (5), Min (5), Max (5), Emergency Call (unchecked), Emergency Priority (1), Emergency Type, SIP Domain (ALL), and Notes. The 'Originating Locations and Routing Policies' section includes an 'Add' button, a table with columns for Originating Location Name, Originating Location Note, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The table shows one entry with Originating Location Name '-ALL-', Originating Location Note 'cmcm704', Rank '1', Routing Policy Disabled '0', Routing Policy Destination 'cmcm704', and Routing Policy Notes. Below the table is a 'Select: All None' button. The 'Denied Originating Locations' section includes an 'Add' button, a table with columns for Originating Location and Notes, and a 'Filter: Enable' button. The table shows one entry with Originating Location 'cmcm704' and Notes. At the bottom of the form are 'Commit' and 'Cancel' buttons.

The following screen shows the dial pattern definition for calls destined for the Mediant 3000.

**Avaya**  
Aura System Manager 7.0

Test logged on at February 18, 2016 4:19 PM  
[User] [Log off Admin]

Home / Elements / Routing / Dial Patterns

### Dial Pattern Details

Commit Cancel

**General**

\* Pattern: 1303442  
\* Min: 7  
\* Max: 11  
Emergency Call: ☐  
Emergency Priority: 1  
Emergency Type:   
SIP Domain: -all-  
Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Lab		ACH3000	6	<input type="checkbox"/>	ACH0000	

Select: All, none

**Denied Originating Locations**

Add Remove

0 Items Filter: Enable

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

Commit Cancel



## 6.7. Add Users for SIP Phones

From the home screen select **Users** → **User Management** → **Manage Users** to display the **User Management** screen (not shown). Click **New** to add a user.

### 6.7.1. Identity

The **New User Profile** screen is displayed. Enter desired **Last Name** and **First Name**. For **Login Name**, enter “n@z”, where “n” is the user extension and “z” is the domain name, in this case “avaya.com” used for compliance testing. Retain the default values in the remaining fields.

The screenshot displays the Avaya System Manager 7.0 interface. The top navigation bar includes 'Home', 'User Management', and a 'Help' link. The left sidebar lists various management options: 'User Management', 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The main content area is titled 'New User Profile' and features four tabs: 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is selected, showing a form with the following fields and values:

- User Provisioning Rule:** A dropdown menu with 'Basic' selected.
- Identity:**
  - Last Name:** 53101
  - Last Name (Latin Translation):** 53101
  - First Name:** Station
  - First Name (Latin Translation):** Station
  - Middle Name:** (empty)
  - Description:** (empty)
  - Login Name:** 53101@avaya.com
  - User Type:** Basic

## 6.7.2. Communication Profile

Select the **Communication Profile** tab. For **Communication Profile Password** and **Confirm Password**, enter the desired password for the SIP user to use for registration. Scroll down to the **Communication Address** sub-section, and click **New** to add a new address.

For **Type**, retain “Avaya SIP”. For **Fully Qualified Address**, enter and select the SIP user extension and domain configured in **Section 6.7.1**. Click **Add**.

Scroll down to check and expand **Session Manager Profile**. For **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence**, and **Home Location**, select the values corresponding to the applicable Session Manager. Retain the default values in the remaining fields. These settings are configured during the initial setup of Session Manager.

Scroll down to check and expand **CM Endpoint Profile**. For **System**, select the value corresponding to the applicable Communication Manager. For **Extension**, enter or select the SIP user extension configured in **Section 6.7.1**. For **Template**, select corresponding Telephone type. Retain the default values in the remaining fields.

Click **Commit** to complete the creation of the new user.

35 of 79  
AC M3KE1 CMSM70

## 7. AudioCodes Mediant 3000 Configuration

This section describes the configuration for enabling the Mediant 3000 to interoperate with Session Manager. The procedures require five distinct operations:

- Configuring the Media Gateway Host IP Network Parameters
- Configuring the Media Gateway TDM and Timing Parameters
- Configuring the Media Gateway Media Settings
- Configuring the Media Gateway Telephony/PSTN Interfaces Parameters
- Configuring the Media Gateway SIP Protocol Parameters

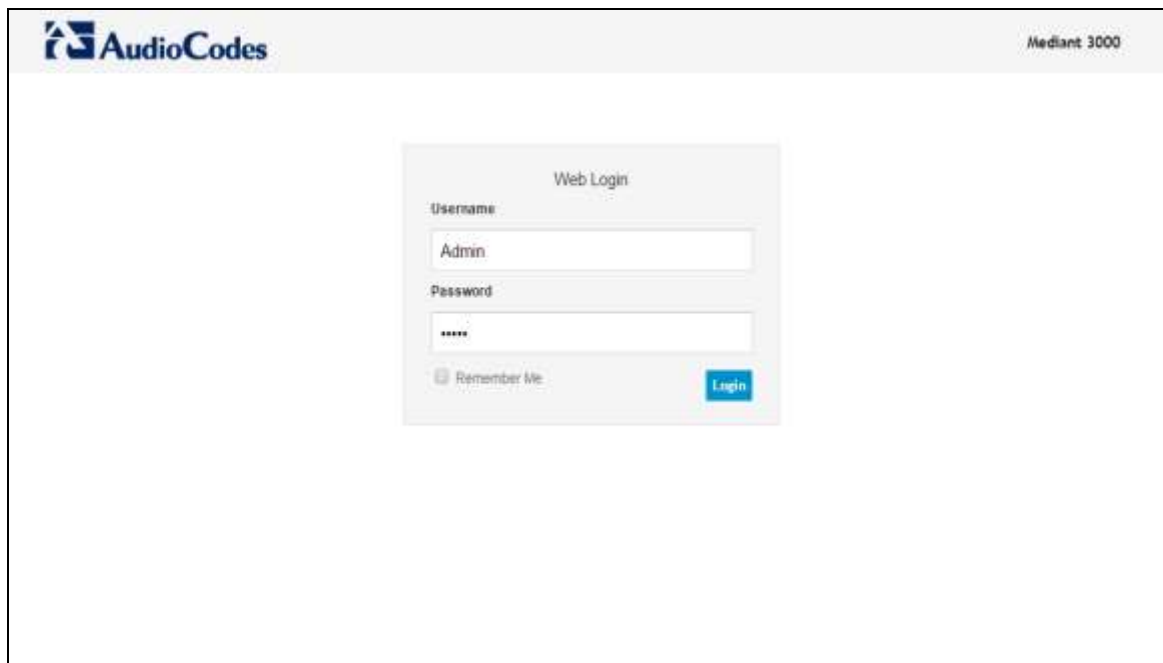
The Mediant 3000 can be administered using the Native Web Interface or AudioCodes Element Management System (EMS) as described in **Reference [3]**. Note that this section displays the provisioning that was utilized for this sample configuration, and does not show exhaustive procedures for administering an initial configuration. In these Application Notes, configuration was accomplished with the web interface.

### 7.1. Log Into Mediant 3000

The configuration of the Mediant 3000 Gateway is done via a Web browser. To access the device, enter the **IP address** of the Mediant 3000 in the **Address** field of the web browser. The IP address was provisioned during initial installation.

#### Login credentials

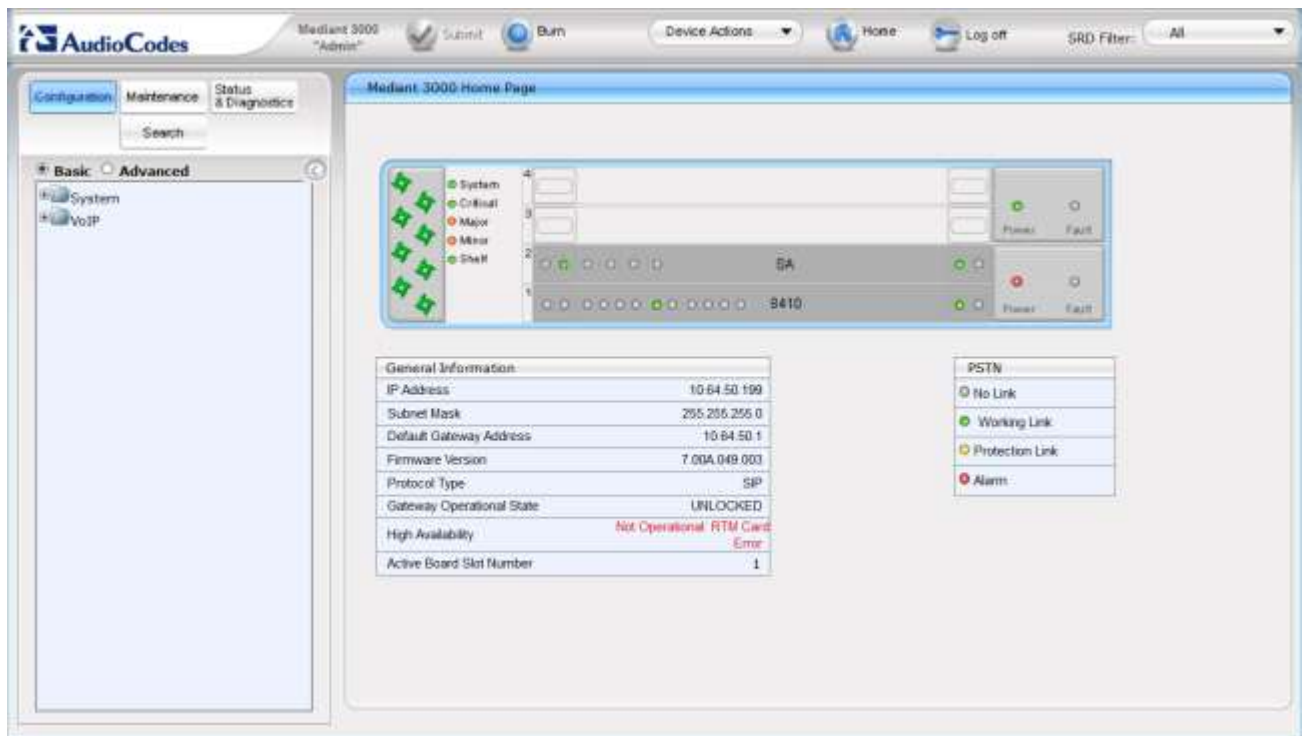
The following pop-up window will appear. Log in with the proper credentials.



The screenshot shows the AudioCodes Mediant 3000 Web Login interface. At the top left is the AudioCodes logo, and at the top right is the text "Mediant 3000". The main content area is a light gray box titled "Web Login". Inside this box, there are two input fields: "Username" with the value "Admin" and "Password" with masked characters "\*\*\*\*\*". Below the password field is a checkbox labeled "Remember Me" and a blue "Login" button.

## Mediant 3000 Home Page

The Mediant 3000 Home Page will appear as shown below.



## 7.2. Configure Media Gateway IP Network Parameters

To configure the network parameters, navigate to **VoIP → Network → IP Interfaces Table** and click on the **Add** button to add an index with **Application Type** of **OAMP + Media + Control** and ensure the **Interface Mode** is set to **IPv4 Manual** and that **IP Address** (i.e., **10.64.50.199**), **Prefix Length** (i.e., **24**), and **Default Gateway** (i.e., **10.64.50.1**) are set according to the expected values.

