



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Aura™ Session Manager and Avaya Aura™ Communication Manager Feature Server with AudioCodes Mediant 3000 Gateway to access E1 PSTN - Issue 1.0

Abstract

These Application Notes describe the procedure to configure an Enterprise network built on Avaya Aura™ Session Manager, and Avaya Aura™ Communication Manager Feature Server to interoperate with AudioCodes Mediant 3000 Gateway to access E1 PSTN using SIP trunking.

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
1.1. AudioCodes Mediant 3000	4
1.2. Interoperability Compliance Testing	5
1.3. Support.....	5
2. Reference Configuration	6
3. Equipment and Software Validated.....	7
4. Configure Avaya AuraTM Communication Manager Feature Server	8
4.1. Verify Avaya Aura TM Communication Manager License	8
4.2. Administer System Parameters Features	9
4.3. Administer IP Node Names	9
4.4. Administer IP Network Region and Codec Set	10
4.5. Administer SIP Trunks with Avaya Aura TM Session Manager	11
4.5.1. Add SIP Signaling Group for Calls within the Enterprise	11
4.5.2. Configure a SIP Trunk Group for Calls within the Enterprise	12
4.5.3. Add SIP Signaling Group for Mediant 3000	13
4.5.4. Configure a SIP Trunk Group for Mediant 3000	14
4.6. Configure Route Patterns.....	15
4.6.1. Route Pattern for Enterprise Calls	15
4.7. Administer Private Numbering	15
4.8. Administer Dial Plan and AAR analysis	16
4.9. Administer ARS Analysis.....	17
4.10. Administer Feature Access Code.....	17
4.11. Save Changes	17
5. Configure Avaya AuraTM Session Manager	18
5.1. Specify SIP Domain.....	19
5.2. Add Locations	20
5.3. Add Adaptations	21
5.4. Add SIP Entities.....	22
5.4.1. Adding Avaya Aura TM Communication Manager Feature Server SIP Entity	22
5.4.2. Adding AudioCodes Mediant 3000 Gateway SIP Entity	23
5.4.3. Adding Avaya Aura TM Session Manager SIP Entity	24
5.5. Add Entity Links.....	25
5.6. Add Routing Policies	27
5.7. Add Dial Patterns.....	28
5.8. Add Avaya Aura TM Session Manager.....	29
5.9. Add Avaya Aura TM Communication Manager as a Feature Server.....	30
5.9.1. Create an Application Entry.....	30
5.9.2. Create a Feature Server Application	32
5.9.3. Create a Feature Server Application Sequence.....	33
5.9.4. Synchronize Avaya Aura TM Communication Manager Data.....	34
5.10. Add Users for SIP Phones.....	34
6. AudioCodes Mediant 3000 Configuration	38

6.1.	Configure the Media Gateway IP Network Parameters.....	38
6.1.1.	Saving settings	39
6.2.	Configure the Media Gateway TDM and Timing Parameters.....	40
6.2.1.	Configure TDM Bus	40
6.2.2.	Configure digital PCM settings	40
6.2.3.	Configure system timing.....	41
6.3.	Configure the Media Gateway Media Settings.....	42
6.3.1.	Configure the Voice parameters	42
6.3.2.	Configure the Fax Parameters.....	43
6.3.3.	Configure the RTP/RTCP Parameters	44
6.4.	Configure the Media Gateway Telephony/PSTN Interface Parameters	45
6.5.	Configure the SIP Protocol Parameters	47
6.5.1.	Configure the Trunk Group Table	47
6.5.2.	Configure the General SIP Protocol Parameters.....	48
6.5.3.	Configure the DTMF and Dialing Parameters.....	49
6.5.4.	Configure the Proxy & Registration Parameters	50
6.5.5.	Configure the Device's Coders	51
6.5.6.	Configure the IP Profile Settings	52
6.5.7.	Configure the Advanced General Protocol Parameters	54
6.5.8.	Configure the Supplementary Services Parameters.....	55
6.5.9.	Configure the Number Manipulation Tables	56
6.5.10.	Configure Inbound IP Routing Rules	56
6.5.11.	Configure Outbound IP Routing Rules.....	57
6.5.12.	Configure Release Cause Mapping.....	59
6.6.	Configure the Syslog Parameters for Debug Assistance	60
7.	Verification Steps	61
7.1.	Verify Avaya Aura™ Communication Manager Feature Server Trunk Status.....	61
7.2.	SIP Monitoring on Avaya Aura™ Session Manager.....	62
7.3.	Utilizing the Web Interface to observe Status	62
7.3.1.	Device Status	63
7.3.2.	Device Information	63
7.3.3.	Trunks and Channels Status.....	64
7.3.4.	Gateway Home Page.....	64
8.	General Test Approach	66
8.1.	Test Results and Remarks.....	66
9.	Conclusion.....	66
10.	Additional References.....	67

1. Introduction

These Application Notes present a sample configuration for an Enterprise network consisting on Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager Feature Server as SIP infrastructure to access the PSTN with AudioCodes Mediant 3000 Gateway using SIP. The AudioCodes Mediant 3000 is a carrier-grade VoIP gateway that supports both media and signaling in a single chassis. It provides any-to-any voice network connectivity and can deliver SIP services into legacy PRI, CAS, and SS7 networks, as well as IP-to-IP transcoding and multimedia border element functions, such as SIP mediation for network edge applications. Its compact 2U high-density design features integrated SS7 termination across multiple gateways, GUI-based management, and software licensing for in-service capacity expansion.

1.1. AudioCodes Mediant 3000

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.

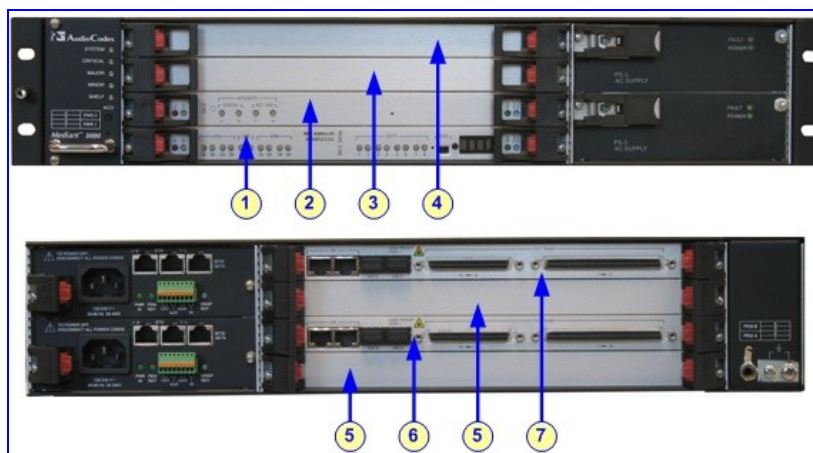


Figure 1: Front and Rear Panel Slot Assignment for AudioCodes Mediant 3000 Simplex with 8410 Blades

Legend:

1. Slot 1 front panel: 8410 blade (active blade for AudioCodes Mediant 3000 HA only).
2. Slot 2 front panel: SA/M3K blade (active blade for AudioCodes Mediant 3000 HA only).
3. Slot 3 front panel: Standby (redundant) 8410 blade (applicable only to AudioCodes Mediant 3000 HA). In Simplex mode, this slot is covered with a blank panel.

4. Slot 4 front panel: Standby (redundant) Alarm and Status blade (applicable only to AudioCodes Mediant 3000 HA). In Simplex mode, this slot is covered with a blank panel.
5. Blank panels covering unoccupied slots.
6. Slot 2 rear panel: RTM-8410 providing PSTN E1/T1 (Trunks 1 to 42, or 1 to 16) and dual Gigabit Ethernet interfaces.
7. Slot 4 rear panel: RTM-8410 providing PSTN E1/T1 (Trunks 43 to 84) interfaces and Gigabit Ethernet interfaces.

1.2. Interoperability Compliance Testing

The primary focus of testing is to verify SIP trunking interoperability between an Avaya Aura[™] SIP-based network and AudioCodes Mediant 3000 Gateway using SIP. Test cases are selected to exercise a sufficiently broad segment of functionality to have a reasonable expectation of interoperability in production configurations.

Basic Interoperability:

- PSTN calls delivered via the AudioCodes Mediant 3000 to an Enterprise endpoint
- PSTN calls sent via the AudioCodes Mediant 3000 from an Enterprise endpoint
- Calling with various Avaya SIP telephone models
- Verify ITU-T codecs: G.711A G.711MU G.729A G.729B support
- Various PTSN dialing plans including national and international calling, toll-free, operator, directory assistance and direct inward dialed calling
- SIP transport using UDP and TCP

Advanced Interoperability:

- 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
- EC500 for Avaya Aura[™] Communication Manager

1.3. Support

Technical Support on AudioCodes Mediant 3000 Gateway can be obtained through email notification to support@audiocodes.com

2. 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 PSTN. The Mediant 3000 is managed by using the web interface, other administration capabilities are available, refer to [15-18] for additional information. Session Manager, with its SM-100 (Security Module) network interface, routes the 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 System Manager via the management network interface.

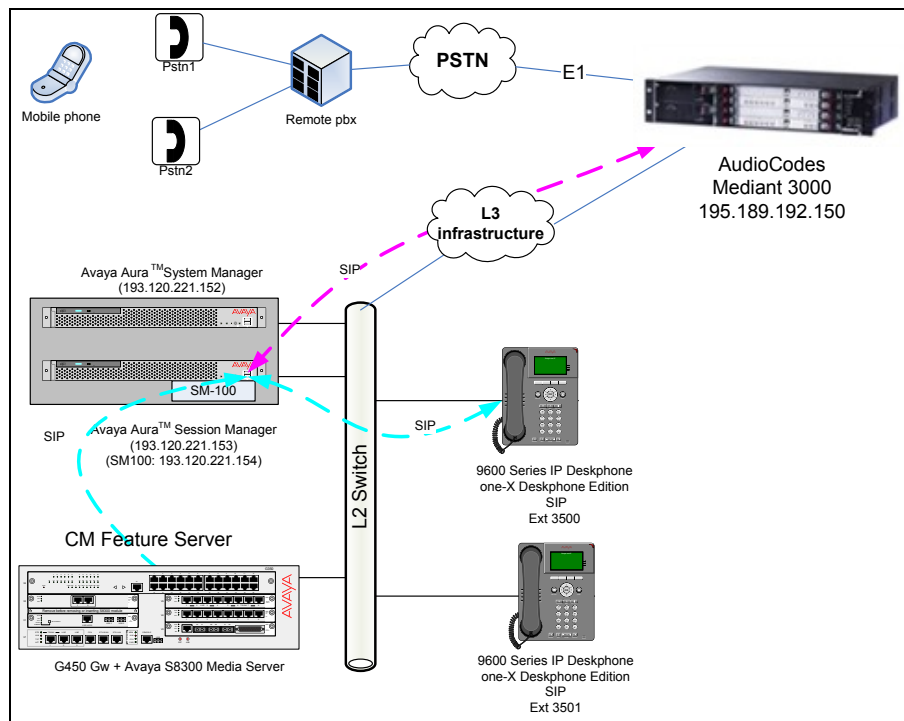


Figure 2: Sample configuration for Avaya Aura™ Communication Manager Feature Server and Avaya Aura™ Session Manager with AudioCodes Mediant 3000 using SIP Trunking

For the sample configuration shown in **Figure 1**, Session Manager runs on an Avaya S8510 Server and Communication Manager Feature Server runs on an Avaya S8300D inside an Avaya G450 Media Gateway. For the Communication Manager Feature Server, the results in these Application Notes are applicable to other supported Communication Manager Server and Media Gateway combinations. These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of the endpoint telephones will not be described. Refer to the appropriate documentation in **Section 10**.

3. Equipment and Software Validated

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

Avaya Product / Hardware Platform	Software Version
Avaya Aura™ Session Manager on Avaya S8510 Server	Avaya Aura™ Session Manager 5.2 5.2.1.1.521012 – 5.2.1 SP1
Avaya Aura™ System Manager Template running on Avaya System Platform S8510 Server	Avaya Aura™ System Manager 5.2 5.2.1.0.521001 - 05_02_GA_01_Dec10
Avaya Aura™ System Platform on Avaya S8510 Server	Avaya Aura™ System Platform Version 1.1.1.0.2
Avaya Aura™ Communication Manager – Feature Server – Avaya Media Server S8300C	Avaya Aura™ Communication Manager R015x.02.1.016.4 – patch 18250 (SP3)
Avaya Media Gateway G450	Firmware 30.13.2
Avaya IP Telephones: 9630 (SIP) 9620 (SIP)	Avaya one-X™ Deskphone SIP 2.5.0
AudioCodes	
Product /Hardware Platform	Software Version
AudioCodes Mediant 3000 chassis equipped with: SA/M3K - Alarm, Status and Synchronization blade TP8410 blades – Trunk Pack RTM-8410, Rear module, proving the I/O connections to the supported interfaces (Gigabit Ethernet and DS1 PSTN).	Mediant 3000 TP 8410 based software 6.00A.014.005 Firmware load: TP8410_SIP_F6.00A.014.005.cmp

4. Configure Avaya Aura™ Communication Manager Feature Server

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 **References [10]** and **[13]**. The procedures include the following areas:

- Verify Avaya Aura™ 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

4.1. 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 10
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	100	0	
Maximum Concurrently Registered IP Stations:	450	0	
Maximum Administered Remote Office Trunks:	0	0	
Maximum Concurrently Registered Remote Office Stations:	0	0	
Maximum Concurrently Registered IP eCons:	0	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	100	0	
Maximum Video Capable IP Softphones:	100	0	
Maximum Administered SIP Trunks:	100	50	

4.2. 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.

