



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura™ Communication Manager, Avaya Modular Messaging, Avaya Aura™ Session Manager and Avaya Aura™ System Manager to Support IPC System Interconnect – Issue 1.0

Abstract

These application notes describe the procedure to configure Avaya Aura™ Communication Manager, Avaya Modular Messaging, Avaya Aura™ Session Manager and Avaya Aura™ System Manager to support IPC Alliance MX and IPC ESS (Enterprise SIP Servers) using SIP (Session Initiation Protocol) connectivity between the two enterprises.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The objective of this compliance test is to verify the System Interconnect (SI) solution provided by IPC can interoperate with Avaya Aura™ Communication Manager, Avaya Modular Messaging, Avaya Aura™ Session Manager and Avaya Aura™ System Manager. System Interconnect is a SIP solution, which consists of the following IPC components:

- IPC Alliance MX
- IPC ESS (Enterprise SIP Server)
- IPC System Center
- IPC turrets

The Alliance MX is a voice technology product designed to provide a high resiliency platform for the provision of telephony and other associated services to financial traders. The Alliance MX provides its users with connectivity to various telephone transport services. IPC ESS is a SIP proxy server, IPC System Center is the administration terminal for the Alliance MX. IPC turrets are SIP-based VoIP turrets. Based on the IPC support policy, there is no IPC configuration documented in this Application Notes. IPC engineers will be responsible for the installation and maintenance of Alliance MX products.

These Application Notes describe the required configuration steps for Avaya Aura™ Communication Manager, Avaya Aura™ System Manager and Avaya Modular Messaging.

1.1. Interoperability Compliance Testing

The interoperability compliance test focused on the ability for the IPC solution to interoperate with the Avaya solution. The following is a summary of the feature and serviceability testing that was undertaken.

- Basic Calls, which included calling/connected party name/number display and restriction
- Codec Negotiation
- Hold, Return from Hold
- Conference
- Call Transfer including calling/connected party name/number display and restriction at the primary and secondary party of the transfer
- Call forward with tests for call forward unconditional, call forward busy and call forward no reply
- Multiple call forward including calling/connected party name/number display at the calling and the diverted to party of the call forward
- Call forward, loop avoidance
- Mail box access and message retrieval
- Message waiting indicator, activation and deactivation

1.2. Support

Technical support for the Avaya products can be obtained from Avaya. See the support link at support.avaya.com for contact information.

Technical support for the IPC products can be obtained from IPC. See the support link at www.ipc.com for contact information.

2. Reference Configuration

Figure 1 illustrates the network topology of the lab environment used for compliance testing. The Avaya and IPC solutions are connected over an IP network; calls are routed between the two solutions and connected via SIP. The SIP connectivity is provided by the Session Manager and the IPC ESS.