The screenshot displays the AudioCodes Mediant 300 configuration web interface. The left sidebar shows a navigation tree with 'Basic' and 'Advanced' tabs. Under 'Advanced', the 'Network' section is expanded, showing 'IP Interfaces Table' as the selected option. The main panel, titled 'Interface Table', contains a table with the following data:

Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS
0	if 0	OAMP + Media + Control	IPv4 Manual	10.64.50.199	24	10.64.50.1	0.0.0.0	0.0.0.0

Below the table, the 'Selected Row #0' details are shown:

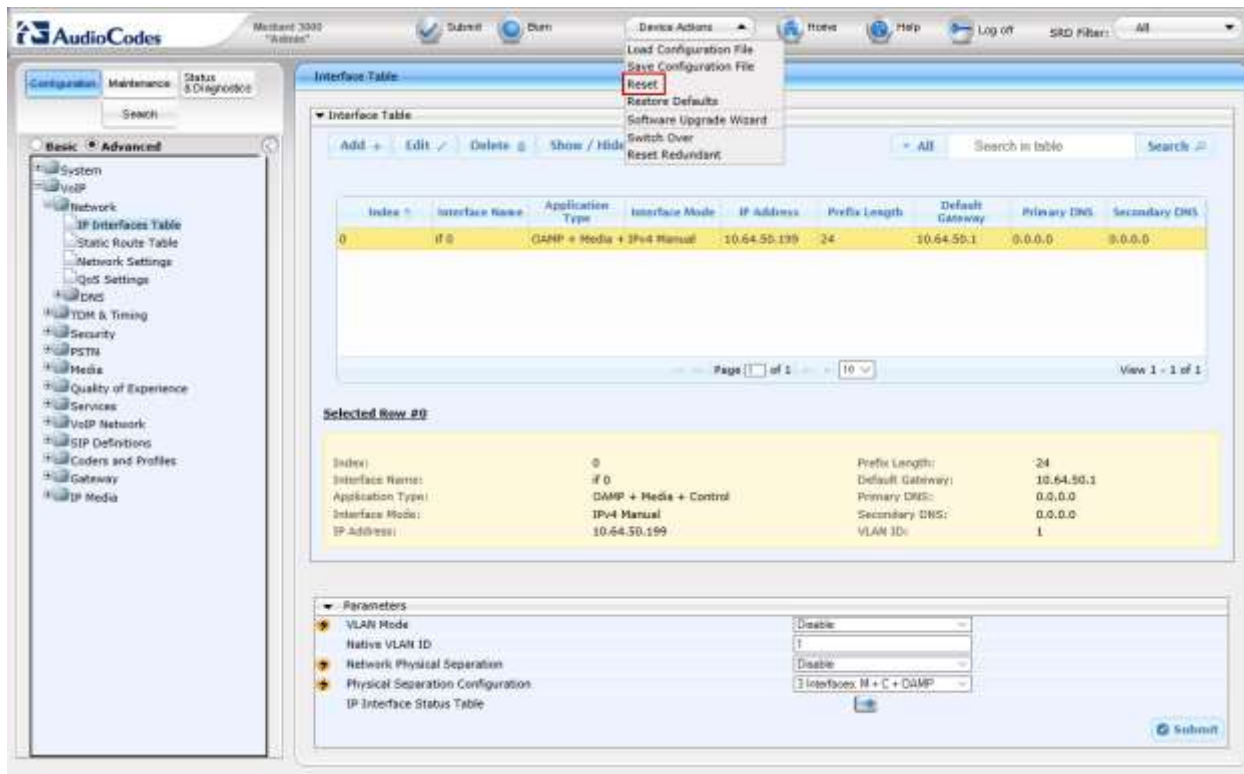
Index:	0	Prefix Length:	24
Interface Name:	if 0	Default Gateway:	10.64.50.1
Application Type:	OAMP + Media + Control	Primary DNS:	0.0.0.0
Interface Mode:	IPv4 Manual	Secondary DNS:	0.0.0.0
IP Address:	10.64.50.199	VLAN ID:	1

At the bottom, the 'Parameters' section includes dropdown menus for 'VLAN Mode' (set to 'Disable'), 'Native VLAN ID' (set to '1'), 'Network Physical Separation' (set to 'Disable'), and 'Physical Separation Configuration' (set to 'Interfaces: N + C = OAMP'). A 'Submit' button is located at the bottom right of the configuration area.

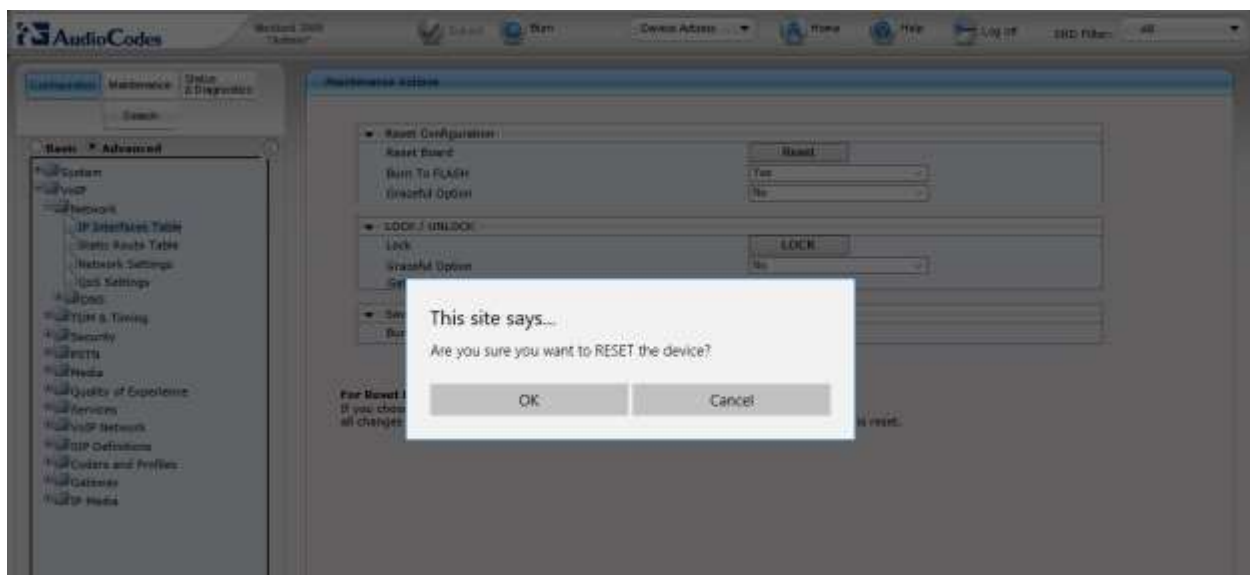
### 7.2.1. Saving Configuration and Resetting Mediant 3000

Save settings to the device's flash memory and reset the device by performing the following:

From the **Device Actions** pull-down menu, click **Reset** to display the **Maintenance Actions** screen.



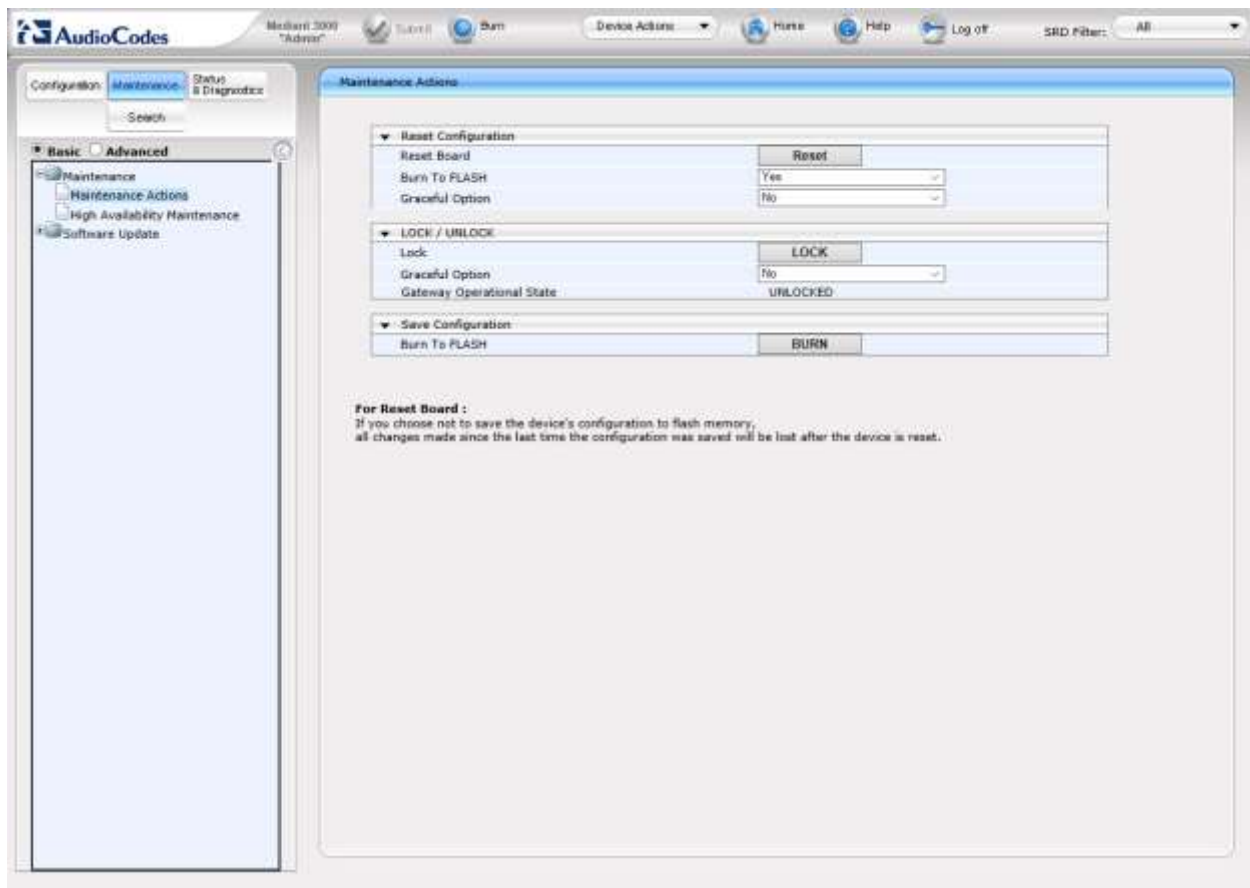
Make sure **Burn To FLASH** is set to **Yes**, and then click the **Reset** button then click **OK** for confirmation. The device's new configuration is saved (burned) to the flash memory and the device resets.



**Note:** if any parameter with the lightening symbol beside it (see the screenshot is **Section 7.4.1** for example) is changed, a Reset with Burn To Flash is required. The reset does not have to be done until all configuration is completed, and there will be a red reset notification at the top of the page (not shown).

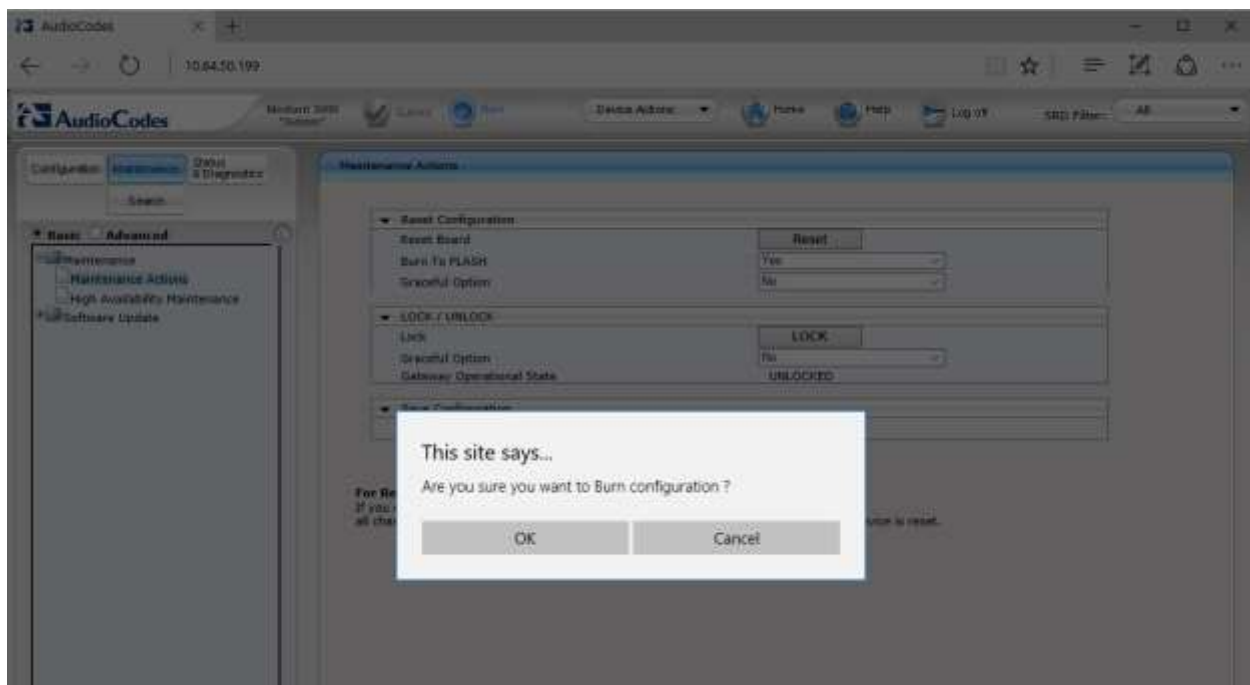
### 7.3. Saving Configuration

To permanently save settings to the device's flash memory, activate the **Maintenance Actions** page (**Maintenance** tab → **Maintenance** → **Maintenance Actions**) and click the **BURN** button under **Save Configuration** as shown below.