Note: This feature poses significant security risk and must be used with caution. As an alternative, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels.

change system-parameters features	Page 1 of 18
FEATURE-RELATED SYSTEM PARAMETERS	
Self Station Display Enabled? y	
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/Tone on Hold: none	
Music (or Silence) on Transferred Trunk Calls? no	
DID/Tie/ISDN/SIP Intercept Treatment: attd	
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred	
Automatic Circuit Assurance (ACA) Enabled? n	

4.3. 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 **193.120.221.180** are entered as **Name** and **IP Address** for the signaling in Communication Manager running on the Avaya S8300 Server. In addition, **SM100** and **193.120.221.154** are entered for Session Manager.

change node-names ip	Page 1 of 2
IP NODE NAMES	
Name	IP Address
default	0.0.0.0
procr	193.120.221.180
sm100	193.120.221.154

4.4. 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 19
                                                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: avaya.com
Name: Enterprise
MEDIA PARAMETERS
  Codec Set: 1
  Intra-region IP-IP Direct Audio: yes
  Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048
  UDP Port Max: 3329
  IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
  RTCP Reporting Enabled? y
  RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? y
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
  AUDIO RESOURCE RESERVATION PARAMETERS
  RSVP Enabled? n
H.323 IP ENDPOINTS
  H.323 Link Bounce Recovery? y
  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. A list of supported by the interoperability compliance testing is presented in **Section 1.2**. The ITU G.711A-law is described here. Configure the IP Codec Set as follows:

- **Audio Codec** Set **G.711A**

Retain the default values for the remaining fields.

```
change ip-codec-set 1                                         Page 1 of 2
                                                                IP Codec Set
Codec Set: 1
Audio Codec
1: G.711A      Silence Suppression  Frames Per Pkt  Packet Size (ms)
2:              n                  2             20
3:
```

4.5. Administer SIP Trunks with Avaya Aura™ Session Manager

In the test configuration, since Communication Manager acts as a Feature Server in this case, trunks with Session Manager must be IMS enabled. Two SIP trunks are needed for the configuration presented in these notes: one for calls with Mediant 3000 and another one for calls within the Enterprise. To administer a SIP Trunk on Communication Manager, two intermediate steps are required: the creation of a signaling group and a trunk group

4.5.1. Add SIP Signaling Group for Calls within the Enterprise

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
- **IMS Enabled:** y
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name from **Section 5.3**
i.e. **sm100**
- **Near-end Listen Port:** 5061
- **Far-end Listen Port:** 5061
- **Far-end Domain:** avaya.com
- **DTMF over IP:** rtp-payload
- **Direct IP-IP Audio Connections:** y

add signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
	Transport Method: tls	
IMS Enabled? y		
IP Video? n		
Near-end Node Name: procr	Far-end Node Name: sm100	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 30	

4.5.2. Configure a SIP Trunk Group for Calls within the Enterprise

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. **with-SessionManager**)
- **TAC:** An available trunk access code (i.e. **101**)
- **Service Type:** **tie**
- **Signaling Group:** The number of the signaling group associated (i.e. **1**)
- **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 licensed verified in **Section 4.1**)

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: with-SessionManager	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 1	
		Number of Members: 20	

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

add trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private			
		UII Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	

4.5.3. Add SIP Signaling Group for Mediant 3000

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
- **IMS Enabled:** y
- **Near-end Node Name:** procr
- **Far-end Node Name:** Session Manager node name from **Section 4.3**
i.e. **sm100**
- **Near-end Listen Port:** 5061
- **Far-end Listen Port:** 5061
- **Far-end Domain:** Leave it blank
- **DTMF over IP:** rtp-payload
- **Direct IP-IP Audio Connections:** y

add signaling-group 3		Page 1 of 1
SIGNALING GROUP		
Group Number: 3	Group Type: sip	
	Transport Method: tls	
IMS Enabled? y		
IP Video? n		
Near-end Node Name: procr	Far-end Node Name: sm100	
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	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 30	

4.5.4. Configure a SIP Trunk Group for Mediant 3000

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. **OUTSIDE CALL**)
- **TAC:** An available trunk access code (i.e. **103**)
- **Service Type:** **tie**
- **Signaling Group:** The number of the signaling group associated (i.e. **3**)
- **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 licensed verified in **Section 4.1**)

Note: The number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

add trunk-group 3		Page 1 of 21	
TRUNK GROUP			
Group Number: 3	Group Type: sip	CDR Reports: y	
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: 103
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 3			
Number of Members: 30			

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

add trunk-group 3		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private			
UII Treatment: service-provider			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			

4.6. Configure Route Patterns

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

4.6.1. Route Pattern for Enterprise Calls

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

- **Pattern Name:** A descriptive name (i.e. **toSessionManager**)
- **Grp No:** The trunk group number from **Section 4.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

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

4.7. 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 **4**-digit extension (**Ext Len**) beginning with **35** (**Ext Code**) will result in a **4**-digit calling number (**Total Len**). The calling party number will be in the SIP “From” header.

change private-numbering 0					NUMBERING - PRIVATE FORMAT				
Ext	Ext		Trk	Private	Total				
Len	Code		Grp (s)	Prefix	Len				
4	35				4	Total Administered: 1			
						Maximum Entries: 540			

4.8. Administer Dial Plan and AAR analysis

Configure the dial plan for dialing 4-digit extensions beginning with **30** to stations registered with Communication Manager Feature Server (not shown in these Application Notes). Use the **change dialplan analysis** command to define **Dialed String 350** as an **aar Call Type**.

change dialplan analysis									
DIAL PLAN ANALYSIS TABLE									
Location: all									
Percent Full: 2									
	Dialed String	Total Length	Call Type		Dialed String	Total Length	Call Type	Dialed String	Total Length
1		3	dac						
	30	4	aar						
	35	4	ext						
9		1	fac						
*		1	fac						

Use the **change aar analysis n** command where **n** is the dial string pattern to configure an **aar** entry for **Dialed String 30** (Extensions on Communication Manager Feature Server) to use **Route Pattern 1** (defined in Section 4.6.1).

change aar analysis 0									
AAR DIGIT ANALYSIS TABLE									
Location: all									
Percent Full: 2									
	Dialed String	Total		Route	Call	Node	ANI		
		Min	Max	Pattern	Type	Num	Reqd		
	30	4	4	1	aar		n		
	35	4	4	1	aar		n		

4.9. Administer ARS Analysis

This section provides sample Auto Route Selection (ARS) used for routing calls with dialed digits beginning with **0** corresponding to national numbers accessible via the Mediant 3000. Use the **change ars analysis 0** 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. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case **0**
- **Total Min:** Minimum number of digits, in this case **3**
- **Total Max:** Maximum number of digits, in this case **25**
- **Route Pattern:** The route pattern number from **Section 4.6.1** i.e. **1**
- **Call Type:** **pubu**

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

change ars analysis 0						Page	1 of	2
ARS DIGIT ANALYSIS TABLE								
Location: all						Percent Full:		1
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
0		3	25	1	pubu		n	

4.10. Administer Feature Access Code

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

change feature-access-codes						Page	1 of	8
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: 9								
Auto Route Selection (ARS) - Access Code 1: *						Access Code 2:		
Automatic Callback Activation:						Deactivation:		

4.11. Save Changes

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

save translation		
SAVE TRANSLATION		
Command Completion Status	Error Code	
Success	0	

5. 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 [3]**. The procedures include adding the following items:

- Specify SIP Domain
- Add Locations
- Add Adaptations
- Add SIP Entities
- Add Entity Links
- Add Routing Policies
- Add Dial Patterns
- Add Session Manager
- Add Avaya Aura™ Communication Manager as Feature Server
- 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 and accept the Copyright Notice. The menu shown below is displayed. Expand the **Network Routing Policy** Link on the left side as shown.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top header shows the Avaya logo, the title "Avaya Aura™ System Manager 5.2", and a user status bar indicating "Welcome, admin" and "Last logged on at Mar. 30, 2010 12:25 AM". A navigation menu on the left lists various system management categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (highlighted with a red box), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities, Time Ranges, Personal Settings, Security, Applications, Settings, and Session Manager. Below the main menu, there are shortcuts for "Change Password", "Landing Page", "Help for Import All Data", "Help for Export All Data", and "Help for Committing configuration changes". The main content area is titled "Introduction to Network Routing Policy (NRP)" and provides a detailed overview of the NRP workflow, including a list of steps from creating domains to regular expressions, and an important note about dial patterns.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last logged on at Mar. 30, 2010 12:25 AM Help | Log off

Home / Network Routing Policy

Network Routing Policy

Introduction to Network Routing Policy (NRP)

Network Routing Policy consists of several NRP applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the NRP applications (that means the overall NRP workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other NRP applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 7: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"
 - (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 8: Create "Dial Pattern"
 - Assign the appropriate "Locations" and "Routing Policies" to the "Dial Pattern"
- Step 9: Create "Regular Expressions"
 - Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of NRP application "Dial pattern". That's why this overall NRP workflow can be interpreted as

"Dial Pattern driven approach to define routing policies"

That means (with regard to steps listed above):

- Step 7: "Routing Policies" are defined
- Step 8: "Dial Pattern" are defined and assigned to "Routing Policies" and "Locations" (one step)
- Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

5.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **SIP Domains** on the left and clicking the **New** button on the right. 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 5.2 interface. The top header includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a welcome message for user 'admin' last logged on at Mar. 26, 2010 12:25 AM. A red navigation bar contains 'Home / Network Routing Policy / SIP Domains'. On the left, a sidebar lists various management categories, with 'SIP Domains' highlighted under 'Network Routing Policy'. The main content area is titled 'Domain Management' and features a table with one item. The table has columns for Name, Type, Default, and Notes. The 'Name' column contains 'avaya.com', the 'Type' column contains 'sip', and the 'Default' column has an unchecked checkbox. Below the table, there is a red asterisk and the text '* Input Required'. At the bottom right of the main area, there are 'Commit' and 'Cancel' buttons.

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

5.2. 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 Feature Server and Mediant 3000 Gateway. To add a location, select **Locations** 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**:

- **Name:** A descriptive name
- **Notes:** Descriptive text (optional)
- **Managed Bandwidth:** Leave the default or customize as described in [5]

Under **Location Pattern**:

- **IP Address Pattern:** A pattern used to logically identify the location. In these Application Notes, the pattern selected defined the networks involved e.g. **193.120.221.*** for referring the Enterprise network and **195.189.192.*** for IP network where the Mediant 3000 Gateway resides.
- **Notes:** Descriptive text (optional)

The screen below shows addition of the **Enterprise** location, which includes all the components of the compliance environment. Click **Commit** to save.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jul. 30, 2010 1:26 AM Help | Log off

Home / Network Routing Policy / Locations / Location Details

Location Details **Commit** **Cancel**

General

* **Name:** Enterprise

Notes:

Managed Bandwidth:

* **Average Bandwidth per Call:** 80 Kbit/sec

* **Time to Live (secs):** 3600

Location Pattern

Add **Remove**

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 195.189.192.*	
<input type="checkbox"/>	* 193.120.221.*	

Select : All, None (0 of 2 Selected)

5.3. 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. Alternatively the numbering plan translation can be implemented in the Mediant 3000 Gateway. Note that the **Digit Conversion for Outgoing Calls from SM** will modify the P-AI field in the SIP invite, requiring the Mediant 3000 privacy setting to be configured as described in **Section 6.5.2**. To add an adaptation, under the **Network Routing Policy** 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**:

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

Under **Digit Conversion for Incoming Calls to SM**:

- **Matching Pattern:** The dialed number from the PSTN
- **Min/Max:** Minimum/Maximum number of digits
- **Delete Digits:** Digits to be deleted
- **Insert Digits:** Digit to be added
- **Address to modify:** Select **destination**

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

- **Matching Pattern:** The dialed number from enterprise network
- **Min/Max:** Minimum/ Maximum number of digits
- **Delete Digits:** Digits to be deleted
- **Insert Digits:** Digit to be added
- **Address to modify:** Select **origination**

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

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Apr. 14, 2010 10:00 AM Help | Log off

Home / Network Routing Policy / Adaptations / Adaptation Details

Adaptation Details [Commit] [Cancel]

General

* Adaptation name: DigitConversionAdapter

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Refresh Filter: Enable

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
1234567890	1	10	1234	5678	destination	modifies To: on Inbound

Select : All, None (0 of 1 Selected)

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Refresh Filter: Enable

Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
1234567890	1	10	1234	5678	origination	modifies P-AI: on Outbound

Select : All, None (0 of 1 Selected)

5.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity is added for the Session Manager the Proc interface for the Communication Manager Feature Server and the Mediant 3000 Gateway IP interface.

5.4.1. Adding Avaya Aura™ Communication Manager Feature Server SIP Entity

To add a SIP Entity, navigate **Network Routing Policy** → **SIP Entities** on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name (i.e. **CM-FS**)
- **FQDN or IP Address:** IP address of the Proc interface of S8300 Server, i.e. **193.120.221.180**
- **Type:** Select **CM**
- **Location:** Select one of the locations defined previously i.e. **Enterprise**
- **Time Zone:** Time zone for this entity

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

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 5.2", and a user status message: "Welcome, admin Last Logged on at Mar. 26, 2010 12:25 AM". A red breadcrumb trail shows the path: "Home / Network Routing Policy / SIP Entities / SIP Entity Details". On the left, a sidebar menu lists various management categories, with "Network Routing Policy" and its sub-item "SIP Entities" highlighted with a red box. The main content area is titled "SIP Entity Details" and contains a "General" tab. The form fields are as follows: "Name" is set to "CM-FS"; "FQDN or IP Address" is set to "193.120.221.180"; "Type" is set to "CM"; "Location" is set to "Enterprise"; and "Time Zone" is set to "Europe/Dublin". There are also checkboxes for "Override Port & Transport with DNS" and "SRV", a "SIP Timer B/F (in seconds)" field set to "4", a "Credential name" field, and a "Call Detail Recording" dropdown set to "none". At the bottom, the "SIP Link Monitoring" dropdown is set to "Use Session Manager Configuration". A red box highlights the "Commit" button in the top right corner of the form area.

5.4.2. Adding AudioCodes Mediant 3000 Gateway SIP Entity

Navigate **Network Routing Policy** → **SIP Entities** on the left and click on the **New** button on the right.