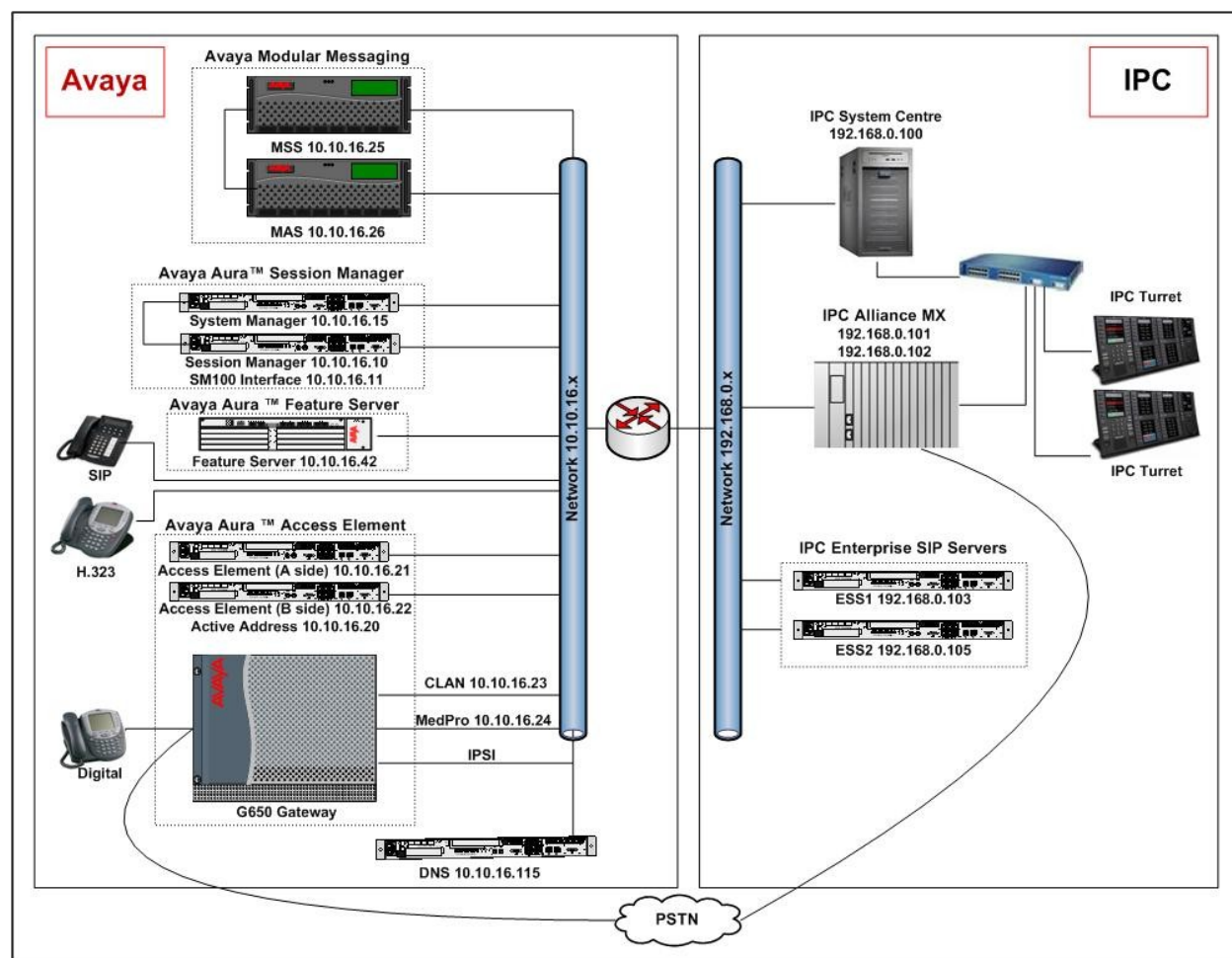


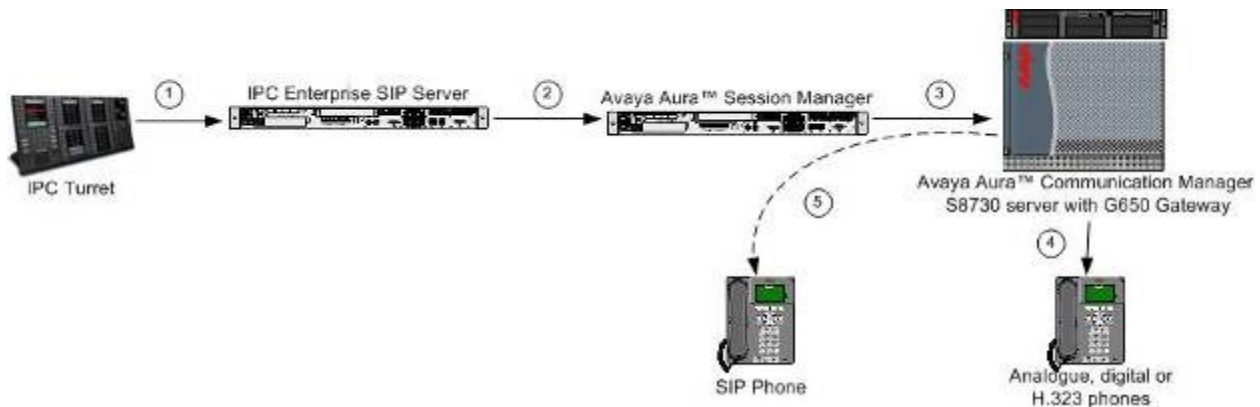
Figure 1: Test Environment Network Topology

To better understand how calls are routed between the two enterprise solutions shown in **Figure 1**. Three example call flows are described in this section, the first call scenario is an incoming call from IPC to an Avaya H.323, digital or analog extension on the Communication Manager Access Element.

1. An IPC user dials a number which is assigned to an Avaya telephone.
2. Based on the dialed number IPC ESS routes the call to the Session Manager
3. Session Manager routes the call to Communication Manager using a SIP trunk
4. Communication Manager rings the analog, digital, or H.323 telephone.