Also note the **Burn** button at the top of the screen. This is the shortest path to do a burn and can be used at any time. When clicked, it will present a pop-up similar to the one shown below.

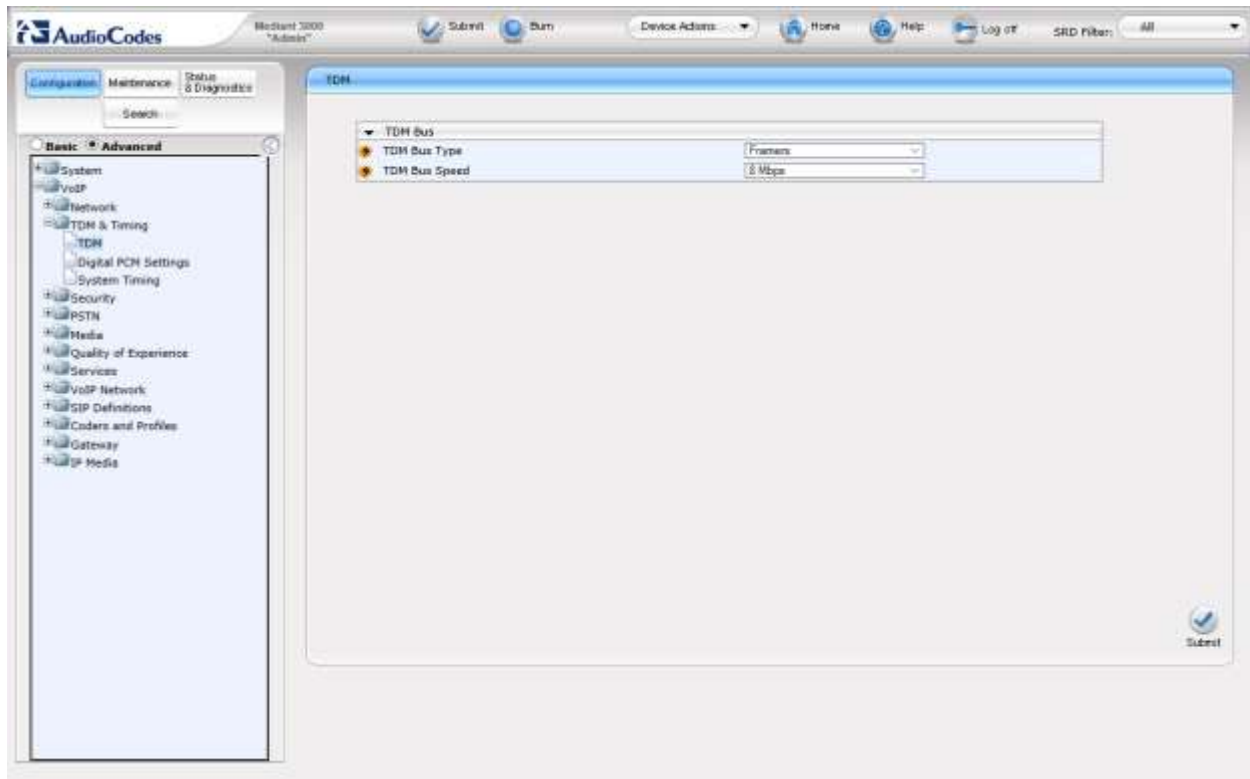




## 7.4. Configure Media Gateway TDM and Timing Parameters

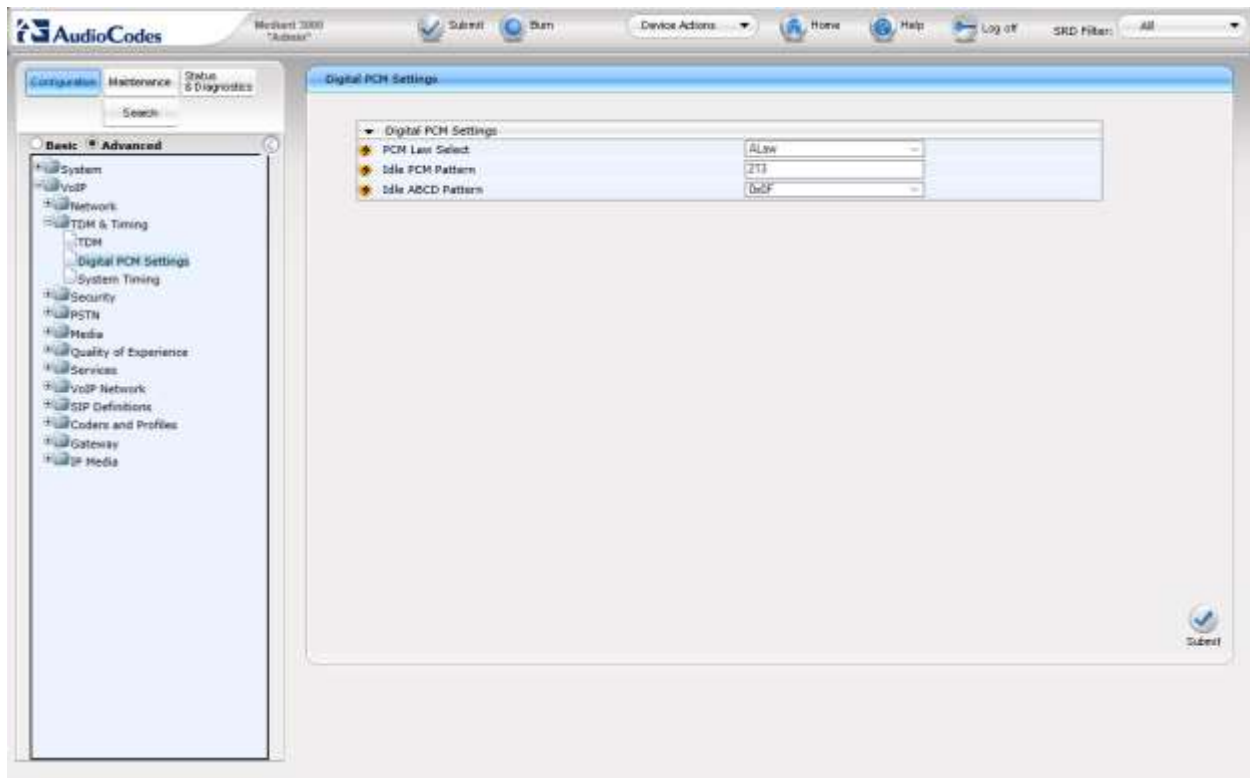
### 7.4.1. Configure TDM Bus

To configure the TDM Bus settings, open the **TDM** page (**Configuration** tab → **VoIP** → **TDM & Timing** → **TDM**), configure **TDM Bus Type** and **TDM Bus Speed** parameters as required. For E1 set **TDM Bus Type** to **Framers** and **TDM Bus speed** to **8Mbps**. Click the **Submit** button to save changes.



## 7.4.2. Configure Digital PCM Settings

To configure the digital PCM settings, open the **Digital PCM Settings** page (**Configuration** tab → **VoIP** → **TDM & Timing** → **Digital PCM Settings**). Configure the parameters as required, i.e., **ALaw** for **PCM Law Select** for E1 and click the **Submit** button to save changes.



### 7.4.3. Configure System Timing

To configure the device's system timing, open the **System Timing** page (**Configuration** tab → **VoIP** → **TDM & Timing** → **System Timing**). Configure the parameters as required. Click the **Submit** button to save changes. The screen below illustrates the configuration of system timing where the Mediant 3000 is configured as Master Clock Source as used in these Application Notes.

The screenshot displays the AudioCodes Mediant 3000 configuration interface. The left sidebar shows the navigation tree with 'System Timing' selected under 'VoIP' > 'TDM & Timing'. The main panel is titled 'System Timing' and contains the following configuration sections:

- Mode:**
  - Timing Module Mode: Slave/None
- Clock Parameters:**
  - TDM Bus Clock Source: Internal
  - TDM Bus Enable Fallback: Manual
  - TDM Bus Fallback Clock Source: Network
  - TDM Bus Clock Reference: 1
  - PLL Out Of Range: DCR 9.2 to 12 ppm
  - TDM Bus Master-Slave Selection: Slave/Mode
  - TDM Bus Net Reference Speed: 8kHz
  - TDM Bus Local Reference: 1
  - TDM Bus PSTN Auto Fallback Clock: Disable
  - TDM Bus PSTN Auto Clock Reverting: Disable
- Timing Module:**
  - Reference Validation Time: 1
  - External Interface Type: E1\_120K
  - Loopback External Ref 1: Disable
  - Loopback External Ref 2: Disable

A 'Submit' button is located at the bottom right of the configuration area.

## 7.5. Configure Media Gateway Media Settings

The Media Settings of the Mediant 3000 Media Gateway can be configured using the web interface.

### 7.5.1. Configure the Voice parameters

Open the **Voice Settings** page (**Configuration** tab → **VoIP** → **Media** → **Voice Settings**). Set **DTMF Transport Type** to **RFC2833 Relay DTMF** as shown below, and click the **Submit** button to save changes.

The screenshot displays the AudioCodes Mediant 3000 web interface. The left sidebar shows a navigation tree with categories like System, VoIP, Network, and Media. The 'Media' category is expanded, showing 'Voice Settings' as the selected option. The main content area is titled 'Voice Settings' and contains two expandable sections. The 'Voice Settings' section is expanded, showing a list of parameters with their current values and dropdown menus for selection. The 'Acoustic Echo Suppressor Settings' section is also expanded, showing a list of parameters with their current values and dropdown menus for selection. A 'Submit' button is located at the bottom right of the page.

Voice Settings	
Voice Volume (-32 to 31 dB)	0
Input Gain (-32 to 31 dB)	0
Silence Suppression	Disable
DTMF Transport Type	RFC 2833 Relay DTMF
DTMF Volume (-31 to 0 dB)	-11
NTE Max Duration	-1
CAS Transport Type	CAS Events Only
DTMF Generation Twist	0
Echo Canceller	Enable

Acoustic Echo Suppressor Settings	
Network Echo Suppressor Enable	Disable
Echo Canceller Type	Low echo canceller
Attenuation Intensity	0
Max ERL Threshold - dB	0
Min Reference Delay x10 msec	0
Max Reference Delay x10 msec	40

## 7.5.2. Configure the Fax Parameters

To configure FAX support, open the **Fax/Modem/CID Settings** page (**Configuration** tab → **VoIP** → **Media** → **Fax/Modem/CID Settings**). Set the following values:

- **Fax Transport Mode:**      **T.38 Relay**
- **Fax Relay Max Rate:**      **Based on T38 version**

Click the **Submit** button to save changes. The screen below illustrates the Fax settings on the Mediant 3000.