Under **General**

- **Name:** A descriptive name (i.e. **Gateway**)
- **FQDN or IP Address:** IP address of the signaling interface of Mediant 3000 Gateway, i.e. **208.209.43.59**
- **Type:** Select **Gateway**
- **Adaptation:** Select the adaptation created in **Section 5.3** i.e. **DigitConversionAdapter**
- **Location:** Select one of the locations defined previously i.e. **Enterprise**
- **Time Zone:** Time zone for this entity

Under **SIP Link Monitoring**, configure **SIP Link Monitoring** as **Use Session Manager Configuration** if Mediant 3000 is in simplex configuration or **Link Monitoring Disabled** for Mediant 3000 Gateway in HA configuration. Defaults can be used for the remaining fields. Click **Commit** to save SIP Entity definition. The screen below shows the configuration of the SIP Entity related to Mediant 3000.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jul. 30, 2010 1:26 AM Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details [Commit] [Cancel]

General

* Name: Gateway

* FQDN or IP Address: 195.189.192.150

Type: Gateway

Notes:

Adaptation: DigitConversionAdapter

Location: Enterprise

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

5.4.3. Adding Avaya Aura™ Session Manager SIP Entity

Navigate **Network Routing Policy** → **SIP Entities** on the left and click on the **New** button on the right.

Under **General**:

- **Name:** A descriptive name, i.e. **SessionManager**
- **FQDN or IP Address:** IP address of the Session Manager i.e. **193.120.221.154**, the SM-100 Security Module
- **Type:** Select **Session Manager**
- **Location:** Select one of the locations defined previously
- **Outbound Proxy:** Select the SIP Entity defined previously for Mediant 3000, i.e. **Gateway**
- **Time Zone:** Time zone for this entity

Create two Port definitions, one for **TLS** and one for **UDP**. Under **Port**, click **Add**, and then edit the fields in the resulting new row as shown below:

- **Port:** Port number on which the system listens for SIP requests
- **Protocol:** Transport protocol to be used to send SIP requests
- **Default Domain** The domain used (e.g., **avaya.com**)

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

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Apr. 08, 2010 4:35 AM Help | Log off

Home / Network Routing Policy / SIP Entities / SIP Entity Details

SIP Entity Details **Commit** **Cancel**

General

* Name: SessionManager

* FQDN or IP Address: 193.120.221.154

Type: Session Manager

Notes:

Location: Enterprise

Outbound Proxy: Gateway

Time Zone: Europe/Dublin

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port **Add** **Remove**

2 Items | Refresh Filter: Enable

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

Select: All, None (0 of 2 Selected)

5.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name
- **SIP Entity 1:** Select the **SessionManager** entity
- **Protocol:** Select the transport protocol between **UDP/TCP/TLS** to align with the definition on the **other end** of the link. In these Application Notes **TLS** was used for **Feature Server** while **UDP** or **TCP** can be used for **Mediant 3000**.
- **Port:** Port number to which the other system sends SIP requests
- **SIP Entity 2:** Select the name of the other system
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box, otherwise calls from the associated SIP Entity specified will be denied

Click **Commit** to save each Entity Link definition. The screen below illustrates adding the Entity Link for Communication Manager Feature Server.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The left-hand navigation pane shows the 'Entity Links' option under the 'Network Routing Policy' section, which is highlighted with a red circle. The main content area is titled 'Entity Links' and contains a table with one row of data. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The data row shows: Name 'SM-CMFS', SIP Entity 1 'SessionManager', Protocol 'TLS', Port '5061', SIP Entity 2 'CM-FS', Port '5061', and the 'Trusted' checkbox is checked. The 'Commit' button is highlighted with a red circle. Below the table, there is a red asterisk and the text '* Input Required'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM-CMFS	* SessionManager	TLS	* 5061	* CM-FS	* 5061	<input checked="" type="checkbox"/>	

The screen below illustrates adding the Entity Link for Mediant 3000 SIP Entity.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jul. 30, 2010 1:26 AM

Home / Network Routing Policy / Entity Links

Entity Links

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
*SM-M3K	*SessionManager	UDP	*5060	*Gateway	*5060	<input checked="" type="checkbox"/>	

* Input Required

Commit Cancel

The screen below summarizes the Entity Links view after the insertion of the two Entity Links.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jul. 30, 2010 1:26 AM

Home / Network Routing Policy / Entity Links

Entity Links

Edit New Duplicate Delete More Actions Commit

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	SM-CMAE	SessionManager	TLS	5061	CM-AE	5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM-CMFS	SessionManager	TLS	5061	CM-FS	5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM-M3K	SessionManager	UDP	5060	Gateway	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM-to-MM	SessionManager	TCP	5060	MM-MAS	5060	<input checked="" type="checkbox"/>	

Select : All, None (0 of 4 Selected)

5.6. Add Routing Policies

Routing policies describe the condition under which calls will be routed to the SIP Entities specified in **Section 5.4**. A routing policy must be added for the Mediant 3000 Gateway. To add a routing policy, select **Routing Policies** on the left and click on the **New** button on the right. The following screen is displayed. Fill in the following:

Under **General**:

- Enter a descriptive name in **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 screen shows the Routing Policy for Mediant 3000.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jul. 30, 2010 1:26 AM Help | Log off

Home / Network Routing Policy / Routing Policies / Routing Policy Details

Routing Policy Details **Commit** **Cancel**

General

* Name: RP-2-Mediant3k

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Gateway	195.189.192.150	Gateway	

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

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

Select : All, None (0 of 1 Selected)

5.7. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration numbers beginning with **0** with 3 to 25 digits reside on the Mediant 3000. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button on the right. Fill in the following, as shown in the screen below, which corresponds to the dial pattern for routing calls to Mediant 3000:

Under **General**:

- **Pattern:** Dialed number or prefix i.e. **0**
- **Min:** Minimum length of dialed number i.e. **3**
- **Max:** Maximum length of dialed number i.e. **24**
- **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 a sample the dial pattern definition for PSTN reachable with Mediant 3000.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jul. 30, 2010 1:26 AM [Help](#) | [Log off](#)

Home / Network Routing Policy / Dial Patterns / **Dial Pattern Details**

Dial Pattern Details [Commit](#) [Cancel](#)

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

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

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

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	RP-2-Mediant3k	0	<input type="checkbox"/>	Gateway	

Select : All, None (0 of 1 Selected)

5.8. Add Avaya Aura™ Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add**, and fill in the fields as described below and shown in the following screen:

Under **General**:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:**
Enter the IP address of the Session Manager management interface

Under **Security Module**:

- **Network Mask:** Enter the network mask corresponding to the IP address of the SM100 interface (i.e., **255.255.255.128**)
- **Default Gateway:** Enter the IP address of the default gateway for SM100 interface (i.e., **193.120.221.129**)

Use default values for the remaining fields. Click **Commit** to add this configuration to Session Manager.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 09, 2010 5:30 PM [Help](#) [Log off](#)

Home / Session Manager / Session Manager Administration / **Edit Session Manager**

Add Session Manager Commit Cancel

General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

General

SIP Entity Name

Description

*Management Access Point Host Name/IP

*Direct Routing to Endpoints

Security Module

SIP Entity IP Address

*Network Mask

*Default Gateway

*Call Control PHB

*QOS Priority

*Speed & Duplex

VLAN ID

5.9. Add Avaya Aura™ Communication Manager as a Feature Server

In order for Communication Manager to provide configuration and Feature Server support to SIP phones when they register to Session Manager, Communication Manager must be added as an application.

5.9.1. Create an Application Entry

Expand **Application** menu, select **Entities** on left, click on **New** (not shown). Enter the following fields and retain defaults for the remaining fields.

Under **Application**:

- **Name:** Enter a descriptive name i.e. **CM-featureServer**
- **Type:** Select **CM**
- **Node:** Select **Other..** and enter the IP address for CM SAT access i.e. **193.120.221.180**

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name, a user welcome message, and a 'Log off' link. A red breadcrumb trail shows the path: Home / Applications / Application Management / Applications Details. On the left, a sidebar menu lists various management categories, with 'Applications' and 'Entities' highlighted. The main content area is titled 'New CM Instance' and contains a form with the following fields: 'Application' (a dropdown menu), 'Name' (text input with 'CM-featureServer'), 'Type' (dropdown menu with 'CM'), 'Description' (a large text area), and 'Node' (dropdown menu with '193.120.221.180'). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

Navigate to the **Attributes** section and enter the following:

- **Login:** Login used for SAT access
- **Password:** Password used for SAT access
- **Confirm Password:** Password used for SAT access

Retain default values for the remaining fields. Click **Commit** to save.

The screenshot shows a web-based configuration form titled "Attributes". The form contains several input fields and checkboxes. Red circles are drawn around the "Login" field (containing "init"), the "Password" field (containing "*****"), the "Confirm Password" field (containing "*****"), and the "Commit" button at the bottom right. Other fields include "Is SSH Connection" (checked), "* Port" (5022), "Alternate IP Address", "RSA SSH Fingerprint (Primary IP)", "RSA SSH Fingerprint (Alternate IP)", "Is ASG Enabled" (unchecked), "ASG Key", "Confirm ASG Key", and "Location". A legend at the bottom left indicates "*Required".

Attributes
Login: init
Password: *****
Confirm Password: *****
Is SSH Connection: <input checked="" type="checkbox"/>
* Port: 5022
Alternate IP Address:
RSA SSH Fingerprint (Primary IP):
RSA SSH Fingerprint (Alternate IP):
Is ASG Enabled: <input type="checkbox"/>
ASG Key:
Confirm ASG Key:
Location:
*Required
Commit Cancel

5.9.2. Create a Feature Server Application

Navigate to **Session Manager** → **Application Configuration** → **Applications** on the left menu. Click on **New** (not shown). Enter following fields and use defaults for the remaining fields:

- **Name** A descriptive name
- **SIP Entity** Select the CM SIP Entity defined in **Section 5.4.2**

Click on **Commit** to save.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Apr. 09, 2010 4:38 AM [Help](#) [Log off](#)

Home / Session Manager / Application Configuration / Application Editor

Application Editor Commit Cancel

Application Editor

* Name

* SIP Entity

Description

Application Attributes (optional)

Name	Value
Application Handle	<input type="text"/>
URI Parameters	<input type="text"/>

5.9.3. Create a Feature Server Application Sequence

From the left menu, navigate to **Application Sequences** under **Session Manager** → **Application Configuration**. Click on **New** (not shown). Enter a descriptive **Name**. Click on the + sign next to the appropriate **Available Applications** and they will move up to the **Applications in this Sequence** section. Click on **Commit** to save.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Apr. 09, 2010 4:38 AM Help Log off

Home / Session Manager / Application Configuration / Application Sequence Editor

Application Sequence Editor [Commit] [Cancel]

Sequence Name

* Name

Description

Applications in this Sequence

[Move First] [Move Last] [Remove]

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	*	App-FeatureServer	CM-FS	<input checked="" type="checkbox"/>	

Select : All, None (0 of 1 Selected)

Available Applications

1 Item Refresh Filter: Enable

	Name	SIP Entity	Description
<input checked="" type="checkbox"/>	App-FeatureServer	CM-FS	

5.9.4. Synchronize Avaya Aura™ Communication Manager Data

Select **Communications System Management** → **Telephony** on the left. Select the appropriate **Element Name**. Select **Initialize data for selected devices**, then click on **Now**. This may take some time.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Apr. 09, 2010 6:17 AM

Home / Communication System Management / Telephony

Synchronize CM Data and Configure Options

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

Synchronize CM Data/Launch Element Cut Through

1 Item	Refresh	Filter: Enable					
<input checked="" type="checkbox"/>	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
<input checked="" type="checkbox"/>	CM-featureServer	193.120.221.180	April 9, 2010 4:00:21 AM +01:00	Incremental	Completed		R015x.02.1.016.4

Select : All, None (1 of 1 Selected)

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

Now Schedule Cancel Launch Element Cut Through

Use the menus on the left under **Monitoring** → **Scheduler** to determine when the task is complete.

5.10. Add Users for SIP Phones

Users must be added via Session Manager and the details will be updated on the CM. Select **User Management** → **User Management** on the left. Then click on **New** (not shown). Enter a **First Name** and **Last Name**.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Apr. 09, 2010 6:17 AM

Home / User Management / User Management / New User

New User Profile

General | Identity | Communication Profile | Roles | Override Permissions | Group Membership | Attribute Sets | Default Contact List | Private Contacts | Expand All | Collapse All

General

* Last Name: Joe

* First Name: Bloggs

Middle Name:

Description:

User Type:

- ☒ administrator
- ☐ communication_user
- ☐ agent
- ☐ supervisor
- ☐ resident_expert
- ☐ service_technician
- ☐ lobby_phone

Commit Cancel

Navigate to the **Identity** section and enter the following and use defaults for other fields:

- **Login Name** The desired phone extension number belonging to the domain defined in **Section 5.1**
- **Password** Password for user to log into SMGR
- **Shared Communication Profile Password** Password to be entered by the user when logging into the phone

Identity ▼

* Login Name: 3500

* Authentication Type: Basic ▼

SMGR Login Password:

* Password: ••••••

* Confirm Password: ••••••

Shared Communication Profile Password: ••••••

Confirm Password: ••••••

Localized Display Name:

Endpoint Display Name:

Honoric :

Language Preference: ▼

Time Zone: ▼

Navigate to and click on the **Communication Profile** section to expand. Then click on **Communication Address** to expand that section. Enter the following and defaults for the remaining fields:

- **Type** Select **SIP**
- **SubType** Select **username**
- **Fully Qualified Address** Enter the extension number i.e. **3500**

Click on **Add**.

Communication Profile

New Delete Done Cancel

Name
Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	SubType	Handle	Domain
No Records found			

Type: sip

SubType: username

* Fully Qualified Address: 3500 @ avaya.com

Add Cancel

Navigate to and click on **System**. Select the CM Entity.

- **Extension:** Enter a desired extension number i.e. **3500**
- **Template:** Select a telephone type template
- **Port:** Select **IP**

The **Session Manager** section to expand. Select the appropriate Session Manager server for **Session Manager Instance**. For **Origination Application Sequence** and **Termination Application Sequence** select the application sequence created in **Section 5.9.3**. Click on **Station Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

The screenshot displays a configuration interface with two main sections: **Session Manager** and **Station Profile**. Both section headers are highlighted with red boxes. In the **Session Manager** section, the following fields are highlighted: *** Session Manager Instance** (dropdown menu showing 'SessionManager'), **Origination Application Sequence** (dropdown menu showing 'AppSeq-FeatureServer'), and **Termination Application Sequence** (dropdown menu showing 'AppSeq-FeatureServer'). In the **Station Profile** section, the following fields are highlighted: *** System** (dropdown menu showing 'CM-featureServer'), **Use Existing Stations** (checkbox, currently unchecked), *** Extension** (text input field containing '3500'), *** Template** (dropdown menu showing 'DEFAULT_9630SIP'), **Set Type** (text input field containing '9630SIP'), **Security Code** (text input field), *** Port** (dropdown menu showing 'IP'), and **Delete Station on Unassign of Station from User** (checkbox, currently unchecked).