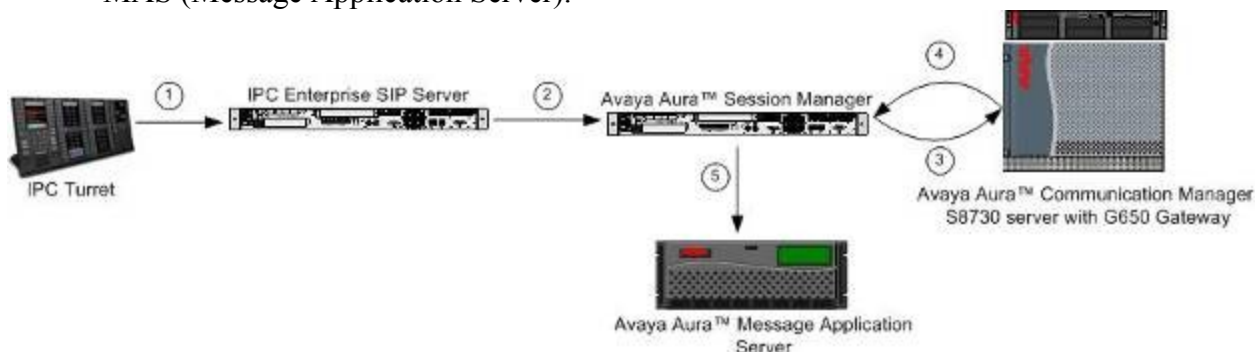
Or

5. If the Communication Manager is a Feature Server, the call will be directed back via the Session Manager to the SIP station that will be registered with it.



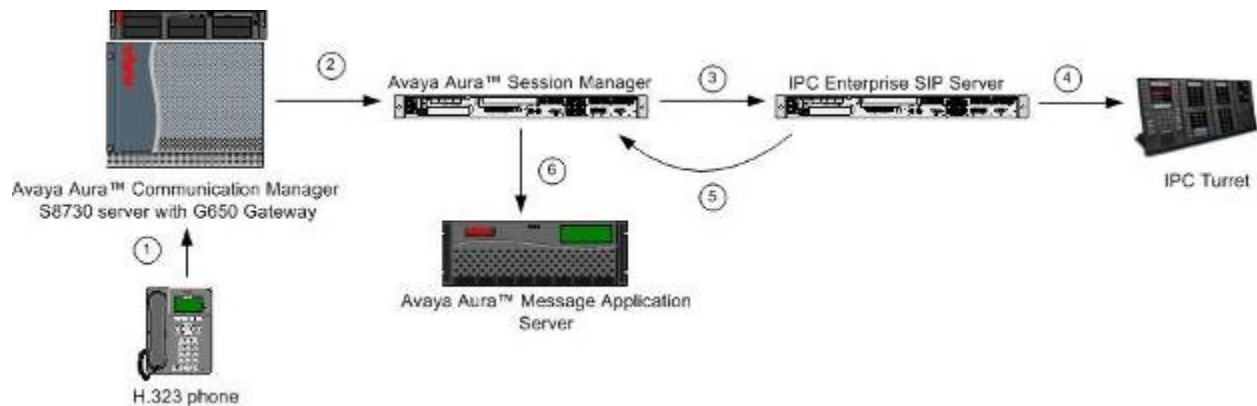
The second call scenario is an incoming call from IPC to an Avaya extension that is diverting to voicemail. An IPC user dials a number provided by Avaya which is assigned to a Communication Manager telephone that is diverted to voicemail.

1. An IPC user dials a number provided by Avaya which is assigned to a Communication Manager telephone.
2. Based on the dialed number, IPC ESS routes the call to the Session Manager.
3. Session Manager routes the call to Communication Manager using a SIP trunk.
4. The Communication Manager extension diverts the call to voicemail and uses the dial plan configuration to route the call back to Session Manager.
5. Session Manager routes the call to Modular Messaging via a SIP trunk configured on the MAS (Message Application Server).



The third call scenario is an outgoing call to IPC from an Avaya extension where the IPC extension is diverting to voicemail. The Avaya phone dials a number provided by IPC which is assigned to a turret line and this turret line is diverted to voicemail.

1. An Avaya station dials a number provided by IPC which is assigned to a turret line appearance.
2. Based on the dialed number, Communication Manager routes the call to the Session Manager via a SIP trunk.
3. Session Manager routes the call to IPC ESS.
4. IPC ESS attempt to contact the turret which is diverted to voicemail.
5. IPC ESS routes the call back to Session Manager.
6. Session Manager routes the call to Modular Messaging via a SIP trunk configured on the MAS.



3. Equipment and Software Validated

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

Equipment	Software
Avaya™ S8510 Server	Avaya Aura™ System Manager 5.2 Service Pack 1
Avaya™ S8510 Server	Avaya Aura™ Session Manager 5.2 Service Pack 1
Avaya™ S8730 Server's	Avaya Aura™ Communication Manager 5.2.1 – S8730-15-02.1.016.4. Service Pack 0
Avaya™ G650 Media Gateway - CLAN - TN799DP - MedPro - TN 2602AP	HW16 FW032 .(35) HW08 FW048. (51)
Avaya™ 3500 Server	Avaya Modular Messaging, Message Application Server 5.1. Service Pack 1 Patch 2
Avaya™ 3500 Server	Avaya Modular Messaging, Message Storage Server 5.1. Service Pack 1 Patch 2
Avaya 9630 IP Telephones	SIP: 2.5.0.0 H.323: R3.0
IPC Information Systems Alliance MX IPC System Center (Sun ULTRA 25) IPC IQ/MAX Turrets	15.03.00 Patch 2
IPC ESS (SIP Proxy Server)	2.00.01-11