The screenshot shows the AudioCodes Mediant 3000 configuration interface. The left sidebar contains a tree view with categories: Basic, Advanced, and Search. Under the Advanced category, the following settings are listed: System, VoIP, Network, TDM & Timing, Security, PSTN, Media, Voice Settings, Fax/Modem/CID Settings (selected), RTP/RTCP Settings, IPMedia Settings, General Media Settings, DSP Templates, AMR Policy Management, Media Security, Quality of Experience, Services, VoIP Network, SIP Definitions, Coders and Profiles, Gateway, and SIP Media. The main content area displays the Fax/Modem/CID Settings page, which is divided into three sections: General Settings, Fax Relay Settings, and Bypass Settings. The General Settings section includes: Fax Transport Mode (T.38 Relay), Caller ID Transport Type (Mute), Caller ID Type (Standard Bellcore), V.21 Modem Transport Type (Disable), V.22 Modem Transport Type (Disable), V.23 Modem Transport Type (Disable), V.32 Modem Transport Type (Disable), V.34 Modem Transport Type (Disable), Fax CHG Mode (Doesn't send T.38 re-INVITE), CHG Detector Mode (Disable), and CED Transfer Mode (Fax Relay or VBD). The Fax Relay Settings section includes: Fax Relay Redundancy Depth (0), Fax Relay Enhanced Redundancy Depth (4), Fax Relay ECH Enable (Enable), Fax Relay Max Rate (Based on T38 version), and T.38 Version (T.38 version 0). The Bypass Settings section includes: Fax/Modem Bypass Codec Type (G711A law 64), Fax/Modem Bypass Packing Factor (1), Fax Bypass Output Gain (0), and Modem Bypass Output Gain (0). A Submit button is located at the bottom right of the page.

Section	Setting	Value
General Settings	Fax Transport Mode	T.38 Relay
	Caller ID Transport Type	Mute
	Caller ID Type	Standard Bellcore
	V.21 Modem Transport Type	Disable
	V.22 Modem Transport Type	Disable
	V.23 Modem Transport Type	Disable
	V.32 Modem Transport Type	Disable
	V.34 Modem Transport Type	Disable
	Fax CHG Mode	Doesn't send T.38 re-INVITE
	CHG Detector Mode	Disable
CED Transfer Mode	Fax Relay or VBD	
Fax Relay Settings	Fax Relay Redundancy Depth	0
	Fax Relay Enhanced Redundancy Depth	4
	Fax Relay ECH Enable	Enable
	Fax Relay Max Rate (bps)	Based on T38 version
	T.38 Version	T.38 version 0
Bypass Settings	Fax/Modem Bypass Codec Type	G711A law 64
	Fax/Modem Bypass Packing Factor	1
	Fax Bypass Output Gain	0
	Modem Bypass Output Gain	0

### 7.5.3. Configure the RTP/RTCP Parameters

Verify and configure RTP parameters by opening the **RTP/RTCP Settings** page (**Configuration** tab → **VoIP** → **Media** → **RTP / RTCP Settings**). Configure the settings as shown below, then click the **Submit** button to save changes. The figure below illustrates settings used for the compliance test.

The screenshot shows the AudioCodes Mediant 3000 'Admin' interface. The left sidebar contains a navigation tree with the following structure:

- Basic
- Advanced
  - System
  - VoIP
  - Network
  - TDM & Timing
  - Security
  - PSTN
  - Media
    - Voice Settings
    - Fax/Modem/CID Settings
    - RTP/RTCP Settings (selected)
    - IPMedia Settings
    - General Media Settings
    - DSP Templates
    - JMR Policy Management
    - Media Security
  - Quality of Experience
  - Services
  - VoIP Network
  - SIP Definitions
  - Coders and Profiles
  - Gateway
  - IP Media

The main panel displays the 'RTP/RTCP Settings' page. It contains three sections:

- General Settings**

Parameter	Value	Icon
Dynamic Jitter Buffer Minimum Delay	10	
Dynamic Jitter Buffer Optimization Factor	10	
RTP Redundancy Depth	0	
Packing Factor	1	✓
RPC 2833 TX Payload Type	101	
RPC 2833 RX Payload Type	96	
RFC 2198 Payload Type	104	
Fax Bypass Payload Type	102	
Modem Bypass Payload Type	103	
Enable RFC 3389 CN Payload Type	Enable	
Comfort Noise Generation Negotiation	Enable	✓
Remote RTP Base UDP Port	0	
RTP Multiplexing Local UDP Port	0	✓
RTP Multiplexing Remote UDP Port	0	✓
RTP Base UDP Port	6000	
- RTP XR Settings**

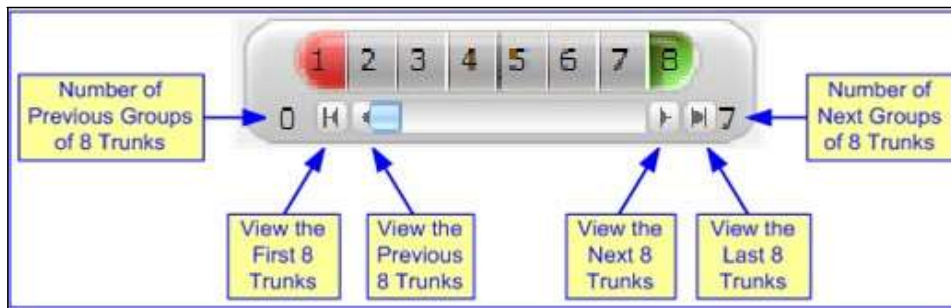
Parameter	Value	Icon
Enable RTP XR	Disable	
Burst Threshold	-1	✓
Delay Threshold	-1	✓
R-Value Delay Threshold	-1	✓
Minimum Gap Size	16	✓
RTP XR Packet Interval	0	
Disable RTP XR Interval Randomization	Disable	
- RTP XR Setting - SIP Collection**



Parameter	Value	Icon
Gateway RTP XR Report Mode	Disable	
RTP XR Collection Server		
RTP XR Collection Server Transport Type	Not Configured	

A 'Submit' button is located at the bottom right of the main panel.

## 7.6. Configure Media Gateway Telephony/PSTN Interface Parameters

Open the **Trunk Settings** page (**Configuration** tab → **VoIP** → **PSTN** → **Trunk Settings**). Select the trunk to be configured, by clicking the desired Trunk number icon in the right pane. The bar initially displays the first eight trunk number icons (i.e., trunks 1 through 8). To scroll through the trunk number icons (i.e., view the next/last or previous/first group of eight trunks), refer to the figure below:

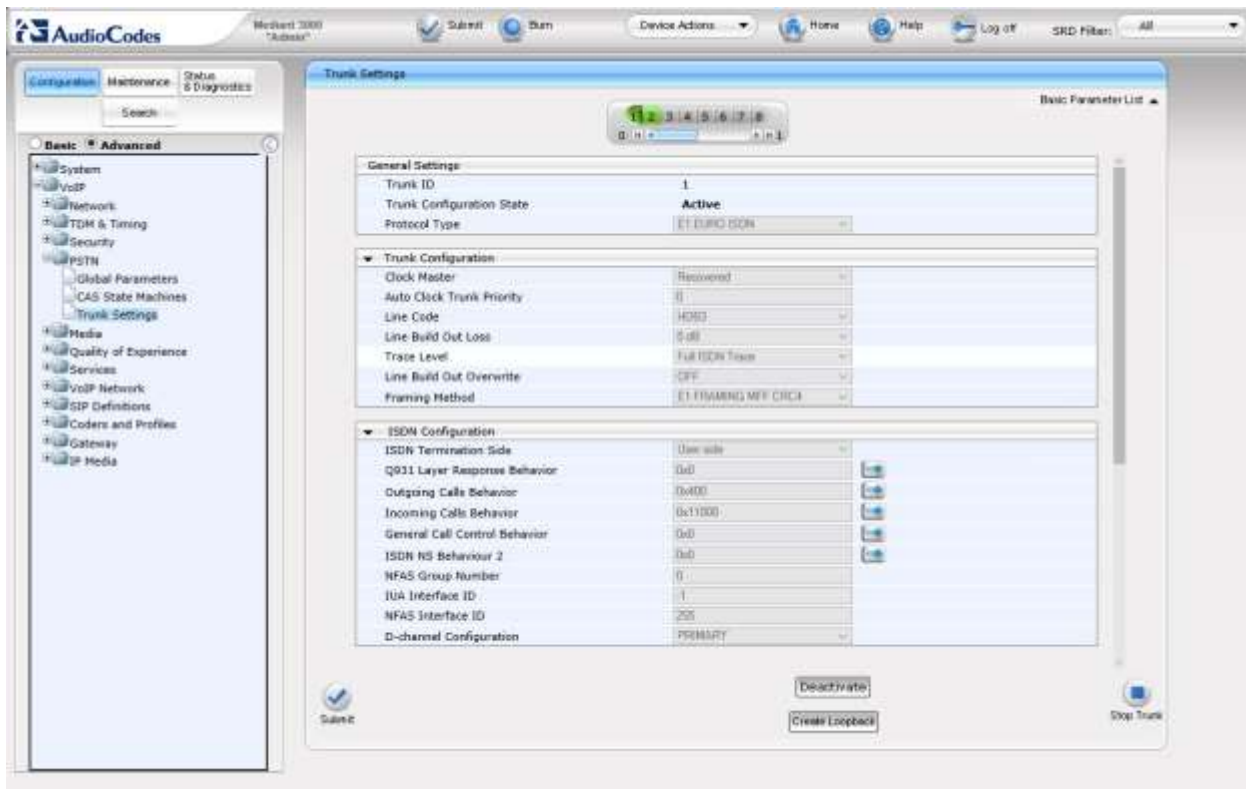


Click the **Stop Trunk**  button (located at the bottom of the page) to take the trunk out of service to allow configuration of the currently grayed out (unavailable) parameters. (Skip this step to configure parameters that are available when the trunk is active). The stopped trunk is indicated by the **Trunk Configuration State** field displaying **Inactive**. The **Stop Trunk** button is replaced by the **Apply Trunk Settings**  button.

In these Application Notes the PSTN interface was configured as follows:

- |                                 |                             |
|---------------------------------|-----------------------------|
| • <b>Protocol Type:</b>         | <b>E1 EURO ISDN</b>         |
| • <b>Line Code:</b>             | <b>HDB3</b>                 |
| • <b>Framing Method:</b>        | <b>E1 FRAMINIG MFF CRC4</b> |
| • <b>ISDN Termination Side:</b> | <b>User side</b>            |





### 7.6.1. Configure Trunk Group Table

Open the **Trunk Group Table** page (**Configuration** tab → **VoIP** → **Gateway** → **Trunk Group** → **Trunk Group**). Select the appropriate **Group Index**, and set the appropriate parameters in the table, i.e., **From /To Trunk**, **Channels**, **Phone Number**, **Trunk Group ID**, **Tel Profile ID**. For detailed information refer to [3]. Click the **Submit** button to save changes. The screen below illustrates setting used for the compliance test.

**Trunk Group Table**

Add Phone Context As Prefix:

Trunk Group Index:

Group Index	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	1	1	1-31	4421000	1	None
2	2	2	1-31	4422000	2	None
3						None
4						None
5						None
6						None
7						None
8						None
9						None
10						None

## 7.7. Configure SIP Protocol Parameters

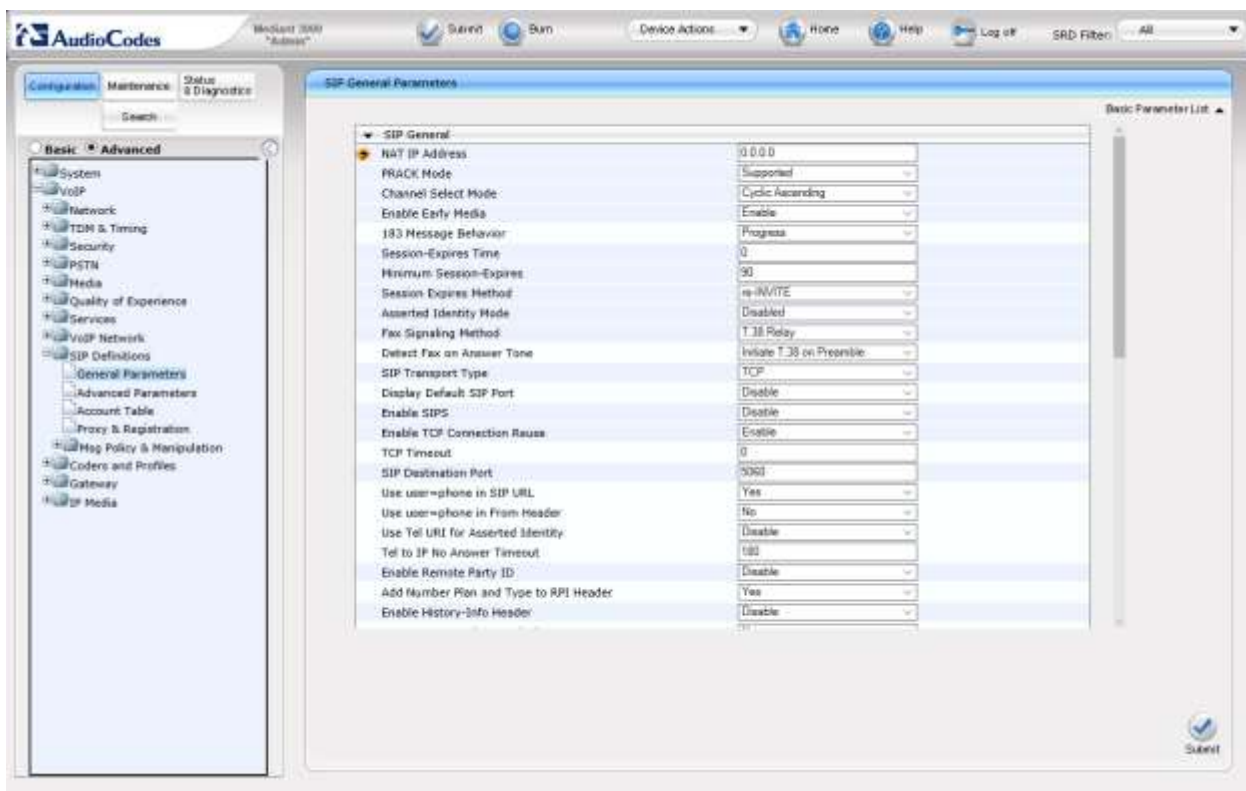
The SIP protocol interface is configured through a series of configuration steps.