Click on **Commit** to save (not shown).

6. AudioCodes Mediant 3000 Configuration

This section displays 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) Refer to [15], [16] and [17]. 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.

6.1. Configure the Media Gateway IP Network Parameters

To configure the network parameters click on **Add Index** button to add and index with **Application Type** of **OAMP + Media + Control** and ensure the **Interface Mode** is set to **IPv4** and that **IP Address** (i.e. **195.189.192.150**) **Prefix Length** (i.e. **24**) and **Gateway** (i.e. **195.180.192.129**) are set according to the expected values.

AudioCodes TrunkPack 8410 Submit Burn Device Actions Home Help Log off

Configuration Management Status & Diagnostics

Scenarios Search

Basic Full

Network Settings

IP Settings

Application Settings

IP Routing Table

QoS Settings

SCTP Settings

Media Settings

PSTN Settings

SS7 Configuration

Multiple Interface Table

Note: Select row index to modify the relevant row.

Add Index **Done**

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP + Media + Control	IPv4 Manual	195.189.192.150	24	195.189.192.129	1	O-M-C

VLAN Mode: Disable

Native VLAN ID: 1

Network Physical Separation: Disable

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

- Navigate (not shown) to the **Maintenance Actions** page (Management tab → **Management Configuration** menu → **Maintenance Actions**).
- Under the **Reset Configuration** group, from the **Burn To FLASH** drop-down list, select **Yes**, and then click the **Reset** button; the device's new configuration (i.e., global IP address) is saved (burned) to the flash memory and the device resets and now enters HA mode (with Active and Redundant blades). The Web interface session terminates (as it's no longer accessible using the blade's private IP address).

The picture below illustrates the saving process for initial IP configuration.

▼ Reset Configuration	
Reset Board	Reset
Burn To FLASH	Yes
Graceful Option	No
▼ LOCK / UNLOCK	
Lock	LOCK
Graceful Option	No
Current Admin State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	BURN

6.1.1. Saving settings

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

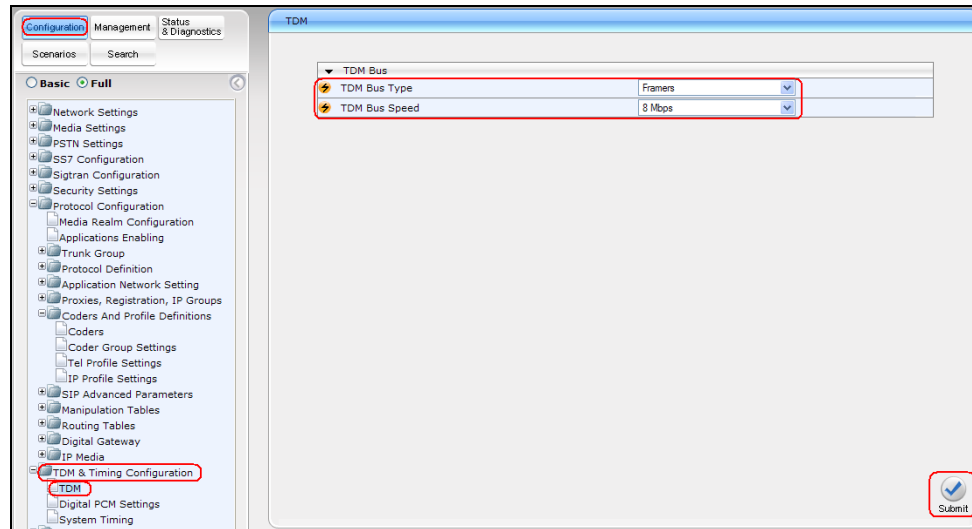
▼ Save Configuration	
Burn To FLASH	BURN

Note: If the value changed is highlighted by a lightning bolt ⚡, the setting will take place after system restart.

6.2. Configure the Media Gateway TDM and Timing Parameters

6.2.1. Configure TDM Bus

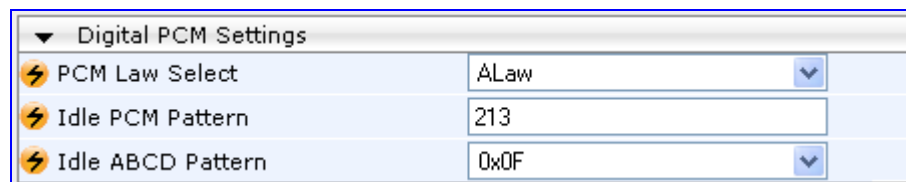
To configure the TDM Bus settings open the **TDM** page (Configuration tab → **TDM & Timing Configuration** menu → **TDM**), configure **TDM Bus Type** and **TDM Bus Speed** parameters as required. (For E1 set **TDM Bus Type** to **Frames** and **TDM Bus speed** to **8Mbps**) Click the **Submit** button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



Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.2.2. Configure digital PCM settings

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



Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.2.3. Configure system timing

To configure the device's system timing, open the **System Timing** page (**Configuration** tab → **TDM & Timing Configuration** menu → **System Timing**). Configure the parameters as required. Click the **Submit** button to save changes. The figure 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 shows the 'System Timing' configuration page. The left sidebar has a tree view with 'Configuration' and 'System Timing' highlighted. The main area displays the 'System Timing' configuration table.

System Timing	
Basic Parameter List ▲	
▼ Mode	
Timing Module Mode	StandAlone
▼ Clock Parameters	
TDM Bus Clock Source	Internal
TDM Bus Enable Fallback	Manual
TDM Bus Fallback Clock Source	Network
TDM Bits Clock Reference	1
PLL Out Of Range	OOR 9.2 to 12 ppm
TDM Bus Master-Slave Selection	SlaveMode
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_CRC4
Loopback External Ref 1	Disable
Loopback External Ref 2	Disable

Submit

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.3. Configure the Media Gateway Media Settings

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

6.3.1. Configure the Voice parameters

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

The screenshot shows the web interface of the Mediant 3000 Media Gateway. The 'Configuration' tab is active, and the 'Media Settings' menu is expanded. The 'Voice Settings' page is displayed, showing a list of parameters. The 'DTMF Transport Type' is set to 'RFC2833 Relay DTMF'. A 'Submit' button is located in the bottom right corner.

Basic Parameter List	
Voice Volume (-32 to 31 dB)	0
Input Gain (-32 to 31 dB)	0
Silence Suppression	Disable
DTMF Transport Type	RFC2833 Relay DTMF
DTMF Volume (-31 to 0 dB)	-11
NTE Max Duration	-1
CAS Transport Type	CASEventsOnly
DTMF Generation Twist	0
Echo Canceller	Enable

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.3.2. Configure the Fax Parameters

To configure FAX support, open the **Fax/Modem/CID Settings** page (**Configuration** tab → **Media Settings** menu → **Fax/Modem/CID Settings**).

Set the following values:

- **Fax Transport Mode:** **Relay/Enable**
- **Fax CNG Mode:** **Enable**
- **Fax Relay Max Rate:** **33600bps** (note that supported bit rate by the entire solution is limited by the capabilities of Communication Manger, capped at 9600bps)

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

Fax/Modem/CID Settings

General Settings	
Fax Transport Mode	Relay/Enable
Caller ID Transport Type	Mute
Caller ID Type	Standard Bellcore
V.21 Modem Transport Type	Disable
V.22 Modem Transport Type	Enable Bypass
V.23 Modem Transport Type	Enable Bypass
V.32 Modem Transport Type	Enable Bypass
V.34 Modem Transport Type	Enable Bypass
Fax CNG Mode	Enable
CNG Detector Mode	Disable

Fax Relay Settings	
Fax Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable
Fax Relay Max Rate (bps)	33600bps
T38 Version	T.38 version 0

Bypass Settings	
Fax/Modem Bypass Coder Type	G711Alaw_64
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0
Modem Bypass Output Gain	0

Submit

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.3.3. Configure the RTP/RTCP Parameters

Verify and configure RTP parameters by opening the **RTP/RTCP Settings** page (**Configuration** tab → **Media Settings** menu → **RTP / RTCP Settings**). Click the **Submit** button to save changes. The figure below illustrates setting use in these sample Application Notes.

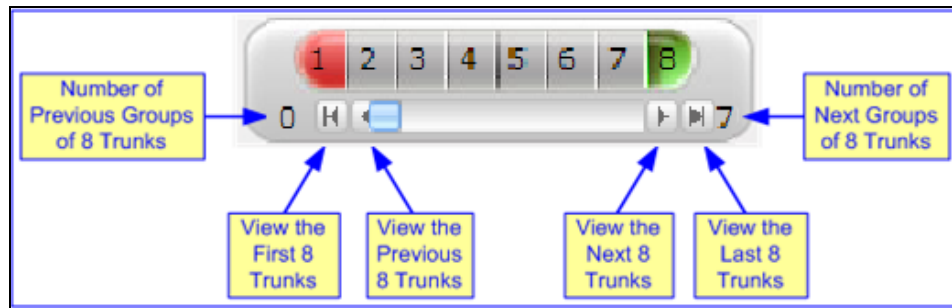
The screenshot shows the AudioCodes TrunkPack 8410 web interface. The top navigation bar includes 'Configuration', 'Management', and 'Status & Diagnostics' tabs. The left sidebar shows a tree view of settings, with 'Media Settings' and 'RTP/RTCP Settings' highlighted. The main content area displays the 'RTP/RTCP Settings' form, which includes a 'General Settings' section with various parameters and a 'Submit' button at the bottom right.

General Settings	
Dynamic Jitter Buffer Minimum Delay	10
Dynamic Jitter Buffer Optimization Factor	10
RTP Redundancy Depth	0
Packing Factor	1
Basic RTP Packet Interval	Default
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
Fax Bypass Payload Type	102
Enable RFC 3389 CN Payload Type	Enable
Comfort Noise Generation Negotiation	Disable
Remote RTP Base UDP Port	0
RTP Multiplexing Local UDP Port	0
RTP Multiplexing Remote UDP Port	0
RTP Base UDP Port	6000

Note: To save the changes to flash memory, refer to **Section 6.1.1**




6.4. Configure the Media Gateway Telephony/PSTN Interface Parameters

Open the **Trunk Settings** page (**Configuration** tab → **PSTN Settings** menu → **Trunk Settings**). Select the trunk to be configured, by clicking the desired Trunk number icon. 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:



After having selected a trunk, the following is displayed:

- The read-only **Trunk ID** field displays the selected trunk number.
- The read-only **Trunk Configuration State** displays the state of the trunk (e.g., **Active** or **Inactive**).
- The parameters displayed in the page pertain to the selected trunk only.

Click the **Stop Trunk**  button (located at the bottom of the page) to take the trunk out of service so that you can configure 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. (When all trunks are stopped, the **Apply to All Trunks**  button also appears.) All the parameters are available and can be modified. Configure the desired trunk parameters. Click the **Apply Trunk Settings** button to apply the changes to the selected trunk (or click **Apply to All Trunks** to apply the changes to all trunks); the **Stop Trunk** button replaces **Apply Trunk Settings** and the **Trunk Configuration State** displays **Active**.

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

- **Protocol Type:** **E1 EURO ISDN**
- **Line Code:** **HDB3**
- **Framing Method:** **E1 FRAMINIG MFF CRC4 EXT**
- **ISDN Termination Side:** **Network**

Refer to [15-18] to configure the different E1 types.

Trunk Settings

Basic Parameter List

General Settings

Trunk ID: 8

Trunk Configuration State: Active

Protocol Type: E1 EURO ISDN

Trunk Configuration

Clock Master: Recovered

Auto Clock Trunk Priority: 0

Line Code: HDB3

Line Build Out Loss: 0 dB

Trace Level: No Trace

Line Build Out Overwrite: OFF

Framing Method: E1 FRAMINIG MFF CRC4 EXT

ISDN Configuration

ISDN Termination Side: Network side

Q931 Layer Response Behavior: 0x0

Outgoing Calls Behavior: 0x400

Incoming Calls Behavior: 0x0

General Call Control Behavior: 0x0

NFAS Group Number: 0

IUA Interface ID: -1

NFAS Interface ID: 255

D-channel Configuration: PRIMARY

Submit

Deactivate

Stop Trunk

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5. Configure the SIP Protocol Parameters

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

6.5.1. Configure the Trunk Group Table

Open the **Trunk Group Table** page (**Configuration** tab → **Protocol Configuration** menu → **Trunk Group** submenu → **Trunk Group**). Select the appropriate **Trunk 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 [15-18]. Click the **Submit** button to save changes. The figure below illustrates setting use in these sample Application Notes.

The screenshot shows the AudioCodes TrunkPack 8410 configuration interface. The left sidebar contains a tree view of configuration categories, with 'Protocol Configuration' and 'Trunk Group' highlighted. The main area displays the 'Trunk Group Table' configuration page. At the top, there are dropdowns for 'Add Phone Context As Prefix' (set to 'Disable') and 'Trunk Group Index' (set to '1-10'). Below these is a table with 10 rows, each representing a Trunk Group Index. The table columns are: Group Index, From Trunk, To Trunk, Channels, Phone Number, Trunk Group ID, and Tel Profile ID. The first row (Index 1) is pre-filled with values: From Trunk: 8, To Trunk: 8, Channels: 1-31, Phone Number: 1000, Trunk Group ID: 5, and Tel Profile ID: 0. A 'Submit' button is located at the bottom right of the table.