4. Configure Avaya Aura™ Communication Manager as Access Element

This section describes the steps for configuring the Communication Manager as an Access Element. All configurations in the section are administered using the System Access Terminal (SAT). These Application Notes assume that the basic Communication Manager configuration has already been administered. The procedures include the following areas:

- Confirm Necessary Features
- Administer Feature Access Codes
- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set
- Administer Inbound Signaling Group
- Administer Outbound Signaling Group
- Administer Inbound Trunk Group
- Administer Outbound Trunk Group
- Administer Public Numbering
- Administer Route pattern
- Administer Dialplan Analysis
- Administer Uniform Dialplan
- Administer AAR
- Administer Modular Messaging Hunt Group
- Administer Modular Messaging Coverage Path

4.1. Confirm Necessary Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Log in to the Communication Manager SAT interface and use the **display system-parameters customer-options** command to determine these values. On **Page 2** verify that the available **Maximum Administered SIP Trunks** is equal to or greater than the desired number of simultaneous SIP trunk connections.

display system-parameters customer-options		Page	2 of 10
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		200	0
Maximum Concurrently Registered IP Stations:		1800	1
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:		0	0
Maximum Video Capable Stations:		0	0
Maximum Video Capable IP Softphones:		0	0
Maximum Administered SIP Trunks:		200	78
Maximum Administered Ad-hoc Video Conferencing Ports:		0	0

On **Page 3**, verify the fields **ARS**, **ARS/AAR Partitioning** and **ARS/AAR Dialing Without FAC** are set to **y**.

display system-parameters customer-options		Page	3 of 10
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? n		
Access Security Gateway (ASG)? n	Authorization Codes? n		
Analog Trunk Incoming Call ID? n	CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? n	CAS Main? n		
Answer Supervision by Call Classifier? n	Change COR by FAC? n		
ARS? y	Computer Telephony Adjunct Links? n		
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y	DCS (Basic)? n		
ASAI Link Core Capabilities? n	DCS Call Coverage? n		

On **Page 4**, verify the fields **ISDN-BRI Trunks**, **ISDN-PRI** and **IPTrunks** are set to **y**.

display system-parameters customer-options		Page	4 of 10
OPTIONAL FEATURES			
Emergency Access to Attendant? y	IP Stations? y		
Enable 'dadmin' Login? y	ISDN Feature Plus? y		
Enhanced Conferencing? y	ISDN/SIP Network Call Redirection? y		
Enhanced EC500? y	ISDN-BRI Trunks? y		
Enterprise Survivable Server? n	ISDN-PRI? y		
Enterprise Wide Licensing? n	Local Survivable Processor? n		
ESS Administration? n	Malicious Call Trace? y		
Extended Cvg/Fwd Admin? y	Media Encryption Over IP? y		
External Device Alarm Admin? n	Mode Code for Centralized Voice Mail? n		
Five Port Networks Max Per MCC? n	Multifrequency Signaling? y		
Flexible Billing? n	Multimedia Call Handling (Basic)? y		
Forced Entry of Account Codes? n	Multimedia Call Handling (Enhanced)? y		
Global Call Classification? n	Multimedia IP SIP Trunking? y		
Hospitality (Basic)? y			
Hospitality (G3V3 Enhancements)? n			
IP Trunks? y			

On **Page 5**, verify the fields **Private Networking** and **Uniform Dialing Plan** are set to **y**.

display system-parameters customer-options		Page	5 of 10
OPTIONAL FEATURES			
Multinational Locations? y	Station and Trunk MSP? y		
Multiple Level Precedence & Preemption? y	Station as Virtual Extension? n		
Multiple Locations? y	System Management Data Transfer? n		
Personal Station Access (PSA)? y	Tenant Partitioning? n		
PNC Duplication? n	Terminal Trans. Init. (TTI)? y		
Port Network Support? y	Time of Day Routing? n		
Posted Messages? y	TN2501 VAL Maximum Capacity? y		
Private Networking? y	Uniform Dialing Plan? y		
Processor and System MSP? n	Usage Allocation Enhancements? y		
Processor Ethernet? y	Wideband Switching? n		

Use the **display system-parameters features** command and navigate to **Page 9**. Confirm that **CPN/ANI/ICLID PARAMETERS** have a relevant text string configured.

```
display system-parameters features                                     Page 9 of 18
                                FEATURE-RELATED SYSTEM PARAMETERS

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

On **Page 18**, confirm that **Direct IP-IP Audio Connections** is set to **y**.