### 7.7.1. Configure General SIP Protocol Parameters

Open the **SIP General Parameters** page (**Configuration** tab → **VoIP** → **SIP Definitions** → **General Parameters**). Set the following values:

- **Enable Early Media:** **Enable**
- **Fax Signaling Method:** **T.38 Relay**
- **SIP Transport Type:** Align with setting in the entity link definition on Session Manager for the Mediant 3000, i.e. **TCP**
- **Use Tel URI for Asserted Identity:** Set to **Disable**

Click the **Submit** button to save changes. The figure below illustrates the **SIP General Parameters** page.



### 7.7.2. Configure DTMF and Dialing Parameters

Open the **DTMF & Dialing** page (**Configuration** tab → **VoIP** → **Gateway** → **DTMF and Supplementary** → **DTMF & Dialing**). Set the following values:

- **Declare RFC 2833 in SDP:**       **Yes**
- **1<sup>st</sup> Tx DTMF Option:**       **RFC 2833**

Click the **Submit** button to save changes. The figure below illustrates the **DTMF & Dialing** page.

Parameter	Value
Max Digits In Phone Num	30
Inter Digit Timeout for Overlap Dialing [sec]	4
Declare RFC 2833 in SDP	Yes
1st Tx DTMF Option	RFC 2833
2nd Tx DTMF Option	
RFC 2833 Payload Type	101
Hook-Flash Option	Not Supported
Digit Mapping Rules	
Dial Plan Index	-1
Min Routing Overlap Digits	1
ISDN Overlap IP-to-Tel Dialing	Disable
Default Destination Number	1000
Special Digit Representation	Special

### 7.7.3. Configure Proxy & Registration Parameters

Open the **Proxy & Registration** page (**Configuration** tab → **VoIP** → **SIP Definitions** → **Proxy & Registration**). Ensure that **Use Default Proxy** is set to **No** and **Enable Registration** is set to **Disable**. Click the **Submit** button to save changes. The screen below displays the **Proxy & Registration** page for the system used for the compliance test.

Proxy & Registration	
Use Default Proxy	No
Proxy Name	
Redundancy Mode	Primary
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Always Use Proxy	Disable
Redundant Routing Mode	Routing Table
SIP Routing Mode	Standard Mode
Gateway Name	
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Password
Challenge	Default_Challenge
Authentication Mode	Per Gateway
Challenge Caching Mode	None
Mutual Authentication Mode	Optional
Use Proxy IP as Host	Disable
Max Generated Register Rate	150
Enable Registration	Disable

Register Un-Register  
Submit

### 7.7.4. Configure Device's Coders

Open the **Coders** page (**Configuration** tab → **VoIP** → **Coders and Profiles** → **Coders**).

- From the **Coder Name** drop-down list, select the required coder
- From the **Packetization Time** drop-down list, select the packetization time (in msec) for the selected coder. The packetization time determines how many coder payloads are combined into a single RTP packet
- From the **Rate** drop-down list, select the bit rate (in kbps) for the selected coder
- In the **Payload Type** field, if the payload type (i.e., format of the RTP payload) for the selected coder is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified)
- From the **Silence Suppression** drop-down list, enable or disable the silence suppression option for the selected coder
- Repeat **Step 2** through **Step 6** for the next optional coders

Click the **Submit** button to save changes. The following screen presented the codecs configured for the compliance test.

The screenshot shows the AudioCodes Mediant 3000 'Admin' interface. The main window displays the 'Coders Table' configuration page. The table has the following columns: Coder Name, Packetization Time, Rate, Payload Type, Silence Suppression, and Coder Specific. The table contains three rows of data:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711u-law	20	64	0	Disabled	
G.711u-law	20	64	0	Disabled	
G.729	20	8	10	Disabled	

The left sidebar shows a navigation tree with 'Coders' selected under 'VoIP'. The 'Submit' button is visible in the bottom right corner of the main window.

### 7.7.5. Configure Advanced General Protocol Parameters

Open the **Advanced Parameters** page (**Configuration** tab → **VoIP** → **SIP Definitions** → **Advanced Parameters**). This page allows the configuration of the defaults protocol parameters in case there is no mach on the previously configured protocol parameters. For the compliance test, only the **Broken Connection Mode** parameter was set to **Ignore**, other configurations may require special care. Click the **Submit** button to save changes.

The screenshot shows the AudioCodes Mediant 3000 'Admin' interface. The left sidebar contains a tree view with the following items: Basic, Advanced, System, VoIP, Network, TDM & Timing, Security, PSTN, Media, Quality of Experience, Services, VoIP Network, SIP Definitions (expanded), General Parameters, Advanced Parameters (selected), Account Table, Proxy & Registration, Hsp Policy & Manipulation, Coders and Profiles, Gateway, and SIP Media. The main content area is titled 'Advanced Parameters' and contains three sections:

- General**
  - SIP Security: Disable
  - Filter Calls to IP: Don't Filter
  - Enable Digit Delivery to Tel: Disable
  - Enable Digit Delivery to SIP: Disable
  - PSTN Alert Timeout: 180
  - QoS Statistics in Release Msg: Disable
- Disconnect and Answer Supervision**
  - Broken Connection Mode: Ignore
  - AMD Mode: Don't disconnect
  - Broken Connection Timeout [100 msec]: 100
  - Disconnect Call on Silence Detection: No
  - Silence Detection Period [sec]: 120
  - Silence Detection Method: None
  - Enable Fax Re-Routing: Disable
- Misc. Parameters**
  - Progress Indicator to IP: Not Configured
  - X-Channel Header: Disable
  - Early 183: Disable
  - SIP T.38 Version: Not Configured
  - Enable Busy Out: Disable
  - Graceful Busy Out Timeout [sec]: 0
  - Default Release Cause: 3
  - Max Number of Active Calls: 4032

The 'Submit' button is located at the bottom right of the interface.



### 7.7.6. Configure Supplementary Services Parameters

Open the **Supplementary Services** page (**Configuration** tab → **VoIP** → **Gateway** → **DTMF and Supplementary** → **Supplementary Services**). Set the following parameters:

- **Enable Hold:**           **Enable**
- **Enable Transfer:**       **Enable**
- **Enable Call Forward:**   **Enable**
- **Enable Call Waiting:**   **Enable**

The screen below illustrates the **Supplementary Services** page.

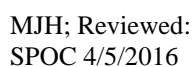
The screenshot shows the AudioCodes Mediant 3000 'Admin' web interface. The left sidebar contains a tree view with the following categories: System, VoIP, Network, TDM & Timing, Security, PSTN, Media, Quality of Experience, Services, VoIP Network, SIP Definitions, Coders and Profiles, Gateway, Trunk Group, Translations, Routing, DTMF and Supplementary, and Digital Gateway. The 'Supplementary Services' page is active, displaying a list of parameters with dropdown menus for configuration. The parameters are as follows:

Parameter	Value
Enable Hold	Enable
Answer Supervision	No
Enable Hold to TSDN	Disable
Hold Format	0000
Hold Timeout	-1
Enable Transfer	Enable
Transfer Prefix	
Enable Call Forward	Enable
Enable Call Waiting	Enable
Enable Caller ID	Disable
Hook-Flash Code	
Enable NRT Subscription	Disable
AS Subscribe IPGroupID	-1
NRT Subscribe Retry Time	120
Call Forward Ring Tone ID	1
Send All Coders on Retrieve	Disable
Generate Measuring Tones	Disable
AcC Support	Disable

Below the list, there is a 'Transfer' section with a 'Blind Transfer' parameter set to an empty field. A 'Submit' button is located at the bottom right of the configuration area.



Open the required **Source Phone Number Manipulation Table for Tel-to-IP Calls** page (**Configuration** tab → **VoIP** → **Gateway** → **Manipulations** → **Source Number Tel→IP**). The relevant Manipulation table page is displayed. The screen below shows the manipulation rule for Tel-to-IP source phone number manipulation, used in the compliance test.



### 7.7.8. Configure IP to Trunk Group Routing Rules

Open the **IP to Trunk Group Routing Table** page (**Configuration** tab → **VoIP** → **Gateway** → **Routing** → **IP to Trunk Group Routing**). Configure the inbound IP routing rules. The screen below illustrates the Inbound IP Routing Table used in the compliance test.

The screenshot shows the AudioCodes Mediant 2000 'Admin' interface. The left sidebar contains a navigation tree with the following items: System, VoIP, Network, TDM & Timing, Security, PSTN, Media, Quality of Experience, Services, VoIP Network, SIP Definitions, Coders and Profiles, Gateway, Trunk Group, Manipulations, Routing, Routing General Params, Tel to IP Routing, IP to Trunk Group Routing (selected), Forward On Busy Trunk, Gateway Routing Policy, Alternative Reasons, DTMF and Supplementary, Digital Gateway, and IP Media. The main area is titled 'IP-to-TrunkGroup Routing' and contains a table with the following columns: Index, Name, Source IP Group, Source SIP Interface, Source IP Address, Source Phone Prefix, Destination Phone Prefix, and Trunk Group ID. The table has two rows: Row 0 with values (0, None, Any, 4421, 1) and Row 1 with values (1, None, Any, 4422, 2). Below the table, the 'Selected Row #0' details are shown, including fields for Name, Source IP Group, Source SIP Interface, Source IP Address, Source Phone Prefix, Destination Phone Prefix, and Trunk Group ID.