Group Index	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	8	8	1-31	1000	5	0
2						
3						
4						
5						
6						
7						
8						
9						
10						

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.2. Configure the General SIP Protocol Parameters

Open the SIP General Parameters page (Configuration tab → Protocol Configuration menu → Protocol Definition submenu → SIP 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. **UDP**.
- **Use Tel URI for Asserted Identity:** Set to **Enable** if Adaptation is used on Session Manager otherwise set to **Disable**

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

SIP General Parameters

Basic Parameter List ▲

⚡ SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Enable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	T.38 Relay
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5064
Enable SIPs	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060
Use user=phone in SIP URL	Yes
Use user=phone in From Header	No
Use Tel URI for Asserted Identity	Disable
Tel to IP No Answer Timeout	180
Enable Remote Party ID	Disable
Add Number Plan and Type to RPI Header	Yes

Submit

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.3. Configure the DTMF and Dialing Parameters

Open the **DTMF & Dialing** page (**Configuration** tab → **Protocol Configuration** menu → **Protocol Definition** submenu → **DTMF & Dialing**). Set the following values:

- **Declare RFC 2833 in SDP:** **Yes**
- **1st Tx DTMF Option:** Select **RFC 2833**

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

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	96
Digit Mapping Rules	
Min Routing Overlap Digits	1
ISDN Overlap IP to Tel Dialing	Disable
Min Routing Overlap Digits	1
ISDN Overlap IP to Tel Dialing	Disable
Default Destination Number	1000
Special Digit Representation	Numeric

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.4. Configure the Proxy & Registration Parameters

Open the **Proxy & Registration** page (**Configuration** tab → **Protocol Configuration** menu → **Proxies, Registration, IP Groups** submenu → **Proxy & Registration**). Ensure that **Used Default Proxy** is set to **No** and **Enable Registration** is set to **Disable**. Click the **Submit** button to save your changes. The figure below displays the **Proxy & Registration** page for the system used in these Application Notes.

Use Default Proxy	No	▼
Proxy Name		
Redundancy Mode	Parking	▼
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 ReRouting Mode	Standard Mode	▼
Enable Registration	Disable	▼
Gateway Name		
Gateway Registration Name		
DNS Query Type	A-Record	▼
Proxy DNS Query Type	A-Record	▼
Subscription Mode	Per Endpoint	▼
Number of RTX Before Hot-Swap	3	
Use Gateway Name for OPTIONS	No	▼
User Name		
Password	Default_Passwd	
Cnonce	Default_Cnonce	
Authentication Mode	Per Endpoint	▼
Set Out-Of-Service On Registration Failure	Enable	▼
Challenge Caching Mode	None	▼
Mutual Authentication Mode	Optional	▼

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.5. Configure the Device's Coders

Open the **Coders** page (**Configuration** tab → **Protocol Configuration** menu → **Coders And Profile Definitions** submenu → **Coders**).

1. From the **Coder Name** drop-down list, select the required coder
2. 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
3. From the **Rate** drop-down list, select the bit rate (in kbps) for the selected coder
4. 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)
5. From the **Silence Suppression** drop-down list, enable or disable the silence suppression option for the selected coder
6. Repeat **Step 2** through **Step 6** for the next optional coders

Click the **Submit** button to save your changes. In the following figure are presented the codecs used in these Application Notes.

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law	20	64	8	Disabled
G.711U-law	20	64	0	Disabled
G.729	20	8	18	Disabled

Note: To save the changes to flash memory, refer to **Section 6.1.1**

The following table describes the Codec Interoperability between Communication Manager and Mediant 3000.

Avaya ip codec set	AudioCodes codec definition	
	(G.729 Annex b=no) Silence suppression=Disabled	(G.729 Annex b=yes) Silence Suppression=Enabled
G.729	ok	ok
G.729A	ok	ok
G.729B	No interop	ok
G.729AB	No interop	ok

6.5.6. Configure the IP Profile Settings

Open the **IP Profile Settings** page (**Configuration** tab → **Protocol Configuration** menu → **Coders And Profile Definitions** submenu → **IP Profile Settings**). Complete the following steps to define the **IP Profile Settings**:

1. From the **Profile ID** drop-down list, select an identification number for the IP Profile.
2. In the **Profile Name** field, enter an arbitrary name that allows you to easily identify the IP Profile.
3. From the **Profile Preference** drop-down list, select the priority of the IP Profile, where **1** is the lowest priority and **20** is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.

Note:

If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.

4. Configure the IP Profile's parameters according to your requirements. Parameters that are unique to IP Profile are described in the table below.
5. From the **Coder Group** drop-down list, select the coder group that need to be assigned assign to the IP Profile. The device's default coders can be set, or one of the coder groups defined in the **Coder Group Settings** page.
6. Repeat **Step 2** through **Step 6** for the next IP Profiles (optional).

Click the **Submit** button to save changes.

In these Application Notes, the following values were set:

- **Disconnect on Broken Connection:** **No**
- **Fax Signaling Method:** **T.38 Relay**
- **Play Ringback tone to IP:** **Play**

The figure below illustrates the **IP Profile Settings** page.

AudioCodes TrunkPack 8410 Submit Burn Device Actions Home Help Log off

Configuration Management Status & Diagnostics

Scenarios Search

Basic **Full**

Network Settings
Media Settings
PSTN Settings
SS7 Configuration
Sigtran Configuration
Security Settings
Protocol Configuration
Media Realm Configuration
Applications Enabling
Trunk Group
Protocol Definition
Application Network Setting
Proxies, Registration, IP Groups
Coders And Profile Definitions
Coders
Coder Group Settings
Tel Profile Settings
IP Profile Settings
SIP Advanced Parameters
Manipulation Tables
Routing Tables
Alternative Routing
Routing General Parameters
Tel to IP Routing
IP to Trunk Group Routing
Internal DNS Table
Internal SRV Table
Release Cause Mapping
Forward On Busy Trunk Dest
Digital Gateway
IP Media

IP Profile Settings Basic Parameter List ▲

Profile ID: 1
Profile Name:

Common Parameters

RTP IP DiffServ	46
Signaling DiffServ	40
Disconnect on Broken Connection	No
Media IP Version Preference	Only IPv4
Dynamic Jitter Buffer Minimum Delay [msec](*)	10
Dynamic Jitter Buffer Optimization Factor(*)	10
RTP Redundancy Depth(*)	0
Echo Canceled(*)	Enable
Input Gain (-32 to 31 dB)(*)	0
Voice Volume (-32 to 31 dB)(*)	0

Gateway Parameters

Fax Signaling Method	T.38 Relay
Play Ringback Tone to IP	Play
Enable Early Media	Enable
Copy Destination Number to Redirect Number	Disable
Media Security Behavior	Mandatory
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured

Submit

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.7. Configure the Advanced General Protocol Parameters

Open the **Advanced Parameters** page (**Configuration** tab → **Protocol Configuration** menu → **SIP Advanced Parameters** submenu → **Advanced Parameters**). This page allows the configuration of the defaults protocol parameters in case there is no mach on the previously configured protocol parameters. In these notes only the **Disconnect on Broken Connection** was set to **No**, other configurations may require special care. Refer to [15-18] for additional information. Click the **Submit** button to save your changes.

The screenshot shows the 'Advanced Parameters' configuration window. It has a title bar 'Advanced Parameters' and a 'Basic Parameter List' link. The window is divided into several sections, each with a collapsed arrow icon on the left:

- General**:
 - IP Security: Disable
 - Filter Calls to IP: Don't Filter
 - Enable Digit Delivery to Tel: Disable
 - Enable Digit Delivery to IP: Disable
 - PSTN Alert Timeout: 180
- Disconnect and Answer Supervision**:
 - Disconnect on Broken Connection: No** (highlighted with a red box)
 - Broken Connection Timeout [100 msec]: 100
 - Disconnect Call on Silence Detection: No
 - Silence Detection Period [sec]: 120
 - Silence Detection Method: Packets Count
 - Enable Fax Re-Routing: Disable
- CDR and Debug**:
 - CDR Server IP Address: (empty)
 - CDR Report Level: None
 - Debug Level: 5
- Misc. Parameters**:
 - Progress Indicator to IP: Not Configured
 - Enable X-Channel Header: Disable
 - Enable Busy Out: Disable
 - Graceful Busy Out Timeout [sec]: 0
 - Default Release Cause: 3
 - Max Number of Active Calls: 4032
 - Max Call Duration [min]: n

At the bottom right, there is a 'Submit' button with a checkmark icon.

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.8. Configure the Supplementary Services Parameters

Open the **Supplementary Services** page (**Configuration** tab → **Protocol Configuration** menu → **SIP Advanced Parameters** submenu → **Supplementary Services**). Set to **Enable** the following services:

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

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

Enable Hold	Enable
Enable Hold to ISDN	Disable
Hold Format	0.0.0.0
Held Timeout	-1
Enable Transfer	Enable
Transfer Prefix	
Enable Call Forward	Enable
Enable Call Waiting	Enable
Hook-Flash Code	
Enable NRT Subscription	Disable
AS Subscribe IPGroupID	-1
NRT Subscribe Retry Time	120
Call Forward Ring Tone ID	1
MLPP	
Call Priority Mode	Disable
MLPP Diffserv	50

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.9. Configure the Number Manipulation Tables

Open the required **Number Manipulation** page (**Configuration** tab → **Protocol Configuration** menu → **Manipulation Tables** submenu → **Dest Number IP→Tel**, **Dest Number Tel→IP**, **Source Number IP→Tel**, or **Source Number Tel→IP**); the relevant Manipulation table page is displayed (e.g., **Source Phone Number Manipulation Table for Tel→IP Calls** page). The figure shows the manipulation rules for Tel-to-IP source phone number manipulation, used in these Application Notes. For more information on Configuring the Number Manipulation tables refer to [15-18].

Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave	Presentation
0	-1	-1	*	*	0	0			255	Restricted

6.5.10. Configure Inbound IP Routing Rules

Open the **Inbound IP Routing Table** page (**Configuration** tab → **Protocol Configuration** menu → **Routing Tables** submenu → **IP to Trunk Group Routing**). Configure the inbound IP routing rules, refer to [15-18] for additional information on Inbound IP Routing Table. The figure below illustrates the Inbound IP Routing Table used in these Application Notes.

Index	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
1			*	*		5	0	-1
2								

6.5.11. Configure Outbound IP Routing Rules

Open the **Outbound IP Routing Table** page (**Configuration** tab → **Protocol Configuration** menu → **Routing Tables** submenu → **Tel to IP Routing**). Configure the **Src. Trunk Group ID** with the appropriate trunk number (i.e. **5**), **Dest. Phone Prefix**, **Source Phone Prefix** with the appropriate patterns (i.e. *****) and **Dest. IP Address** with the IP Address of signalling interface of Session Manager (i.e. **193.120.221.154**). For additional information on configuring Outbound IP Routing Table, refer to [15-18]. Click on **Submit** button to save changes. The following pictures illustrate the configuration done in these Application Notes.

Outbound IP Routing Table

Basic Parameter List ▲

Routing Index 1-10 ▼

Tel To IP Routing Mode Route calls before manipula

	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address
1			5	*	*	193.120.221.154
2						
3						
4						
5						
6						
7						
8						
9						
10						

Outbound IP Routing Table

Basic Parameter List ▲

1-10 ▼
Route calls before manipulation ▼

Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	IP Profile ID	Status
	193.120.221.154		Not Configured ▼	0		n/a
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			
			Not Configured ▼			

Submit

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.5.12. Configure Release Cause Mapping

Open the **Release Cause Mapping** page (**Configuration** tab → **Protocol Configuration** menu → **Routing Tables** submenu → **Release Cause Mapping**). The page is separated into two sections:

- In the **Release Cause Mapping from ISDN to SIP** group, map different Q.850 Release Causes to SIP Responses
- In the **Release Cause Mapping from SIP to ISDN** group, map different SIP Responses to Q.850 Release Causes

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 your changes. The figure below illustrates the **Release Cause Mapping** Page.

The screenshot displays the 'Release Cause Mapping' configuration page, which is divided into two main sections. The top section, titled 'Release Cause Mapping from ISDN to SIP', contains a table with 12 rows. The first row is highlighted with a red box, showing a mapping from 'Q.850 Cause' 28 to 'SIP Response' 404. The bottom section, titled 'Release Cause Mapping from SIP to ISDN', contains a table with 7 rows, all of which are currently empty. The tables have headers for 'Q.850 Cause' and 'SIP Response' respectively.

Release Cause Mapping from ISDN to SIP		
	Q.850 Cause	SIP Response
1	28	404
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Release Cause Mapping from SIP to ISDN		
	SIP Response	Q.850 Cause
1		
2		
3		
4		
5		
6		
7		

Note: To save the changes to flash memory, refer to **Section 6.1.1**

6.6. Configure the 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 **Management Settings** page (**Management** tab → **Management Configuration** menu → **Management 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. **195.189.192.148**)
- **Syslog Server Port:** Set to port utilized on the Syslog Server listening device (i.e. **514**)
- **Debug Level:** Set to **5** to capture proper level of debug information

Click the **Submit** button to save changes. The figure below illustrates setting use in these sample Application Notes.

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

The screenshot displays the 'Management Settings' page in a web interface. On the left, a navigation pane shows 'Management' selected, with 'Management Settings' highlighted under 'Management Configuration'. The main area is titled 'Management Settings' and contains three sections: 'Syslog Settings', 'SNMP Settings', and 'Activity Types to Report via 'Activity Log' Messages'. In the 'Syslog Settings' section, 'Enable Syslog' is set to 'Enable', 'Syslog Server IP Address' is '195.189.192.148', 'Syslog Server Port' is '514', 'Debug Level' is '5', and 'Trunks Filter' is '-1'. The 'SNMP Settings' section shows 'Disable SNMP' set to 'No'. The 'Activity Types to Report' section has several checkboxes, with 'Device Reset' checked. A 'Submit' button is located in the bottom right corner.

Section	Setting	Value
Syslog Settings	Enable Syslog	Enable
	Syslog Server IP Address	195.189.192.148
	Syslog Server Port	514
	Debug Level	5
	Trunks Filter	-1
SNMP Settings	SNMP Trap Destinations	[button]
	SNMP Community String	[button]
	SNMP V3 Table	[button]
	SNMP Trusted Managers	[button]
	Disable SNMP	No
Activity Types to Report via 'Activity Log' Messages	Parameters Value Change	<input type="checkbox"/>
	Auxiliary Files Loading	<input type="checkbox"/>
	Device Reset	<input checked="" type="checkbox"/>
	Flash Memory Burning	<input type="checkbox"/>
	Device Software Update	<input type="checkbox"/>
	Access to Restricted Domains	<input type="checkbox"/>
	Non-Authorized Access	<input type="checkbox"/>
Sensitive Parameters Value Change	<input type="checkbox"/>	

Note: To save the changes to flash memory, refer to **Section 6.1.1**

7. Verification Steps

This section provides the verification steps that may be performed to verify that Avaya Aura™ enterprise network can establish and receive calls with Mediant 3000.