```
display system-parameters features                                     Page 18 of 18
                                FEATURE-RELATED SYSTEM PARAMETERS

IP PARAMETERS

                                Direct IP-IP Audio Connections? y
                                IP Audio Hairpinning? n
```

4.2. Administer Feature Access Codes

Use the **display feature-access-codes** command to verify the following. On **Page 1**, confirm that **Auto Alternate Routing (AAR) Access Code** is set to a valid feature access code according to the dial plan.

```
display 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: #3
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 1
Auto Route Selection (ARS) - Access Code 1: *7      Access Code 2:
Automatic Callback Activation: *4      Deactivation: #4
Call Forwarding Activation Busy/DA: *2      All: *3      Deactivation: #2
Call Forwarding Enhanced Status:      Act: 622      Deactivation: 623
Call Park Access Code: #5
Call Pickup Access Code: *6
CAS Remote Hold/Answer Hold-Unhold Access Code: #6
```

4.3. Administer IP Node Names

Use the **change node-names ip** command to add The IP address of the Session Manager interface, also make note of the CLAN name as this will be used to configure the SIP signaling groups.

```
change node-names ip
IP NODE NAMES
Name      IP Address
CLAN1     10.10.16.23
Gateway   10.10.16.1
MedProl   10.10.16.24
SM100    10.10.16.11
default   0.0.0.0
procr     10.10.16.20
```

4.4. Administer IP Network Region

Use the **change ip-network-region n** command, where **n** is the network region number to configure the network region being used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise, a descriptive **Name** for this ip-network-region and set the **Codec Set** to the number of the codec set that will be used. **Intra-region IP-IP Direct Audio** and **Intra-region IP-IP Direct Audio** should be set to **yes** to enable IP shuffling. Although not highlighted, note also that the **IP Network Region** form is used to set the QoS packet parameters that provide priority treatment for signaling and audio packets over other data traffic. These parameters may need to be aligned with the specific values expected by the IP network.