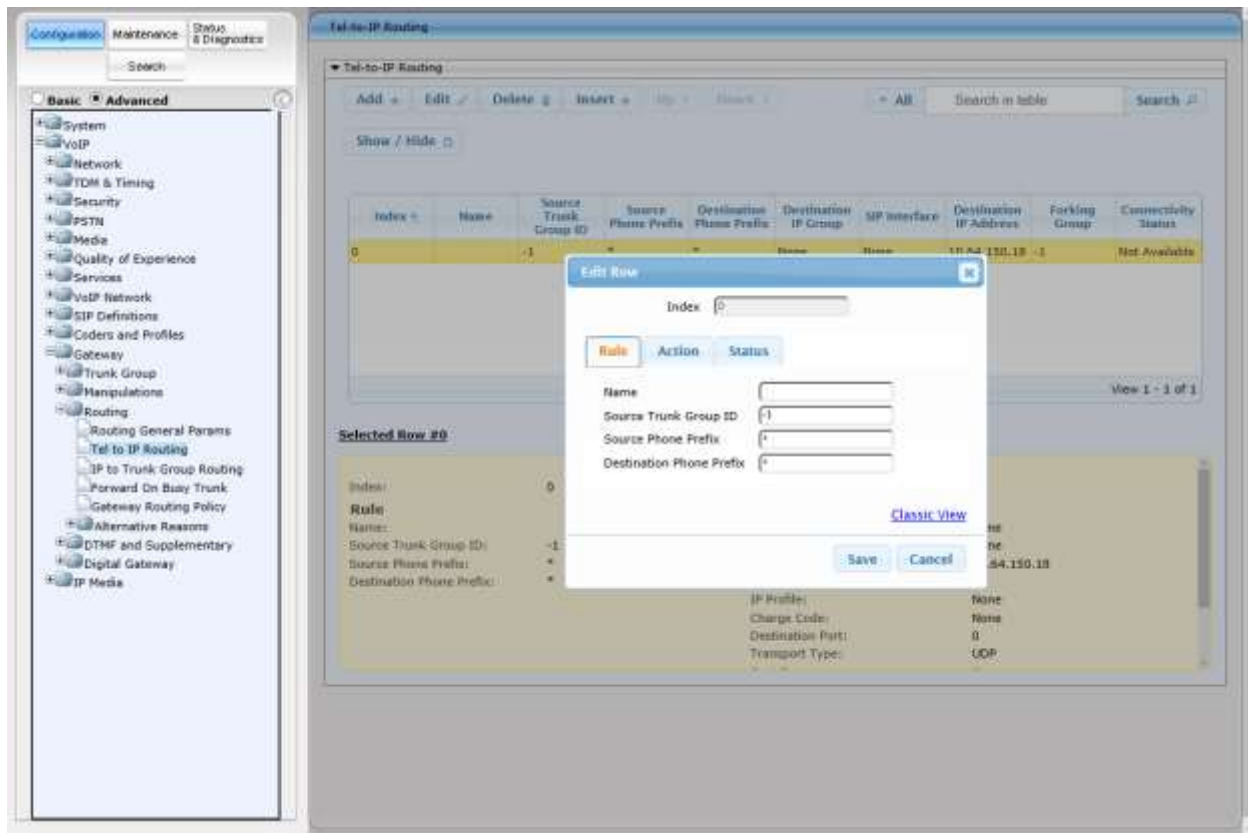
Index	Name	Source IP Group	Source SIP Interface	Source IP Address	Source Phone Prefix	Destination Phone Prefix	Trunk Group ID
0		None	Any			4421	1
1		None	Any			4422	2

Selected Row #0

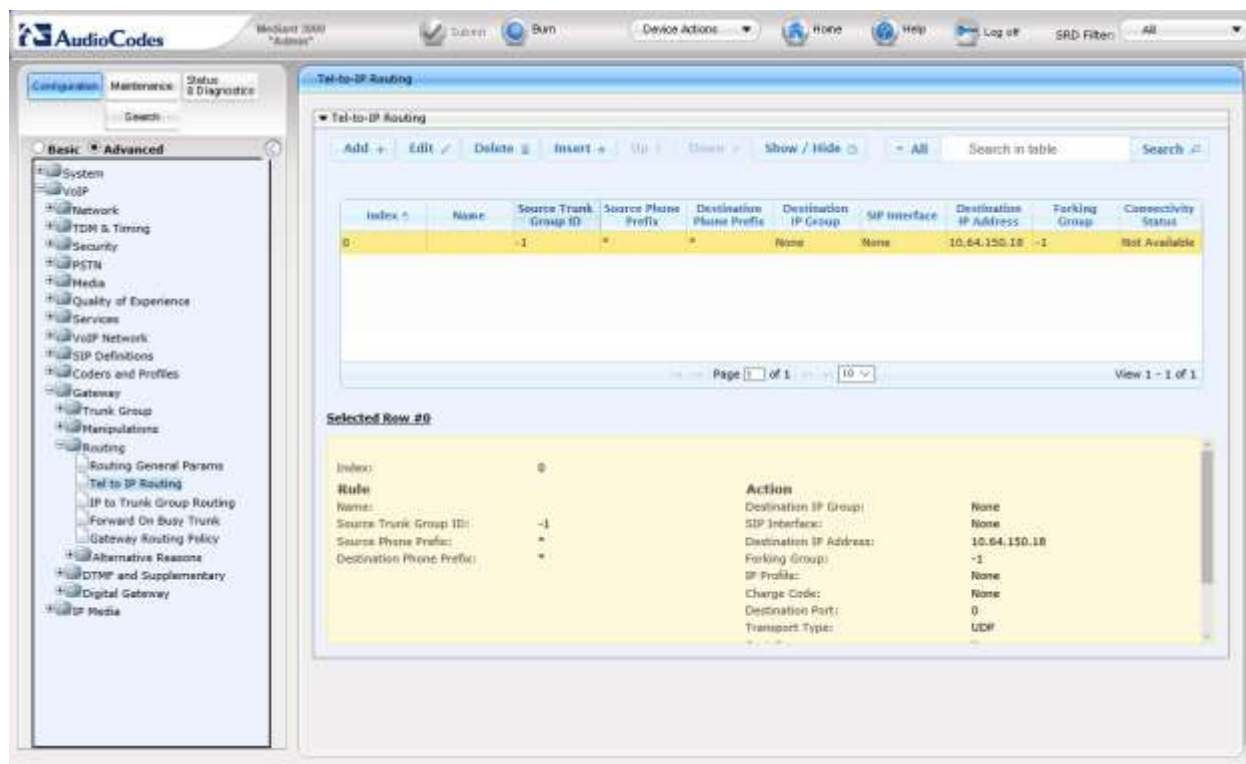
Index	0	Action
Name		Trunk Group ID: 1
Source IP Group	None	IP Profile: None
Source SIP Interface	Any	Trunk ID: -1
Source IP Address		Call Setup Rules Set ID: -1
Source Phone Prefix		Destination Type: Trunk Group
Destination Phone Prefix	4421	
Destination Host Prefix		
Source Host Prefix		

### 7.7.9. Configure Outbound IP Routing Rules

Open the **Tel to IP Routing** page (Configuration tab → VoIP → Gateway → Routing → Tel to IP Routing). Click the **Add** or **Edit** button to add or edit an index row.



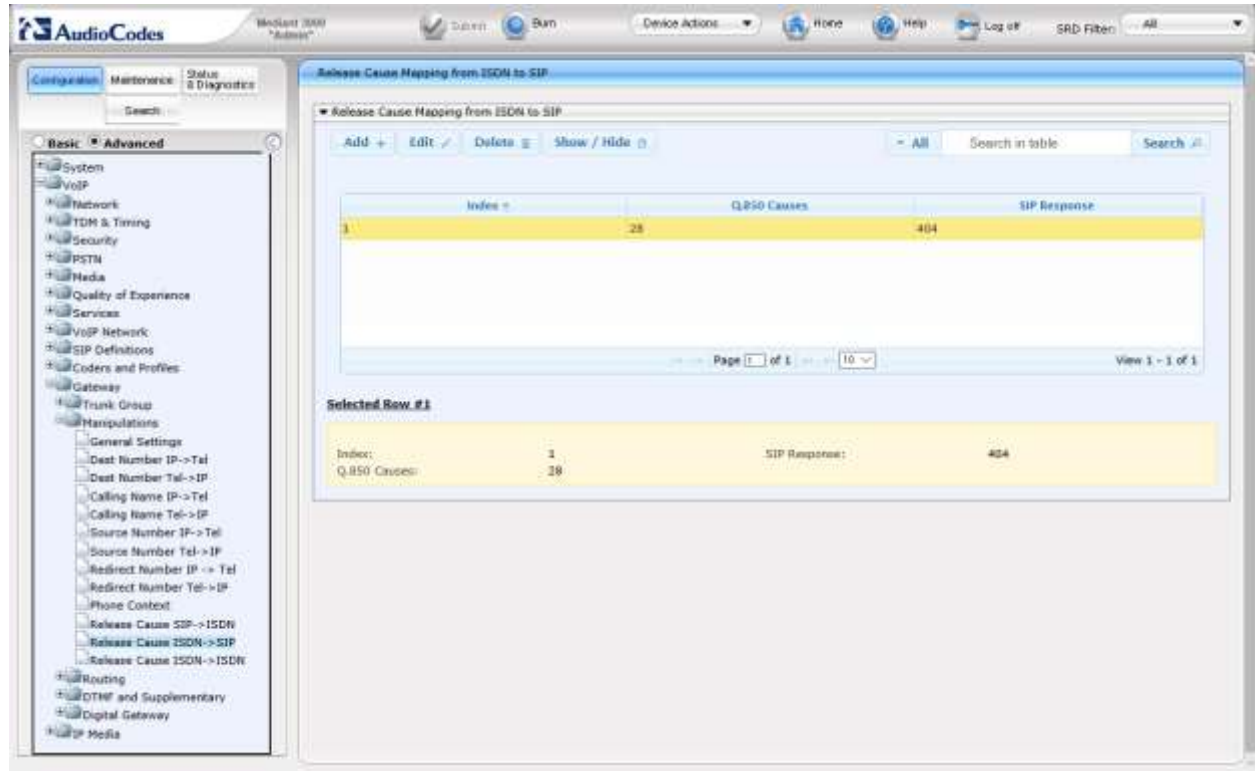
Configure the **Source Trunk Group ID** with the appropriate trunk number, **Destination Phone Prefix**, **Source Phone Prefix** with the appropriate patterns (i.e., \*) and **Destination IP Address** with the IP Address of signalling interface of Session Manager (i.e., **10.64.150.18**). Set the **Transport Type** to the appropriate value (i.e, **UDP**). Click on the **Submit** button to save changes. The following screen illustrates the configuration done for the compliance test.



### 7.7.10. Configure Release Cause Mapping

Open the **Release Cause Mapping from ISDN to SIP** page (**Configuration** tab → **VoIP** → **Gateway** → **Manipulations** → **Release Cause ISDN -> SIP**).

In these Application Notes, mapping from **Q.850 Cause** value **28** is mapped into **SIP Response** message **404**, this was used to ensure the mapping of Invalid Number in the Q.850 was mapped to a SIP 404 for the appropriate interworking. Click the **Submit** button to save changes. The screen below illustrates the **Release Cause Mapping from ISDN to SIP** page.



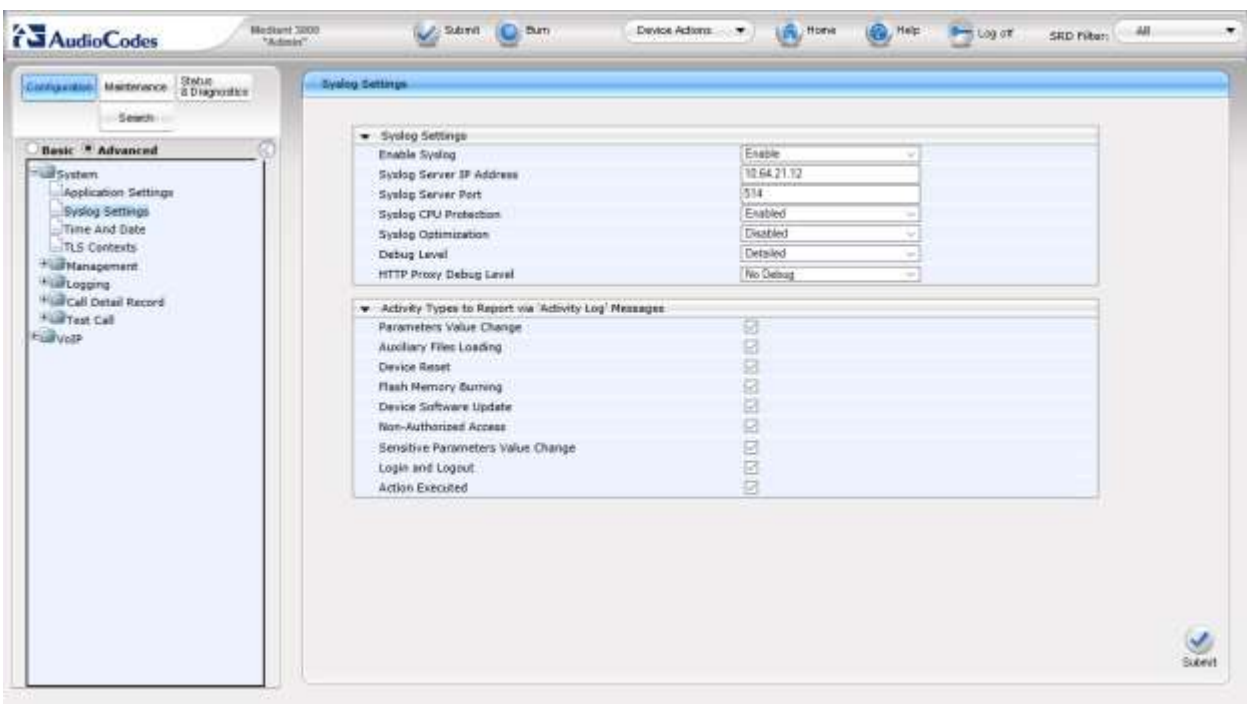
### 7.7.11. Configure Syslog Parameters for Debug Assistance

The Mediant 3000 Media Gateway can be configured to output logs to an external Syslog Server for debug assistance. To configure Syslog facility, open the **Syslog Settings** page (**Configuration** tab → **System** → **Syslog Settings**). Configure the following settings:

- **Enable Syslog:** Set to **Enable**
- **Syslog Server IP Address:** Set to IP address of device running a Syslog Server Application (i.e., **10.64.21.12**)
- **Syslog Server Port:** Set to port utilized on the Syslog Server listening device (i.e., **514**)
- **Debug Level:** Set to **Detailed** to capture proper level of debug information

Click the **Submit** button to save changes. The screen below illustrates settings used during compliance testing.