7.1. Verify Avaya Aura™ Communication Manager Feature Server Trunk Status

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

```
status signaling-group 1
                        STATUS SIGNALING GROUP
      Group ID: 2
      Group Type: sip
      Signaling Type: facility associated signaling
      Group State: in-service
                        Active NCA-TSC Count: 0
                        Active CA-TSC Count: 0
```

```
status signaling-group 3
                        STATUS SIGNALING GROUP
      Group ID: 3
      Group Type: sip
      Signaling Type: facility associated signaling
      Group State: in-service
                        Active NCA-TSC Count: 0
                        Active CA-TSC Count: 0
```

7.2. SIP Monitoring on Avaya Aura™ Session Manager

Expand the menu on the left and navigate **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.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Apr. 14, 2010 3:50 PM [Help](#) [Log off](#)

Home / Session Manager / System Status / SIP Entity Monitoring

SIP Entity Link Monitoring Status Summary
This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances
[Refresh](#)

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
SessionManager	0/3	0	0	0

All Monitored SIP Entities
[Refresh](#)

3 Items Filter: [Enable](#)

SIP Entity Name
CM-AE
CM-FS
Gateway

7.3. Utilizing the 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.

7.3.1. Device Status

To view the status of the device's hardware components, open the **Components Status** page (**Status & Diagnostics** tab → **Status & Diagnostics** menu → **Components Status**). The figure below illustrates **Component Status** page for an HA/Redundant gateway where the TP18410 board in slot 1 is active and the second in slot 3 is Redundant.

The screenshot shows the AudioCodes TrunkPack 8410 web interface. The top navigation bar includes 'Configuration', 'Management', and 'Status & Diagnostics' (highlighted). The left sidebar shows the 'Status & Diagnostics' menu with 'Components Status' selected. The main content area displays the 'Components Status' page with the following data:

Slots	
Slot #1	TP8410, Active, Temperature(Celsius)=40
Slot #2	SAT 2, Active
Slot #3	TP8410, Redundant, Temperature(Celsius)=41
Slot #4	SAT 2, Redundant

Fan Status	
Tray	Fan Tray ID : 3, Version 0
1 Bottom Front Fan	Speed = 13440 (RPM)
2 Bottom Middle Fan	Speed = 13560 (RPM)
3 Bottom Middle Fan	Speed = 13560 (RPM)
4 Bottom Rear Fan	Speed = 11520 (RPM)
5 Top Front Fan	Speed = 13560 (RPM)
6 Top Middle Fan	Speed = 13560 (RPM)
7 Top Middle Fan	Speed = 13560 (RPM)
8 Top Rear Fan	Speed = 11520 (RPM)

Power Supply	
Top	Major
Bottom	No Alarm

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

7.3.2. Device Information

To access the **Device Information** page Open the **Device Information** page (**Status & Diagnostics** tab → **Status & Diagnostics** menu → **Device Information**).

The screenshot shows the AudioCodes TrunkPack 8410 web interface. The left sidebar shows the 'Status & Diagnostics' menu with 'Device Information' selected. The main content area displays the 'Device Information' page with the following data:

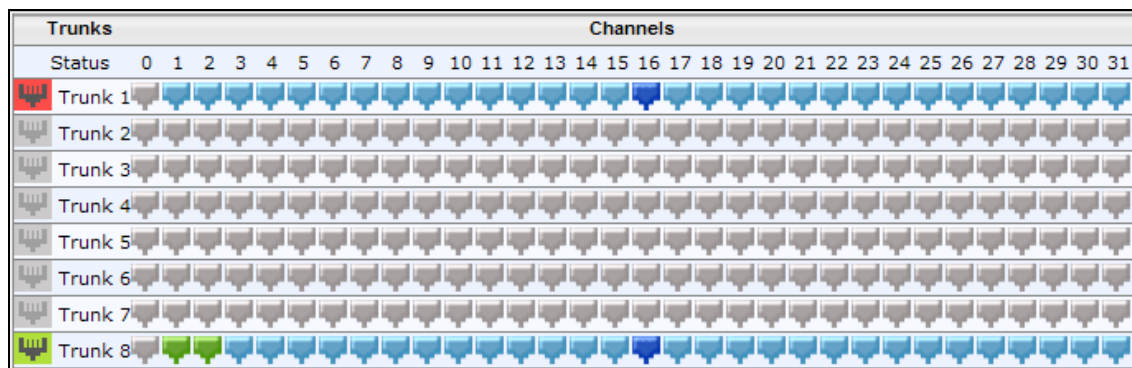
General Settings	
MAC Address:	00908f1e7553
Serial Number:	1996115
Board Type:	TrunkPack 8410
Device Up Time:	0d:4h:11m:30s:88th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [bytes]:	33554432
RAM Size [bytes]:	536870912
CPU Speed [MHz]:	450

Versions	
Version ID:	6.00A.014.005
DSP Type:	2
DSP Software Version:	60017
DSP Software Name:	491096AE3
Flash Version:	217

Loaded Files	
Call Progress Tones File Name:	usa_tones_1221.dat Delete
Loaded Coder Table :	Default CODERTABLE

7.3.3. 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 → **Status & Diagnostics** menu → **Trunks & Channels Status**). The following figure illustrates the Trunks and Channel status, where the symbol of the port in green represent channels engaged with a call.

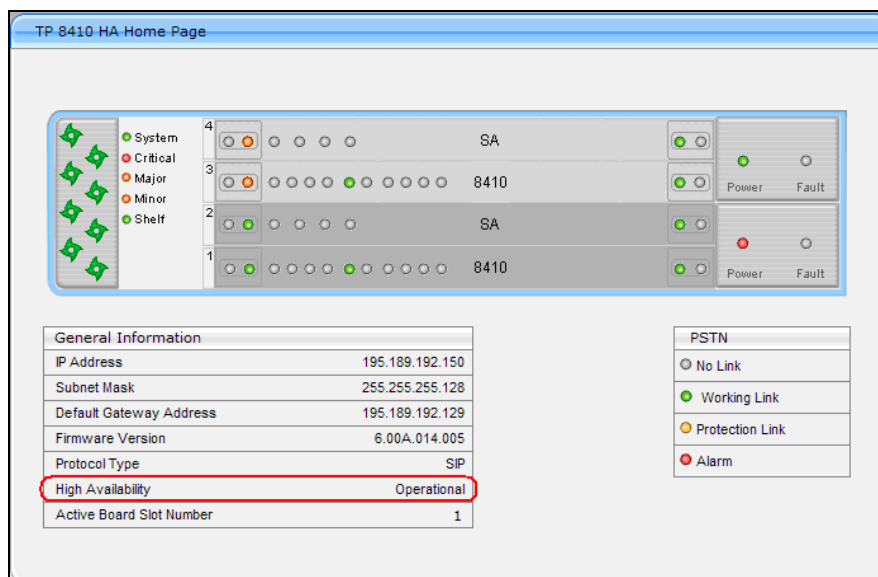


7.3.4. Gateway Home Page

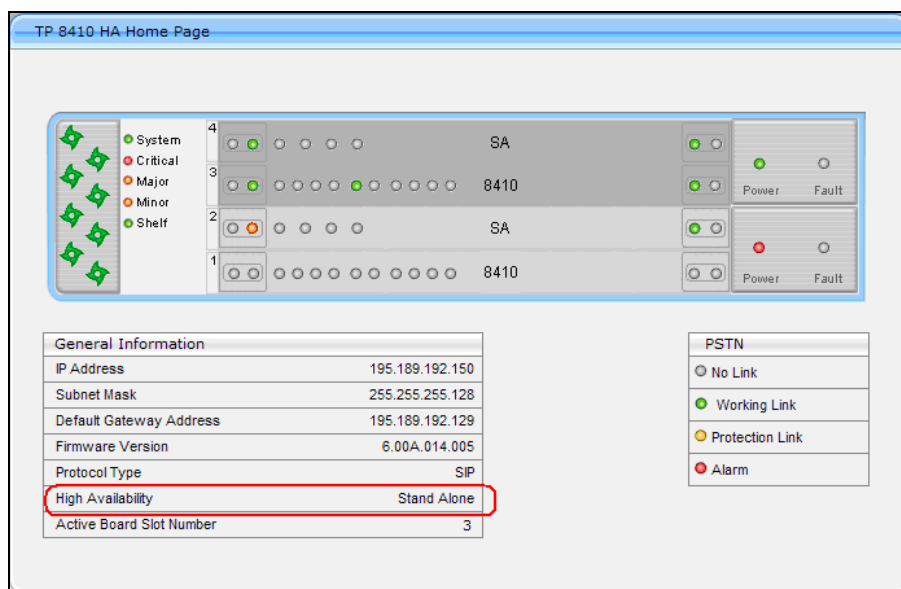
To view the status of the device home page, open the **Home** page by selecting from the top the



following ICON: . The following figure displays and HA system that has both TP8410 modules in service, ready for switchover, as described by the General information table, where **High Availability** is **Operational**.



The following figure display and HA system that has both TP8410 modules in service, but not ready for switchover, as described by the General information table, where **High Availability** is **Stand Alone**.



8. General Test Approach

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

Basic Interoperability:

- PSTN calls from and to Avaya IP endpoint
- Calling with various Avaya SIP telephone models
- Support G.711A/MU G.729A/B
- Various PTSN dialing plans including national and international calling, toll-free, operator, directory assistance and direct inward dialed calling
- SIP transport using UDP and TCP

Advanced Interoperability:

- 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
- EC500 for Communication Manager

The serviceability testing focused on verifying the ability of solution to recover from adverse conditions, such as network failures and failover between the Active/ Standby modules on the gateway.

8.1. Test Results and Remarks

All test cases were executed. During the compliance testing, it has been noted and issue with hold /resume on incoming call to SIP endpoints if shuffling is enabled on the signaling trunk group. A workaround is available by disabling shuffling on the trunk used.

9. Conclusion

As illustrated in these Application Notes, AudioCodes Mediant 3000 Gateway can successfully offer access to E1 PSTN to an enterprise telephony network built on Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager Feature Server.

10. Additional References

Avaya references, available at <http://support.avaya.com>

- [1] “Avaya Aura™ Session Manager Overview”, Document Number 03-603323, Issue 2, Release 5.2, November 2009
- [2] “Installing and Upgrading Avaya Aura™ Session Manager”, Document Number 03-603473, Issue 2, Release 5.2, November 2009
- [3] “Administering Avaya Aura™ Session Manager”, Document Number 03-603324, Issue 2.1, Release 5.2, August 2010
- [4] “Avaya Aura™ Session Manager Case Studies”, Document Number 03-603478, Issue 3, Release 6.0, June 2010
- [5] “Maintaining and Troubleshooting Avaya Aura™ Session Manager, Document Number 03-603325, Issue 1.3, Release 5.2, January 2010
- [6] “Installing and Configuring Avaya Aura™ System Platform”, Release 1.1, November 2009
- [7] “Installing and Upgrading Avaya Aura™ System Manager”, Release 5.2, January 2010
- [8] “Avaya Aura™ Communication Manager Overview”, Document Number 03-300468, Issue 6, Release 5.2, May 2009
- [9] “Administering Avaya Aura™ Communication Manager”, Document Number 03-300509, Issue 5.0, Release 5.2, May 2009
- [10] “Avaya Aura™ Communication Manager Feature Description and Implementation”, Document Number 555-245-205, Issue 7.0, Release 5.2, May 2009
- [11] “Administering Network Connectivity on Avaya Aura™ Communication Manager”, Document Number 555-233-504, Issue 14, May 2009
- [12] “SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers”, Document Number 555-245-206, Issue 9, May 2009
- [13] “Administering Avaya Aura™ Communication Manager as a Feature Server”, Document Number 03-603479, Issue 1.2, Release 5.2, January 2010
- [14] “Configuring 9600-Series SIP Phones with Avaya Aura™ Session Manager Release 5.2 – Issue 1.0”, Application Note, February 2010

AudioCodes Mediant 3000 references, are available at <http://www.audiocodes.com/support>

- [15] LTRT-69017_Mediant_2000_and_Mediant_3000_SIP_Release_Notes_Ver_6.0.pdf
- [16] LTRT-89708_Mediant_3000_SIP_User's_Manual_Ver_6.0.pdf
- [17] LTRT-94706_Mediant_3000_and_IPmedia_3000_SIP-MGCP-MEGACO_Installation_Manual_Ver_6.0.pdf
- [18] LTRT-52305_Product_Reference_Manual_for_SIP_CPE_Devices_Ver_6.0.pdf

APPENDIX

In this section are presented the relevant configuration files for the devices used in the DevConnect compliance testing.

Configure the Number Manipulation tables

Open the required **Number Manipulation** page (**Configuration** tab→**Protocol Configuration** menu → **Manipulation Tables** submenu → **Dest Number IP→Tel**, **Dest Number Tel→IP**, **Source Number IP→Tel**, or **Source Number Tel→IP**); the relevant Manipulation table page is displayed (e.g., **Source Phone Number Manipulation Table for Tel→IP Calls** page). The figure shows an example of the use of manipulation rules for Tel-to-IP source phone number manipulation:

Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left
1	-1	2	03	201	0
2	0	0		1001	4
3	-1	-1	*	123451001#	0
4	-1	-1	*	[30-40]x	0
5	-1	-1	[6,7,8]	2001	5

Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave	Presentation
0	971		255	Allowed
0	5	23	255	Restricted
0		8	4	Not Configured
1	2		255	Not Configured
0	3		255	Not Configured

Index 1: When the destination number has the prefix 03 (e.g., 035000), source number prefix 201 (e.g., 20155), and from source IP Group ID 2, the source number is changed to, for example, 97120155.

Index 2: When the source number has prefix 1001 (e.g., 1001876), it is changed to 587623.

Index 3: When the source number has prefix 123451001 (e.g., 1234510012001), it is changed to 20018.

Index 4: When the source number has prefix from 30 to 40 and a digit (e.g., 3122), it is changed to 2312.