```
change ip-network-region 1
IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: avaya.com
Name: Default Region
MEDIA PARAMETERS
Codec Set: 1      Intra-region IP-IP Direct Audio: yes
                  Inter-region IP-IP Direct Audio: yes
                  IP Audio Hairpinning? n
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
RTCP Reporting Enabled? y
RTCP MONITOR SERVER PARAMETERS
Use Default Server Parameters? y
AUDIO RESOURCE RESERVATION PARAMETERS
RSVP Enabled? n
Page 1 of 19
```

4.5. Administer IP Codec Sets

Use the **change ip-codec-set n** command, where **n** is the codec set specified in the **IP Network Region** form. Enter the codecs eligible to be used; the codecs defined here must be supported by the far end device.

change ip-codec-set 1

Page 1 of 2

IP Codec Set

Codec Set: 1

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

4.6. Administer Inbound Signaling Group

Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system.

- Set the **Group Type** field to be **sip**
- The **Near-end Node Name** is set to the name of the CLAN (**CLAN1**) that will be used to process the signaling. The clan name is assigned in the IP Node-names form
- The **Far-end Node Name** is set to the name of the Session Manager (**SM100**) that was entered into the IP Node-names form
- The **Far-end Network Region** to the region configured in **Section 4.4**
- The **Far-end Domain** is left blank so that the signaling group accepts any domain

add signaling-group 1		SIGNALING GROUP	
Group Number: 1	Group Type: sip		
	Transport Method: tcp		
IMS Enabled? n			
IP Video? n			
Near-end Node Name: CLAN1		Far-end Node Name: SM100	
Near-end Listen Port: 5060		Far-end Listen Port: 5060	
Far-end Domain:		Far-end Network Region: 1	
		Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate		RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3		IP Audio Hairpinning? n	
Enable Layer 3 Test? y		Direct IP-IP Early Media? n	
H.323 Station Outgoing Direct Media? n		Alternate Route Timer(sec): 6	

4.7. Administer Outbound Signaling Group

Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system.

- Set the **Group Type** field to be **sip**
- The **Near-end Node Name** is set to the name of the CLAN (**CLAN1**) that will be used to process the signaling. The clan name is assigned in the IP Node-names form
- The **Far-end Node Name** is set to the name of the Session Manager (**SM100**) that was entered into the IP Node-names form
- The **Far-end Network Region** to the region configured in **Section 4.4**
- The **Far-end Domain** is set to the name of the domain name that is used by Session Manager and Modular Messaging

add signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
IP Video? n		
Near-end Node Name: CLAN1	Far-end Node Name: SM100	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	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? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

4.8. Administer Inbound SIP Trunk Group

To create a SIP trunk group use the command, **add trunk-group n** where **n** is the number of the trunk group to create.

- Set the **Group Type** field to be **sip**
- Add a descriptive name into the **Group Name** field
- Set the **TAC** field to a valid dial access code (dac) according to the dial plan configuration
- Set the **Service Type** field to **tie**
- Set the **Signaling Group** field to the signaling group set up in **Section 4.6**
- Set the **Number of Members** field to the number of channels required on the trunk group

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: ASM<>CM	COR: 1	TN: 1	TAC: 501
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 1			
Number of Members: 30			

On **Page 2** of the trunk-group form, the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with IPC to prevent unnecessary sip messages during call setup.

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n		Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 600			

On **Page 3** of the trunk-group form, set the **Numbering Format** field to **public** and ensure the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields are set to **y**.

add trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		
UI Treatment: service-provider		
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		
Show ANSWERED BY on Display? y		

On **Page 4** of the trunk-group form, set the **Support Request History** field to **y**.

add trunk-group 1		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type:		

4.9. Administer Outbound SIP Trunk Group

To create a SIP trunk group, use the command, **add trunk-group n** where **n** is the number of the trunk group to create.

- Set the **Group Type** field to be **sip**
- Add a descriptive name into the **Group Name** field
- Set the **TAC** field to a valid dial access code (dac) according to the dial plan configuration
- Set the **Service Type** field to **tie**
- Set the **Signaling Group** field to the signaling group set up in **Section 4.7**
- Set the **Number of Members** field to the number of channels required on the trunk group

add trunk-group 2		Page 1 of 21
TRUNK GROUP		
Group Number: 2	Group Type: sip	CDR Reports: y
Group Name: SIP Outbound	COR: 1	TN: 1 TAC: 502
Direction: two-way	Outgoing Display? n	Night Service:
Dial Access? n		
Queue Length: 0		
Service Type: tie	Auth Code? n	
Signaling Group: 2		
Number of Members: 48		

On **Page 2** of the trunk-group form, the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with IPC so the initial SIP INVITE message from Avaya to IPC will contain a value the IPC network finds acceptable, removing the need for extra SIP messaging to establish mutually-acceptable session expiration and refresh timing for each call.

add trunk-group 2		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
Redirect On OPTIM Failure: 5000		
SCCAN? n	Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 600		

On **Page 3** of the trunk-group form, set the **Numbering Format** field to **public**.

add trunk-group 2		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		
UI Treatment: service-provider		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		
Show ANSWERED BY on Display? y		