**Note:** The Syslog facility should be used only for Debugging purposes. **Enable** the Syslog service as needed and revert to **Disable** once troubleshooting is completed.



**Note:** Once configuration of the Mediant 3000 is complete refer to Section 7.3 to save the configuration.

## 8. Verification Steps

This section provides the verification steps that may be performed to verify the configuration.

### 8.1. Verify Avaya Aura® Communication Manager Trunk Status

On Communication Manager, ensure that all the signalling groups are in service by issuing the command status **signalling-group n** where **n** is the signalling group number.

```
status signaling-group 2
                        STATUS
SIGNALING GROUP
    Group ID: 2
    Group Type: sip
    Group State: in-service
```

## 8.2. SIP Monitoring on Avaya Aura® Session Manager

From System Manager's Home screen, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing. The screen below shows the link status between Session Manager and the Mediant 3000.

The screenshot displays the Avaya Aura Session Manager System Manager interface. The left sidebar shows the navigation menu with 'SIP Entity Monitoring' selected under 'System Status'. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a summary of entity links to a specific SIP entity (A4M3000). A table below shows the connection status for the selected Session Manager (sm15010).

Session Manager Name	SIP Entity Resolved IP	Port	Proto	Deep	Conn. Status	Reason Code	Link Status
sm15010	10.64.50.104	5060	UDP	FALSE	UP	200 OK	UP



## 8.3. Utilizing Mediant 3000 Web Interface to Observe Status

The **Status & Diagnostics** menu is used to view and monitor the device's channels, Syslog messages, hardware and software product information, and to assess the device's statistics and IP connectivity information.

### 8.3.1. Device Status

To view the status of the device's hardware components, open the **Components Status** page (**Status & Diagnostics** tab → **System Status** → **Components Status**). The screen below illustrates the **Component Status** page for the gateway where the TP8410 board in slot 1 is active.

The screenshot displays the AudioCodes Mediant 3000 web interface. The left sidebar shows the navigation menu with 'Status & Diagnostics' selected. The main content area is titled 'Components Status' and contains several tables of device information.

Slots	
Slot #1	TP8410, StandAlone, Temperature(Celsius)=30
Slot #2	SAT 2, StandAlone
Slot #3	Not Occupied
Slot #4	Not Occupied

Fan Status	
Tray	Fan Tray ID : 3, Version 0
1 Bottom Front Fan	Speed = 13560 (RPM)
2 Bottom Middle Fan	Speed = 13560 (RPM)
3 Bottom Middle Fan	Speed = 13560 (RPM)
4 Bottom Rear Fan	Speed = 11320 (RPM)
5 Top Front Fan	Speed = 13560 (RPM)
6 Top Middle Fan	Speed = 13460 (RPM)
7 Top Middle Fan	Speed = 13560 (RPM)
8 Top Rear Fan	Speed = 11320 (RPM)

Alarm Severity of Power Supply	
Top	No Alarm
Bottom	Major

PEM	
Top	PEM 2 Tray ID : 2, Version : 6, EPLO Version : 3, XBoard ID 2, XBoard Assembly 3
Bottom	PEM 1 Tray ID : 2, Version : 6, EPLO Version : 3, XBoard ID 2, XBoard Assembly 3, Disconnected

### 8.3.2. Device Information

Open the **Device Information** page (**Status & Diagnostics** tab → **System Status** → **Device Information**).

The screenshot displays the AudioCodes Mediant 3000 web interface. The top navigation bar includes tabs for Configuration, Maintenance, and Status & Diagnostics. The left sidebar shows a tree view with categories like Basic and Advanced, and sub-items such as System Status, Message Log, Activity Log, Device Information, Ethernet Port Information, Components Status, Carrier-Grade Alarms, Performance Monitoring, and VoIP Status. The main content area is titled 'Device Information' and contains three sections: General Settings, Versions, and Loaded Files.

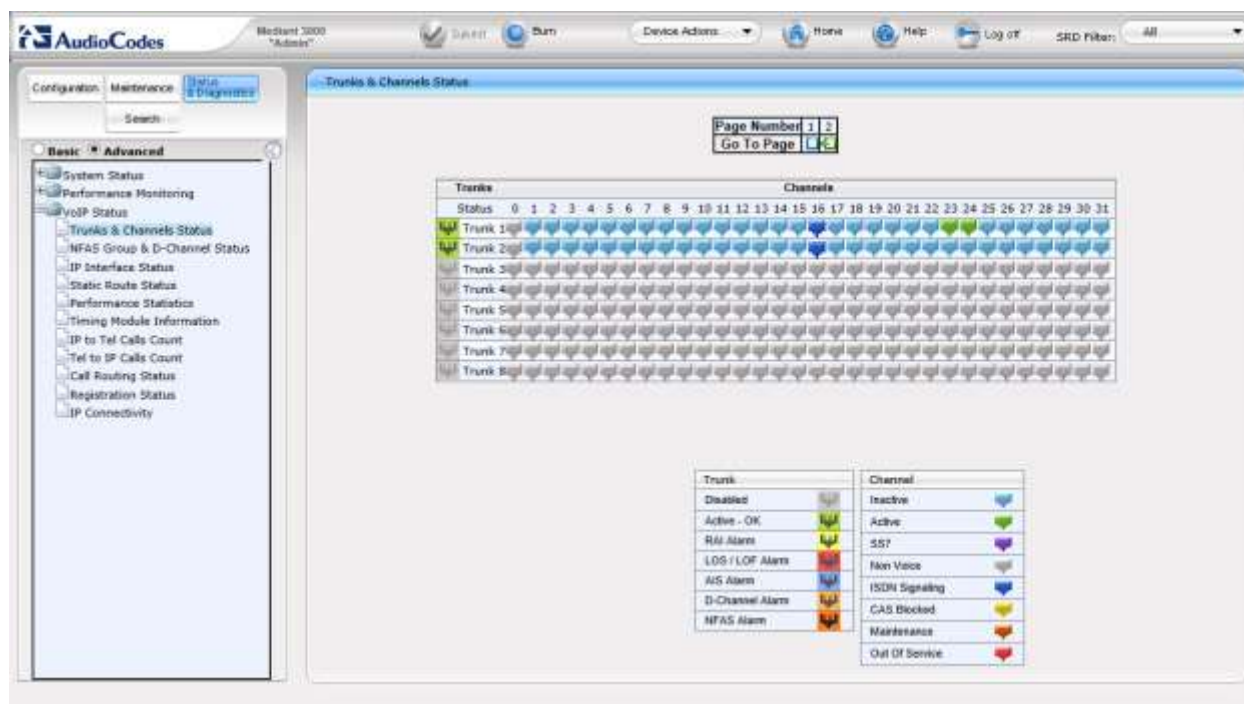
General Settings	
MAC Address:	0090a13c7ea2
Serial Number:	3994578
Board Type:	Mediant 3000
Device Up Time:	14d:20h:47m:23s:55th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size (Mbytes):	32
RAM Size (Mbytes):	512
CPU Speed (MHz):	480

Versions	
Version ID:	7.004.049.003
DSP Type:	2
DSP Software Version:	70037
DSP Software Name:	491095AE3
Flash Version:	220

Loaded Files	
Call Progress Tones File Name:	MJK_usa_tones.dat <a href="#">Delete</a>
Loaded Codec Table :	Default: CODERTABLE

### 8.3.3. Trunks and Channels Status

To view the status of the device's trunks and the trunks' channels, open the **Trunks & Channels Status** page (**Status & Diagnostics** tab → **VoIP Status** → **Trunks & Channels Status**). The following screen illustrates the **Trunks and Channel Status** page, where the symbols of the port in green represent channels engaged with a call.



## 9. Conclusion

These Application Notes describe the procedures required to configure the AudioCodes Mediant 3000 Gateway to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The AudioCodes Mediant 3000 Gateway successfully passed compliance testing.

## 10. Additional References

This section references the product documentation relevant for these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Document 03-300509
- [2] *Administering Avaya Aura® Session Manager*, Document 03-603324
- [3] *User's Manual Mediant™ 3000 Gateway & E-SBC* Version 6.8 November 2014 Document # LTRT-89725

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>.

## 11. Appendix

The AudioCodes M3000 .ini file was generated after completing the compliance test. Its contents were copied below. Please use it only for reference purposes.

```
;*****
;** Ini File **
;*****

;Board: Mediant 3000
;HW Board Type: 63  FK Board Type: 49
;M3K Board Type: TrunkPack 8410
;Serial Number: 3964578
;Slot Number: 1
;Software Version: 7.00A.049.003
;DSP Software Version: 491096AE3=> 700.27
;Board IP Address: 10.64.50.199
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 10.64.50.1
;Ram size: 512M  Flash size: 32M
;Num of DSP Cores: 36  Num DSP Channels: 504
;Profile: NONE
;;;Key features;;Board Type: Mediant 3000 ;PSTN STM1\SONET Interface Not
Supported ;E1Trunks=16 ;T1Trunks=21 ;IP Media: VXML CALEA ;PSTN
Protocols: ISDN IUA=84 CAS V5.2 ;Channel Type: RTP DspCh=504 ;HA ;Coders:
G723 G729 GSM-FR G727 ILBC ;Security: IPSEC MediaEncryption
StrongEncryption EncryptControlProtocol ;DSP Voice features: IpmDetector
AMRPolicyManagement ;Control Protocols: MSFT MGCP MEGACO SIP ;Default
features;;Coders: G711 G726;
;-----

[SYSTEM Params]

;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value
SyslogServerIP = 10.64.21.12
EnableSyslog = 1
ENABLEPARAMETERSMONITORING = 1
ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'naa', 'spc', 'll',
'ae'
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '0.0.0.0'
;LastConfigChangeTime is hidden but has non-default value
;RootFileLastUpdateTime is hidden but has non-default value
;PkeyFileLastUpdateTime is hidden but has non-default value

[BSP Params]

PCMLawSelect = 1
```

```
TDMBusSpeed = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95
```

```
[ControlProtocols Params]
```

```
AdminStateLockControl = 0
cpRecordCoder = 'PCMA'
```

```
[MGCP Params]
```

```
[MEGACO Params]
```

```
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
```

```
[PSTN Params]
```

```
TraceLevel_0 = 1
TraceLevel_1 = 0
TraceLevel_2 = 0
TraceLevel_3 = 0
TraceLevel_4 = 0
TraceLevel_5 = 0
TraceLevel_6 = 0
TraceLevel_7 = 0
TraceLevel_8 = 0
TraceLevel_9 = 0
TraceLevel_10 = 0
TraceLevel_11 = 0
TraceLevel_12 = 0
TraceLevel_13 = 0
TraceLevel_14 = 0
TraceLevel_15 = 0
ProtocolType_0 = 1
ProtocolType_1 = 1
ProtocolType_2 = 0
ProtocolType_3 = 0
ProtocolType_4 = 0
ProtocolType_5 = 0
ProtocolType_6 = 0
ProtocolType_7 = 0
ProtocolType_8 = 0
ProtocolType_9 = 0
ProtocolType_10 = 0
ProtocolType_11 = 0
ProtocolType_12 = 0
```