Index 5: When the destination number has the prefix 6, 7, or 8 (e.g., 85262146), source number prefix 2001, it is changed to 3146.

From the **Table Index** drop-down list, select the range of entries that you want to edit. Configure the Number Manipulation table according to the table below. Click the **Submit** button to save your changes.

Configure outbound IP routing rules

Open the **Outbound IP Routing Table** page (**Configuration** tab → **Protocol Configuration** menu → **Routing Tables** submenu → **Tel to IP Routing**).

Routing Index

1-10

Tel To IP Routing Mode

Route calls before manipulation

	Src. IPGroupID	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	< >	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	IP Profile ID	Status
1	<div></div>			*	10	100		10.33.45.63		Not Configured <div></div>	<div></div> 1		n/a
2	<div></div>			0	20	*				Not Configured <div></div>	1 <div></div> 0		n/a
3	<div></div>			1	[30-40]	*		10.33.45.64		Not Configured <div></div>	<div></div> 0		n/a
4	<div></div>			*	[5,7-9]	*		domain.com		Not Configured <div></div>	<div></div> 0		n/a
5	<div></div>			*	00	*		0.0.0.0		Not Configured <div></div>	<div></div> 0		n/a
6	2 <div></div>	domain.com			*	*		10.33.45.65		Not Configured <div></div>	<div></div>		

The figure above shows the following configured outbound IP routing rules:

- Rule 1:** If the called phone prefix is 10 and the caller's phone prefix is 100, the call is assigned settings configured for IP Profile ID 1 and sent to IP address 10.33.45.63.
- Rule 2:** If the called phone prefix is 20 and the caller is all prefixes (*), the call is sent to the destination according to IP Group 1 (which in turn is associated with a Proxy Set ID providing the IP address).
- Rule 3:** If the called phone prefix is between 30 and 40, and the caller belongs to Trunk Group ID 1, the call is sent to IP address 10.33.45.64.
- Rule 4:** If the called phone prefix is either 5, 7, 8, or 9 and the caller is all (*), the call is sent to domain.com.
- Rule 5:** If the called phone prefix is 00 and the caller is all (*), the call is discarded.
- Rule 6:** If an incoming IP call pertaining to Source IP Group 2 with domain.com as source host prefix in its Request URI, the IP call is sent to IP address 10.33.45.65. From the **Routing Index** drop-down list, select the range of entries that you want to add. Configure the outbound IP routing rules according to the table below. Click the **Submit** button to apply your changes.

Configure inbound IP routing rules

Open the **Inbound IP Routing Table** page (**Configuration** tab → **Protocol Configuration** menu → **Routing Tables** submenu → **IP to Trunk Group Routing**).

Routing Index		1-12						
IP To Tel Routing Mode		Route calls before manipulation						
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
1			1x	*		1	2	-1
2			[501-502]	101		2	1	
3		domain.com	*	*		3		
4			*	*	10.13.64.5	-1		4

The previous figure shows the following configured inbound IP routing rules:

- Rule 1:** If the incoming IP call destination phone prefix is between 10 and 19, the call is assigned settings configured for IP Profile ID 2 and routed to Trunk Group ID 1.
- Rule 2:** If the incoming IP call destination phone prefix is between 501 and 502, and source phone prefix is 101, the call is assigned settings configured for IP Profile ID 1 and routed to Trunk Group ID 2.
- Rule 3:** If the incoming IP call has a From URI host prefix as domain.com, the call is routed to Trunk Group ID 3.
- Rule 4:** If the incoming IP call has IP address 10.13.64.5 in the INVITE's Contact header, the call is considered an IP-to-IP call and assigned to Source IP Group 4. This call is later routed according to the outbound IP routing rules for this Source IP Group configured in the **Outbound IP Routing Table**.

From the **Routing Index** drop-down list, select the range of entries that you want to add. Configure the inbound IP routing rule according to the table below. Click the **Submit** button to save your changes.

AudioCodes Mediant 3000 configuration file

Here it is presented the Mediant 3000 ini file used in these Application Notes.

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

;Board: TrunkPack 8410
;Serial Number: 1996115
;Slot Number: 1
;Software Version: 6.00A.014.005
;DSP Software Version: 491096AE3 => 600.17
;Board IP Address: 195.189.192.150
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 195.189.192.129
;Ram size: 512M   Flash size: 32M
;Num of DSP Cores: 126   Num DSP Channels: 2016
;Profile: NONE
;Key features:
;Board Type: TrunkPack 8410
;SS7 Links: MTP2=16 MTP3=16 M2UA=16 M3UA=1
;IP Media: Conf VoicePromptAnnounc(H248.9) CALEA TrunkTesting POC
;DSP Voice features: IpmDetector RTCP-XR AMRPolicyManagement
;Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB
G722 H263 H264 MPEG4 EG711
;PSTN FALLBACK Supported
;ElTrunks=84
;TlTrunks=84;Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
;PSTN Protocols: IUA=16
;Channel Type: RTP ATM PCI DspCh=2016 IPMediaDspCh=480
;M3K HA
;Control Protocols: MGCP MEGACO H323 SIP TPNCP SASurvivability IP2IP=100 MSFT
;Default features:
;Coders: G711 G726
;
;-----

[SYSTEM Params]
DNSPriServerIP = 80.179.52.100
SyslogServerIP = 195.189.192.148
EnableSyslog = 1

[BSP Params]
PCMLawSelect = 1
TDMBusSpeed = 3
StorageServerNetworkAddress = 255.255.255.255

[ControlProtocols Params]
AdminStateLockControl = 0
cpRecordCoder = 'PCMA'
[MGCP Params]

[MEGACO Params]
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 0
EP_Num_3 = 0
EP_Num_4 = 0

[PSTN Params]
```

```
ProtocolType_0 = 1
ProtocolType_1 = 0
ProtocolType_2 = 0
ProtocolType_3 = 0
ProtocolType_4 = 0
ProtocolType_5 = 0
ProtocolType_6 = 0
ProtocolType_7 = 1
ProtocolType_8 = 0
ProtocolType_9 = 0
ProtocolType_10 = 0
ProtocolType_11 = 0
ProtocolType_12 = 0
ProtocolType_13 = 0
ProtocolType_14 = 0
ProtocolType_15 = 0
ProtocolType_16 = 0
ProtocolType_17 = 0
ProtocolType_18 = 0
ProtocolType_19 = 0
ProtocolType_20 = 0
ProtocolType_21 = 0
ProtocolType_22 = 0
ProtocolType_23 = 0
ProtocolType_24 = 0
ProtocolType_25 = 0
ProtocolType_26 = 0
ProtocolType_27 = 0
ProtocolType_28 = 0
ProtocolType_29 = 0
ProtocolType_30 = 0
ProtocolType_31 = 0
ProtocolType_32 = 0
ProtocolType_33 = 0
ProtocolType_34 = 0
ProtocolType_35 = 0
ProtocolType_36 = 0
ProtocolType_37 = 0
ProtocolType_38 = 0
ProtocolType_39 = 0
ProtocolType_40 = 0
ProtocolType_41 = 0
ProtocolType_42 = 0
ProtocolType_43 = 0
ProtocolType_44 = 0
ProtocolType_45 = 0
ProtocolType_46 = 0
ProtocolType_47 = 0
ProtocolType_48 = 0
ProtocolType_49 = 0
ProtocolType_50 = 0
ProtocolType_51 = 0
ProtocolType_52 = 0
ProtocolType_53 = 0
ProtocolType_54 = 0
ProtocolType_55 = 0
ProtocolType_56 = 0
ProtocolType_57 = 0
ProtocolType_58 = 0
ProtocolType_59 = 0
ProtocolType_60 = 0
ProtocolType_61 = 0
```



```
ProtocolType_62 = 0
ClockMaster_0 = 1
ClockMaster_1 = 0
ClockMaster_2 = 0
ClockMaster_3 = 0
ClockMaster_4 = 0
ClockMaster_5 = 0
ClockMaster_6 = 0
ClockMaster_7 = 0
ClockMaster_8 = 0
ClockMaster_9 = 0
ClockMaster_10 = 0
ClockMaster_11 = 0
ClockMaster_12 = 0
ClockMaster_13 = 0
ClockMaster_14 = 0
ClockMaster_15 = 0
ClockMaster_16 = 0
ClockMaster_17 = 0
ClockMaster_18 = 0
ClockMaster_19 = 0
ClockMaster_20 = 0
ClockMaster_21 = 0
ClockMaster_22 = 0
ClockMaster_23 = 0
ClockMaster_24 = 0
ClockMaster_25 = 0
ClockMaster_26 = 0
ClockMaster_27 = 0
ClockMaster_28 = 0
ClockMaster_29 = 0
ClockMaster_30 = 0
ClockMaster_31 = 0
ClockMaster_32 = 0
ClockMaster_33 = 0
ClockMaster_34 = 0
ClockMaster_35 = 0
ClockMaster_36 = 0
ClockMaster_37 = 0
ClockMaster_38 = 0
ClockMaster_39 = 0
ClockMaster_40 = 0
ClockMaster_41 = 0
ClockMaster_42 = 0
ClockMaster_43 = 0
ClockMaster_44 = 0
ClockMaster_45 = 0
ClockMaster_46 = 0
ClockMaster_47 = 0
ClockMaster_48 = 0
ClockMaster_49 = 0
ClockMaster_50 = 0
ClockMaster_51 = 0
ClockMaster_52 = 0
ClockMaster_53 = 0
ClockMaster_54 = 0
ClockMaster_55 = 0
ClockMaster_56 = 0
ClockMaster_57 = 0
ClockMaster_58 = 0
ClockMaster_59 = 0
ClockMaster_60 = 0
```

```
ClockMaster_61 = 0
ClockMaster_62 = 0
TerminationSide_0 = 1
TerminationSide_1 = 0
TerminationSide_2 = 0
TerminationSide_3 = 0
TerminationSide_4 = 0
TerminationSide_5 = 0
TerminationSide_6 = 0
TerminationSide_7 = 1
TerminationSide_8 = 0
TerminationSide_9 = 0
TerminationSide_10 = 0
TerminationSide_11 = 0
TerminationSide_12 = 0
TerminationSide_13 = 0
TerminationSide_14 = 0
TerminationSide_15 = 0
TerminationSide_16 = 0
TerminationSide_17 = 0
TerminationSide_18 = 0
TerminationSide_19 = 0
TerminationSide_20 = 0
TerminationSide_21 = 0
TerminationSide_22 = 0
TerminationSide_23 = 0
TerminationSide_24 = 0
TerminationSide_25 = 0
TerminationSide_26 = 0
TerminationSide_27 = 0
TerminationSide_28 = 0
TerminationSide_29 = 0
TerminationSide_30 = 0
TerminationSide_31 = 0
TerminationSide_32 = 0
TerminationSide_33 = 0
TerminationSide_34 = 0
TerminationSide_35 = 0
TerminationSide_36 = 0
TerminationSide_37 = 0
TerminationSide_38 = 0
TerminationSide_39 = 0
TerminationSide_40 = 0
TerminationSide_41 = 0
TerminationSide_42 = 0
TerminationSide_43 = 0
TerminationSide_44 = 0
TerminationSide_45 = 0
TerminationSide_46 = 0
TerminationSide_47 = 0
TerminationSide_48 = 0
TerminationSide_49 = 0
TerminationSide_50 = 0
TerminationSide_51 = 0
TerminationSide_52 = 0
TerminationSide_53 = 0
TerminationSide_54 = 0
TerminationSide_55 = 0
TerminationSide_56 = 0
TerminationSide_57 = 0
TerminationSide_58 = 0
TerminationSide_59 = 0
```

```
TerminationSide_60 = 0
TerminationSide_61 = 0
TerminationSide_62 = 0
FramingMethod_0 = c
FramingMethod_1 = 0
FramingMethod_2 = 0
FramingMethod_3 = 0
FramingMethod_4 = 0
FramingMethod_5 = 0
FramingMethod_6 = 0
FramingMethod_7 = c
FramingMethod_8 = 0
FramingMethod_9 = 0
FramingMethod_10 = 0
FramingMethod_11 = 0
FramingMethod_12 = 0
FramingMethod_13 = 0
FramingMethod_14 = 0
FramingMethod_15 = 0
FramingMethod_16 = 0
FramingMethod_17 = 0
FramingMethod_18 = 0
FramingMethod_19 = 0
FramingMethod_20 = 0
FramingMethod_21 = 0
FramingMethod_22 = 0
FramingMethod_23 = 0
FramingMethod_24 = 0
FramingMethod_25 = 0
FramingMethod_26 = 0
FramingMethod_27 = 0
FramingMethod_28 = 0
FramingMethod_29 = 0
FramingMethod_30 = 0
FramingMethod_31 = 0
FramingMethod_32 = 0
FramingMethod_33 = 0
FramingMethod_34 = 0
FramingMethod_35 = 0
FramingMethod_36 = 0
FramingMethod_37 = 0
FramingMethod_38 = 0
FramingMethod_39 = 0
FramingMethod_40 = 0
FramingMethod_41 = 0
FramingMethod_42 = 0
FramingMethod_43 = 0
FramingMethod_44 = 0
FramingMethod_45 = 0
FramingMethod_46 = 0
FramingMethod_47 = 0
FramingMethod_48 = 0
FramingMethod_49 = 0
FramingMethod_50 = 0
FramingMethod_51 = 0
FramingMethod_52 = 0
FramingMethod_53 = 0
FramingMethod_54 = 0
FramingMethod_55 = 0
FramingMethod_56 = 0
FramingMethod_57 = 0
FramingMethod_58 = 0
```