On **Page 4** of the trunk-group form, ensure the **Support Request History** field is set to **y** as MM relies on the History Info headers to select an appropriate mail box.

add trunk-group 2		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type:		

4.10. Administer Public Numbering

To ensure that the caller number is correctly presented to IPC the trunk group references the public numbering table, use the command, **change public-unknown-numbering n** where **n** is the number of the private numbering table to be edited. The following values should be set:

- Set **Ext Len** field to **4** this is the length of the extensions that will be using the table.
- Set **Ext Code** to match the leading digits of extension ranges to be used.
- Set **Total Len** to **4** this is the total length of the calling number that will be presented by the trunk group.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp (s)	CPN Prefix	Total CPN Len	
4	66			4	Total Administered: 1 Maximum Entries: 9999

4.11. Administer Route Pattern

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration trunk group 2 is added under the **Grp No** field.

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

4.12. Administer Dialplan Analysis

Use the **change dialplan analysis** command to administer the dialplan. In this configuration, extensions in the range 33xx are assigned to IPC SIP turrets and are configured as **udp** to send calls via the UDP (uniform dial plan). Extensions ranges **66xx** and **88xx** are Communication Manager extensions and are configured as **ext**.

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 1			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	1	ext	663	4	udp				
1	1	fac	7	4	ext				
2	4	udp	88	4	ext				
30	9	udp	89	4	ext				
3005	8	udp	972	5	udp				
31	4	udp	99	4	ext				
33	4	udp	*	2	fac				
37	4	udp	#	2	fac				
38	5	aar							
4	4	aar							
4	5	ext							
5	3	dac							
6	3	fac							
61	4	ext							
66	4	ext							

4.13. Administer Uniform Dialplan

Use the **change uniform-dialplan** command to administer the UDP routing. It is possible to use the UDP to manipulate the dialed digits but in this configuration UDP is used to direct the matching calls to AAR (alternate access routing).

change uniform-dialplan							
UNIFORM DIAL PLAN TABLE							
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node	Num
31	4	0		aar	n		
33	4	0		aar	n		
37	4	0		aar	n		
663	4	0		aar	n		
8889	4	0		aar	n		
972	5	0		aar	n		

4.14. Administer AAR

Use the **change aar analysis n** command to specify which route pattern to use based upon the number dialed **n**. In this example, **Route Pattern 2** is used for IPC extensions beginning **33** and for the Modular Messaging pilot number **8889**.

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all					Percent Full:		1	
	Dialed String	Total		Route	Call	Node	ANI	
		Min	Max	Pattern	Type	Num	Reqd	
	31	4	4	3	aar		n	
	33	4	4	2	aar		n	
	37	4	4	7	aar		n	
	663	4	4	2	aar		n	
	8889	4	4	2	aar		n	
	972	5	5	4	aar		n	

4.15. Administer Modular Messaging Hunt Group

Use the **add hunt-group n** command, where **n** is the number of the hunt-group to add. Give the hunt group a descriptive **Group Name** and a valid **Group Extension** according to the dial plan. Set **ISDN/SIP Caller Display** to **grp-name**.

change hunt-group 2		Page 1 of 60	
HUNT GROUP			
Group Number: 2		ACD? n	
Group Name: Modular Messaging		Queue? n	
Group Extension: 8999		Vector? n	
Group Type: ucd-mia		Coverage Path:	
TN: 1		Night Service Destination:	
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display: grp-name			

On **Page 2** of the hunt group form, set the **Message Center** to be **sip-adjunct**, enter a **Voice Mail Number** and **Voice Mail Handle**, in this configuration both are set to **8889**. Enter the AAR access code as defined in the feature access codes form (**Section 4.2**) for **Routing Digits**

change hunt-group 2

Page 2 of 60

HUNT GROUP

Message Center: sip-adjunct

Voice Mail Number	Voice Mail Handle	Routing Digits
		(e.g., AAR/ARS Access Code)
8889	8889	1

4.16. Administer Modular Messaging Coverage Path

Use the **change coverage path n** command, where n is the number of the coverage path to administer. Set **Point 1** to **h2** to send covered calls using this coverage path to hunt group 2.

change coverage path 2	Page 1 of 1		
COVERAGE PATH			
Coverage Path Number: 2			
Cvg Enabled for VDN Route-To Party? n	Hunt after Coverage? n		
Next Path Number:	Linkage		
COVERAGE CRITERIA			
Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 2
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: h2	Rng:	Point2:	
Point3:		Point4:	

Use the **change station n** command to add the coverage path to a station where n is the extension number of the station to administer. Enter the coverage path number in the **Coverage Path 1** field.

change station 6621	Page 1 of 5	
STATION		
Extension: 6621	Lock Messages? n	BCC: 0
Type: 9630	Security Code: ****	TN: 1
Port: S00002	Coverage Path 1: 2	COR: 1
Name: IP2nd	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
Speakerphone: 2-way	Personalized Ringing Pattern: 1	
Display Language: english	Message Lamp Ext: 6621	
Survivable GK Node Name:	Mute Button Enabled? y	
Survivable COR: internal	Button Modules: 0	
Survivable Trunk Dest? y	Media Complex Ext:	
	IP SoftPhone? n	
	IP Video? n	
	Customizable Labels? y	

5. Configure Avaya Aura™ Communication Manager as Feature Server

This section describes the steps for configuring the Communication Manager as a Feature Server. All Configurations in the section are administered using the System Access Terminal (SAT). These Application notes assume that the basic Communication Manager configuration has already been administered. The procedures covered include the following areas:

- Administer IP Node Names
- Administer IP Network Region
- Administer IP Codec Set
- Administer Signaling Group on Feature Server
- Administer Trunk Group on Feature Server

5.1. Administer IP Node Names

Use the **change node-names ip** command to add the IP address of the Session Manager (**sm100**) interface, also make note of the procr name as this will be used to configure the SIP signaling groups.