ProtocolType\_13 = 0  
ProtocolType\_14 = 0  
ProtocolType\_15 = 0  
FramingMethod\_0 = b  
FramingMethod\_1 = b  
FramingMethod\_2 = 0  
FramingMethod\_3 = 0  
FramingMethod\_4 = 0  
FramingMethod\_5 = 0  
FramingMethod\_6 = 0  
FramingMethod\_7 = 0  
FramingMethod\_8 = 0  
FramingMethod\_9 = 0  
FramingMethod\_10 = 0  
FramingMethod\_11 = 0  
FramingMethod\_12 = 0  
FramingMethod\_13 = 0  
FramingMethod\_14 = 0  
FramingMethod\_15 = 0  
LineCode\_0 = 2  
LineCode\_1 = 2  
LineCode\_2 = 0  
LineCode\_3 = 0  
LineCode\_4 = 0  
LineCode\_5 = 0  
LineCode\_6 = 0  
LineCode\_7 = 0  
LineCode\_8 = 0  
LineCode\_9 = 0  
LineCode\_10 = 0  
LineCode\_11 = 0  
LineCode\_12 = 0  
LineCode\_13 = 0  
LineCode\_14 = 0  
LineCode\_15 = 0  
CASProtocolEnable = 0

[SS7 Params]

[Voice Engine Params]

CallProgressTonesFilename = 'M2K\_usa\_tones.dat'  
V22ModemTransportType = 0  
V23ModemTransportType = 0  
V32ModemTransportType = 0  
V34ModemTransportType = 0  
RFC2833TxPayloadType = 101  
AnswerDetectorSilenceTime = 0  
AnswerDetectorSensitivity = 0  
EnergyDetectorQualityFactor = 0  
EnergyDetectorThreshold = 0

[WEB Params]

LogoWidth = '145'  
HTTPSCipherString = 'RC4:EXP'  
;HTTPSPkeyFileName is hidden but has non-default value  
;HTTPSCertFileName is hidden but has non-default value

[SIP Params]

GWDEBUGLEVEL = 5  
;ISPRACKREQUIRED is hidden but has non-default value  
ENABLEEARLYMEDIA = 1  
DISCONNECTONBROKENCONNECTION = 0  
ISFAXUSED = 1  
SIPTRANSPORTTYPE = 1  
BCHANNELNEGOTIATIONFORTRUNK\_0 = 0  
BCHANNELNEGOTIATIONFORTRUNK\_1 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_2 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_3 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_4 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_5 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_6 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_7 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_8 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_9 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_10 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_11 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_12 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_13 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_14 = -1  
BCHANNELNEGOTIATIONFORTRUNK\_15 = -1  
MSLDAPPRIMARYKEY = 'telephoneNumber'  
FIRSTTXDTMFOPTION = 4  
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]

[VXML Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

;ContextEngineID is hidden but has non-default value

[Video Params]

[ InterfaceTable ]

```
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress;
InterfaceTable_0 = 6, 10, 10.64.50.199, 24, 10.64.50.1, 1, "if 0",
0.0.0.0, 0.0.0.0;
```

[ \InterfaceTable ]

[ DspTemplates ]

```
FORMAT DspTemplates_Index = DspTemplates_DspTemplateName,
DspTemplates_DspResourcesPercentage;
DspTemplates_0 = 0, 100;
```

[ \DspTemplates ]

[ WebUsers ]

```
FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers_0 = "Admin",
"$1$YQVaVldWB1JaDlpcXwkKDEAUQUpHFkVCQE9DQ09JGk21t7rlsbyysr256+66uO3tqaX0q
qT0866hrPur/qmoqcU=", 1, 0, 2, 15, 60, 200,
"39ea427ac3a5abe249eb8e0e3bb18e26";
WebUsers_1 = "User",
"$1$Wj44aG9rbVFTV1IHVVVTXgxZWFUMWAwUF0UREhAXThlKtK4YRBhI5eK2s+Hhsb+6vem8t
bjqvvgJo6eg8fei+fo=", 1, 0, 2, 15, 60, 50,
"bb9a70129d690ca6545321ae6d4e1999";
```

[ \WebUsers ]

[ TLSContexts ]

```
FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
```



```
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, 0.0.0.0, 0.0.0.0,
2560, 0;
```

```
[ \TLSContexts ]
```

```
[ IpProfile ]
```

```
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,
IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,
IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,
IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,
IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,
IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,
IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,
IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,
IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,
IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,
IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport,
IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPptimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
```

```

IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW;
IpProfile_1 = "IpProfile_1", 1, 0, 1, 10, 10, 46, 40, 0, 0, 0, 0, 0, 0,
0, 1, 1, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1,
0, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0,
1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "",
0;

```

[ \IpProfile ]

[ CpMediaRealm ]

```

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm_0 = "DefaultRealm", "if 0", "", 6000, 4032, 46319, 1, "",
"";

```

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

```

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy_0 = "Default_SBCRoutingPolicy", 0, 0, 1, "";

```

[ \SBCRoutingPolicy ]

[ SRD ]

```

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName;
SRD_0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "";

```

[ \SRD ]

[ SIPInterface ]

```
FORMAT SIPInterface_Index = SIPInterface_InterfaceName,  
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,  
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,  
SIPInterface_SRDName, SIPInterface_MessagePolicyName,  
SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication,  
SIPInterface_TCPKeepaliveEnable,  
SIPInterface_ClassificationFailureResponseType,  
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,  
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,  
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,  
SIPInterface_EnableUnAuthenticatedRegistrations,  
SIPInterface_UsedByRoutingServer;  
SIPInterface_0 = "SIPInterface_0", "if 0", 0, 5060, 5060, 5061,  
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "", 0, -1, -1, -1, 0;
```

[ \SIPInterface ]

[ ProxySet ]

```
FORMAT ProxySet_Index = ProxySet_ProxyName,  
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,  
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,  
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,  
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,  
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,  
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_SASIPv4SIPInterfaceName,  
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,  
ProxySet_SASIPv6SIPInterfaceName;  
ProxySet_0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",  
"SIPInterface_0", "", "", "", "", "", "";
```

[ \ProxySet ]

[ IPGroup ]

```
FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,  
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,  
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,  
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,  
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,  
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,  
IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput,  
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,  
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,  
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
```

```

IPGroup_AlwaysUseSourceAddr, IGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IGroup_SIPConnect, IGroup_SBCPSAPMode,
IPGroup_DTLSContext, IGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IGroup_SBCKeepOriginalCallID,
IPGroup_SBCDialPlanName;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 1, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
"", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";

```

[ \IPGroup ]

[ PREFIX ]

```

FORMAT PREFIX_Index = PREFIX_RouteName, PREFIX_DestinationPrefix,
PREFIX_DestAddress, PREFIX_SourcePrefix, PREFIX_ProfileName,
PREFIX_MeteringCodeName, PREFIX_DestPort, PREFIX_DestIPGroupName,
PREFIX_TransportType, PREFIX_SrcTrunkGroupID,
PREFIX_DestSIPInterfaceName, PREFIX_CostGroup, PREFIX_ForkingGroup,
PREFIX_CallSetupRulesSetId, PREFIX_ConnectivityStatus;
PREFIX 0 = "", "*", "10.64.150.18", "*", "", "", 0, "", 0, -1, "", "", -
1, -1, "Not Available";

```

[ \PREFIX ]

[ TrunkGroup ]

```

FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel,
TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber,
TrunkGroup_ProfileName, TrunkGroup_LastTrunkId, TrunkGroup_Module;
TrunkGroup 0 = 1, 0, 1, 31, "4421000", "", 0, 255;
TrunkGroup 1 = 2, 1, 1, 31, "4422000", "", 1, 255;

```

[ \TrunkGroup ]

[ SourceNumberMapTel2Ip ]

```

FORMAT SourceNumberMapTel2Ip_Index =
SourceNumberMapTel2Ip_ManipulationName,
SourceNumberMapTel2Ip_DestinationPrefix,
SourceNumberMapTel2Ip_SourcePrefix, SourceNumberMapTel2Ip_NumberType,
SourceNumberMapTel2Ip_NumberPlan, SourceNumberMapTel2Ip_RemoveFromLeft,
SourceNumberMapTel2Ip_RemoveFromRight,
SourceNumberMapTel2Ip_LeaveFromRight, SourceNumberMapTel2Ip_Prefix2Add,
SourceNumberMapTel2Ip_Suffix2Add,
SourceNumberMapTel2Ip_IsPresentationRestricted,
SourceNumberMapTel2Ip_SrcTrunkGroupID;

```

```
SourceNumberMapTel2Ip 1 = "", "*", "*", 255, 255, 0, 0, 255, "", "", 0, -1;
```

```
[ \SourceNumberMapTel2Ip ]
```

```
[ PstnPrefix ]
```

```
FORMAT PstnPrefix_Index = PstnPrefix_RouteName, PstnPrefix_DestPrefix,  
PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix,  
PstnPrefix_SourceAddress, PstnPrefix_ProfileName,  
PstnPrefix_SrcIPGroupName, PstnPrefix_DestHostPrefix,  
PstnPrefix_SrcHostPrefix, PstnPrefix_SrcSIPInterfaceName,  
PstnPrefix_TrunkId, PstnPrefix_CallSetupRulesSetId, PstnPrefix_DestType;  
PstnPrefix 0 = "", "4421", 1, "", "", "", "", "", "", "Any", -1, -1, 0;  
PstnPrefix 1 = "", "4422", 2, "", "", "", "", "", "", "Any", -1, -1, 0;
```

```
[ \PstnPrefix ]
```

```
[ CauseMapIsdn2Sip ]
```

```
FORMAT CauseMapIsdn2Sip_Index = CauseMapIsdn2Sip_IsdnReleaseCause,  
CauseMapIsdn2Sip_SipResponse;  
CauseMapIsdn2Sip 1 = 28, 404;
```

```
[ \CauseMapIsdn2Sip ]
```

```
[ TrunkGroupSettings ]
```

```
FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId,  
TrunkGroupSettings_ChannelSelectMode,  
TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName,  
TrunkGroupSettings_ContactUser, TrunkGroupSettings_ServingIPGroupName,  
TrunkGroupSettings_MWIInterrogationType,  
TrunkGroupSettings_TrunkGroupName,  
TrunkGroupSettings_UsedByRoutingServer, TrunkGroupSettings_AdminState;  
TrunkGroupSettings 0 = 1, 1, 255, "", "", "", 255, "", 0, 0;  
TrunkGroupSettings 1 = 2, 1, 255, "", "", "", 255, "", 0, 0;
```

```
[ \TrunkGroupSettings ]
```

```
[ CodersGroup0 ]
```

```
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,  
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,  
CodersGroup0_CoderSpecific;  
CodersGroup0 0 = "g711Alaw64k", 20, 0, -1, 0, "";  
CodersGroup0 1 = "g711Ulaw64k", 20, 0, -1, 0, "";  
CodersGroup0 2 = "g729", 20, 0, -1, 0, "";
```

```

[ \CodersGroup0 ]

[ RoutingRuleGroups ]

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

[ \RoutingRuleGroups ]

[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 0, 1, "";

[ \GwRoutingPolicy ]

[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 0;
ResourcePriorityNetworkDomains 2 = "dod", 0;
ResourcePriorityNetworkDomains 3 = "drsn", 0;
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 0;

[ \ResourcePriorityNetworkDomains ]

```

---

**©2016 Avaya Inc. All Rights Reserved.**

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

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