```
FramingMethod_59 = 0
FramingMethod_60 = 0
FramingMethod_61 = 0
FramingMethod_62 = 0
LineCode_0 = 2
LineCode_1 = 0
LineCode_2 = 0
LineCode_3 = 0
LineCode_4 = 0
LineCode_5 = 0
LineCode_6 = 0
LineCode_7 = 2
LineCode_8 = 0
LineCode_9 = 0
LineCode_10 = 0
LineCode_11 = 0
LineCode_12 = 0
LineCode_13 = 0
LineCode_14 = 0
LineCode_15 = 0
LineCode_16 = 0
LineCode_17 = 0
LineCode_18 = 0
LineCode_19 = 0
LineCode_20 = 0
LineCode_21 = 0
LineCode_22 = 0
LineCode_23 = 0
LineCode_24 = 0
LineCode_25 = 0
LineCode_26 = 0
LineCode_27 = 0
LineCode_28 = 0
LineCode_29 = 0
LineCode_30 = 0
LineCode_31 = 0
LineCode_32 = 0
LineCode_33 = 0
LineCode_34 = 0
LineCode_35 = 0
LineCode_36 = 0
LineCode_37 = 0
LineCode_38 = 0
LineCode_39 = 0
LineCode_40 = 0
LineCode_41 = 0
LineCode_42 = 0
LineCode_43 = 0
LineCode_44 = 0
LineCode_45 = 0
LineCode_46 = 0
LineCode_47 = 0
LineCode_48 = 0
LineCode_49 = 0
LineCode_50 = 0
LineCode_51 = 0
LineCode_52 = 0
LineCode_53 = 0
LineCode_54 = 0
LineCode_55 = 0
LineCode_56 = 0
LineCode_57 = 0
```

```
LineCode_58 = 0
LineCode_59 = 0
LineCode_60 = 0
LineCode_61 = 0
LineCode_62 = 0
CASProtocolEnable = 0
[SS7 Params]
[Voice Engine Params]
CallProgressTonesFilename = 'usa_tones_1221.dat'
DisableRTCPRandomize = 1
DTMFDetectorSensitivity = 1
SRPTxPacketMKISize = 1
[WEB Params]
LogoWidth = '145'
HTTPSCipherString = 'ALL'
```

```
[SIP Params]
PLAYRBTONE2IP = 1
MEDIACHANNELS = 60
PLAYRBTONE2TEL = 1
USESIPURIFORDIVERSIONHEADER = 1
CHANNELSELECTMODE = 1
GWDEBUGLEVEL = 5
ENABLEEARMEDIA = 1
SIPGATEWAYNAME = '195.189.192.138'
DISCONNECTONBROKENCONNECTION = 0
ISFAXUSED = 1
HOLDFORMAT = 1
SIPTRANSPORTTYPE = 1
TLSLOCALSIPPORT = 5064
LOCALISDNRBSSOURCE = 1
MEDIASECURITYBEHAVIOUR = 1
USEDIGITFORSPECIALDTMF = 1
FAXCNGMODE = 1
DIGITALOOSBEHAVIORFORTRUNK_0 = 0
DIGITALOOSBEHAVIORFORTRUNK_1 = -1
DIGITALOOSBEHAVIORFORTRUNK_2 = -1
DIGITALOOSBEHAVIORFORTRUNK_3 = -1
DIGITALOOSBEHAVIORFORTRUNK_4 = -1
DIGITALOOSBEHAVIORFORTRUNK_5 = -1
DIGITALOOSBEHAVIORFORTRUNK_6 = -1
DIGITALOOSBEHAVIORFORTRUNK_7 = 0
DIGITALOOSBEHAVIORFORTRUNK_8 = -1
DIGITALOOSBEHAVIORFORTRUNK_9 = -1
DIGITALOOSBEHAVIORFORTRUNK_10 = -1
DIGITALOOSBEHAVIORFORTRUNK_11 = -1
DIGITALOOSBEHAVIORFORTRUNK_12 = -1
DIGITALOOSBEHAVIORFORTRUNK_13 = -1
DIGITALOOSBEHAVIORFORTRUNK_14 = -1
DIGITALOOSBEHAVIORFORTRUNK_15 = -1
DIGITALOOSBEHAVIORFORTRUNK_16 = -1
DIGITALOOSBEHAVIORFORTRUNK_17 = -1
DIGITALOOSBEHAVIORFORTRUNK_18 = -1
DIGITALOOSBEHAVIORFORTRUNK_19 = -1
DIGITALOOSBEHAVIORFORTRUNK_20 = -1
DIGITALOOSBEHAVIORFORTRUNK_21 = -1
DIGITALOOSBEHAVIORFORTRUNK_22 = -1
DIGITALOOSBEHAVIORFORTRUNK_23 = -1
DIGITALOOSBEHAVIORFORTRUNK_24 = -1
DIGITALOOSBEHAVIORFORTRUNK_25 = -1
DIGITALOOSBEHAVIORFORTRUNK_26 = -1
DIGITALOOSBEHAVIORFORTRUNK_27 = -1
```

```

DIGITALOOSBEHAVIORFORTRUNK_28 = -1
DIGITALOOSBEHAVIORFORTRUNK_29 = -1
DIGITALOOSBEHAVIORFORTRUNK_30 = -1
DIGITALOOSBEHAVIORFORTRUNK_31 = -1
DIGITALOOSBEHAVIORFORTRUNK_32 = -1
DIGITALOOSBEHAVIORFORTRUNK_33 = -1
DIGITALOOSBEHAVIORFORTRUNK_34 = -1
DIGITALOOSBEHAVIORFORTRUNK_35 = -1
DIGITALOOSBEHAVIORFORTRUNK_36 = -1
DIGITALOOSBEHAVIORFORTRUNK_37 = -1
DIGITALOOSBEHAVIORFORTRUNK_38 = -1
DIGITALOOSBEHAVIORFORTRUNK_39 = -1
DIGITALOOSBEHAVIORFORTRUNK_40 = -1
DIGITALOOSBEHAVIORFORTRUNK_41 = -1
DIGITALOOSBEHAVIORFORTRUNK_42 = -1
DIGITALOOSBEHAVIORFORTRUNK_43 = -1
DIGITALOOSBEHAVIORFORTRUNK_44 = -1
DIGITALOOSBEHAVIORFORTRUNK_45 = -1
DIGITALOOSBEHAVIORFORTRUNK_46 = -1
DIGITALOOSBEHAVIORFORTRUNK_47 = -1
DIGITALOOSBEHAVIORFORTRUNK_48 = -1
DIGITALOOSBEHAVIORFORTRUNK_49 = -1
DIGITALOOSBEHAVIORFORTRUNK_50 = -1
DIGITALOOSBEHAVIORFORTRUNK_51 = -1
DIGITALOOSBEHAVIORFORTRUNK_52 = -1
DIGITALOOSBEHAVIORFORTRUNK_53 = -1
DIGITALOOSBEHAVIORFORTRUNK_54 = -1
DIGITALOOSBEHAVIORFORTRUNK_55 = -1
DIGITALOOSBEHAVIORFORTRUNK_56 = -1
DIGITALOOSBEHAVIORFORTRUNK_57 = -1
DIGITALOOSBEHAVIORFORTRUNK_58 = -1
DIGITALOOSBEHAVIORFORTRUNK_59 = -1
DIGITALOOSBEHAVIORFORTRUNK_60 = -1
DIGITALOOSBEHAVIORFORTRUNK_61 = -1
DIGITALOOSBEHAVIORFORTRUNK_62 = -1

```

[SCTP Params]

[VXML Params]

[IPsec Params]

[Audio Staging Params]

[SNMP Params]

[Video Params]

```

;
; *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts
;
;
; *** TABLE PREFIX ***
;
;
[ PREFIX ]
FORMAT PREFIX_Index = PREFIX_DestinationPrefix, PREFIX_DestAddress,
PREFIX_SourcePrefix, PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort,
PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_DestIPGroupID,
PREFIX_SrcHostPrefix, PREFIX_TransportType, PREFIX_SrcTrunkGroupID;

```

```

PREFIX 0 = *, 193.120.221.154, *, 0, 255, 0, -1, , -1, , -1, 5;
[ \PREFIX ]
;
; *** TABLE CoderName ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts
;
;
; *** TABLE TrunkGroup ***
;
;
[ TrunkGroup ]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber,
TrunkGroup_ProfileId, TrunkGroup_LastTrunkId, TrunkGroup_Module;
TrunkGroup 0 = 5, 7, 1, 31, 1000, 0, 7, 255;
[ \TrunkGroup ]
;
; *** TABLE NumberMapIp2Tel ***
;
;
[ NumberMapIp2Tel ]
FORMAT NumberMapIp2Tel_Index = NumberMapIp2Tel_DestinationPrefix,
NumberMapIp2Tel_SourcePrefix, NumberMapIp2Tel_SourceAddress,
NumberMapIp2Tel_NumberType, NumberMapIp2Tel_NumberPlan,
NumberMapIp2Tel_RemoveFromLeft, NumberMapIp2Tel_RemoveFromRight,
NumberMapIp2Tel_LeaveFromRight, NumberMapIp2Tel_Prefix2Add,
NumberMapIp2Tel_Suffix2Add, NumberMapIp2Tel_IsPresentationRestricted,
NumberMapIp2Tel_SrcTrunkGroupID, NumberMapIp2Tel_SrcIPGroupID;
NumberMapIp2Tel 1 = *, *, *, 255, 255, 0, 0, 255, , , 255, -1, -1;
[ \NumberMapIp2Tel ]
;
; *** TABLE NumberMapTel2Ip ***
;
;
[ NumberMapTel2Ip ]
FORMAT NumberMapTel2Ip_Index = NumberMapTel2Ip_DestinationPrefix,
NumberMapTel2Ip_SourcePrefix, NumberMapTel2Ip_SourceAddress,
NumberMapTel2Ip_NumberType, NumberMapTel2Ip_NumberPlan,
NumberMapTel2Ip_RemoveFromLeft, NumberMapTel2Ip_RemoveFromRight,
NumberMapTel2Ip_LeaveFromRight, NumberMapTel2Ip_Prefix2Add,
NumberMapTel2Ip_Suffix2Add, NumberMapTel2Ip_IsPresentationRestricted,
NumberMapTel2Ip_SrcTrunkGroupID, NumberMapTel2Ip_SrcIPGroupID;
NumberMapTel2Ip 0 = +, 44*, *, 255, 255, 0, 0, 255, , , 255, -1, -1;
NumberMapTel2Ip 1 = , 44*, *, 255, 255, 0, 0, 255, +1, , 255, -1, -1;
[ \NumberMapTel2Ip ]
;
; *** TABLE SourceNumberMapIp2Tel ***
;
;
[ SourceNumberMapIp2Tel ]
FORMAT SourceNumberMapIp2Tel_Index = SourceNumberMapIp2Tel_DestinationPrefix,
SourceNumberMapIp2Tel_SourcePrefix, SourceNumberMapIp2Tel_SourceAddress,
SourceNumberMapIp2Tel_NumberType, SourceNumberMapIp2Tel_NumberPlan,
SourceNumberMapIp2Tel_RemoveFromLeft, SourceNumberMapIp2Tel_RemoveFromRight,
SourceNumberMapIp2Tel_LeaveFromRight, SourceNumberMapIp2Tel_Prefix2Add,
SourceNumberMapIp2Tel_Suffix2Add, SourceNumberMapIp2Tel_IsPresentationRestricted,
SourceNumberMapIp2Tel_SrcTrunkGroupID, SourceNumberMapIp2Tel_SrcIPGroupID;
SourceNumberMapIp2Tel 0 = *, +1, *, 255, 255, 2, 0, 255, , , 255, -1, -1;
SourceNumberMapIp2Tel 1 = *, +, *, 255, 255, 1, 0, 255, , , 255, -1, -1;
[ \SourceNumberMapIp2Tel ]
;

```

```

; *** TABLE PstnPrefix ***
;
;
[ PstnPrefix ]
FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId,
PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId,
PstnPrefix_SrcIPGroupId, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix;
PstnPrefix_0 = *, 5, *, , 0, -1, , ;
[ \PstnPrefix ]
;
; *** TABLE CauseMapIsdn2Sip ***
;
;
[ CauseMapIsdn2Sip ]
FORMAT CauseMapIsdn2Sip_Index = CauseMapIsdn2Sip_IsdnReleaseCause,
CauseMapIsdn2Sip_SipResponse;
CauseMapIsdn2Sip_0 = 28, 404;
[ \CauseMapIsdn2Sip ]
;
; *** TABLE ProxyIp ***
;
;
[ ProxyIp ]
FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_ProxySetId;
ProxyIp_2 = 195.189.192.142, 0, 3;
[ \ProxyIp ]
;
; *** TABLE TxDtmfOption ***
;
;
[ TxDtmfOption ]
FORMAT TxDtmfOption_Index = TxDtmfOption_Type;
TxDtmfOption_0 = 4;
[ \TxDtmfOption ]
;
; *** TABLE ProxySet ***
;
;
[ ProxySet ]
FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD,
ProxySet_ClassificationInput;
ProxySet_0 = 0, 60, 0, 0, 0, 0;
ProxySet_3 = 0, 60, 0, 0, 0, 0;
[ \ProxySet ]
;
; *** TABLE IPGroup ***
;
;
[ IPGroup ]
FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability,
IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable,
IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet,
IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet,
IPGroup_OutboundManSet;
IPGroup_1 = 0, , -1, , , 0, -1, 0, 0, -1, 0, , 1, 0, -1, -1, -1;
IPGroup_2 = 0, , -1, , , 0, -1, 0, 0, -1, 0, , 1, 0, -1, -1, -1;
[ \IPGroup ]
;
; *** TABLE CodersGroup0 ***
;

```



```

;
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime, CodersGroup0_rate,
CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g711Alaw64k, 20, 0, -1, 0;
CodersGroup0 1 = g711Ulaw64k, 20, 0, -1, 0;
CodersGroup0 2 = g729, 20, 0, -1, 0;
[ \CodersGroup0 ]
;
; *** TABLE CodersGroup1 ***
;
;
[ CodersGroup1 ]
FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime, CodersGroup1_rate,
CodersGroup1_PayloadType, CodersGroup1_Sce;
CodersGroup1 0 = g711Alaw64k, 20, 0, -1, 0;
[ \CodersGroup1 ]
;
; *** TABLE CodersGroup2 ***
;
;
[ CodersGroup2 ]
FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime, CodersGroup2_rate,
CodersGroup2_PayloadType, CodersGroup2_Sce;
CodersGroup2 0 = g729, 20, 0, -1, 0;
[ \CodersGroup2 ]
;
; *** TABLE InterfaceTable ***
;
;
[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength,
InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName;
InterfaceTable 0 = 6, 10, 195.189.192.150, 24, 195.189.192.129, 1, O+M+C;
[ \InterfaceTable ]

```

©2010 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.