```
change node-names ip
```

Name	IP Address
DefGW	10.10.16.1
procr	10.10.16.42
default	0.0.0.0
medpro	10.10.16.43
sm100	10.10.16.11

5.2. Administer IP Network Region

Use the **change ip-network-region n** command where **n** is the network region number to configure the network region being used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise, a descriptive **Name** for this ip-network-region and set the **Codec Set** to the number of the codec set that will be used. **Intra-region IP-IP Direct Audio** and **Intra-region IP-IP Direct Audio** should be set to **yes** to enable IP shuffling. Although not highlighted, note also that the **IP Network Region** form is used to set the QoS packet parameters that provide priority treatment for signaling and audio packets over other data traffic. These parameters may need to be aligned with the specific values expected by the IP network.

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: 1 Authoritative Domain: avaya.com		
Name: SIP IPNR		
MEDIA PARAMETERS		
Codec Set: 1		Intra-region IP-IP Direct Audio: yes
UDP Port Min: 2048		Inter-region IP-IP Direct Audio: yes
UDP Port Max: 3329		IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46		Use Default Server Parameters? y
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
AUDIO RESOURCE RESERVATION PARAMETERS		
H.323 IP ENDPOINTS		RSVP Enabled? n
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		

5.3. Administer IP codec sets

Use the **change ip-codec-set n** command, where **n** is the codec set specified in the IP Network Region form. Enter the codecs eligible to be used. The codecs defined here must be supported by the far end device.

change ip-codec-set 1		Page 1 of 2	
IP Codec Set			
Codec Set: 1			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)
1: G.711MU	n	2	20
2: G.711A	n	2	20
3: G.729	n	2	20
4:			
5:			

5.4. Administer Signaling Group

Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system.

- Set the **Group Type** field to be **sip**
- The **Near-end Node Name** is set to the name of the procr that will be used to process the signaling. The procr name is assigned in the IP Node-names form
- The **Far-end Node Name** is set to the Session Manager name (**sm100**) configured in the Node-Names IP form
- Set the **Far-end Network Region** to the region configured in **Section 5.2**
- Set the **IMS Enabled** field to **y**

add signaling-group 200		Page 1 of 1
SIGNALING GROUP		
Group Number: 200	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? y		
Near-end Node Name: procr	Far-end Node Name: sm100	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	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? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

5.5. Administer SIP Trunk Group

Use the **add trunk-group n** command, where **n** is the number of the trunk group to create.

- Set the **Group Type** field to be **sip**
- Add a descriptive name into the **Group Name** field
- Set the **TAC** field to a valid dial access code (dac) according to the dial plan configuration
- Set the **Service Type** field to **tie**
- Set the **Signaling Group** field to the signaling group set up in **Section 5.4**
- Set the **Number of Members** field to the number of channels required.

add trunk-group 200		Page 1 of 21
TRUNK GROUP		
Group Number: 200	Group Type: sip	CDR Reports: y
Group Name: toASM	COR: 1	TN: 1
Direction: two-way	Outgoing Display? n	TAC: *20
Dial Access? n		Night Service:
Queue Length: 0		
Service Type: tie	Auth Code? n	
		Signaling Group: 200
		Number of Members: 30

On **Page 2** of the trunk-group form, the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with IPC to prevent unnecessary sip messages during call setup.

add trunk-group 200	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
	Redirect On OPTIM Failure: 5000
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 600	

On **Page 3** of the trunk-group form set the **Numbering Format** field to **private** and ensure the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields are set to **y**

add trunk-group 200	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y

On **Page 4** of the trunk-group form set the **Support Request History** field to **y**.

add trunk-group 200	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type:	

6. Configuring Avaya Aura™ System Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured via the System Manager. The procedures include the following areas:


- Log in to Avaya Aura™ Session Manager
- Administer SIP domain
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Time Ranges
- Administer Routing Policies
- Administer Dial Patterns
- Administer Session Manager

6.1. Log in to Avaya Aura™ System Manager

Access the System Manager using a Web Browser and entering **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in using appropriate credentials and accept the subsequent Copyright Legal Notice.

6.2. Administer SIP domain

Add the SIP domains that will be used with Session Manager. Select **SIP Domains** on the left panel menu and click the **New** button (not shown) to create a new SIP domain entry. In the **Name** field, enter the domain name (e.g., **avaya.com** or **ipc.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes.

 Avaya Aura™ System Manager 5.2 Welcome, ad

Home / Network Routing Policy / SIP Domains

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Domain Management

Edit New Duplicate Delete More Actions ▼

2 Items | Refresh

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

Select : All, None (0 of 2 Selected)

6.3. Administer Locations

As the Avaya and IPC enterprises are on different subnets, a location is set up for each one. To add a location, select **Locations** on the left panel menu and then click on the **New** button (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page, under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, '*' is used to specify any number of allowed characters at the end of the string. The following screen shows the location for the Avaya enterprise.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 08, 2010 12:16 PM [Help](#) | [Log off](#)

Home / Network Routing Policy / Locations / Location Details

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

General

* **Name:**

Notes:

Managed Bandwidth:

* **Average Bandwidth per Call:** **kbit/sec** ▼

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

Location Pattern

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

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

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.16.*	<input type="text"/>

Select : All, None (0 of 1 Selected)

The following screen shows the location for the IPC enterprise.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 08, 2010 12:16 PM

Help | Log off

Home / Network Routing Policy / Locations / Location Details

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

Location Details

Commit Cancel

General

* Name: IPCLab

Notes:

Managed Bandwidth:

* Average Bandwidth per Call: 80 Kbit/sec

* Time to Live (secs): 3600

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

	IP Address Pattern	Notes
<input type="checkbox"/>	*192.168.0.*	

Select : All, None (0 of 1 Selected)

6.4. Administer Adaptations

Session Manager is installed with a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as host names in the Request-URI (Uniform Resource Identifier). In this configuration the adaptation is used with the IPC SIP entities defined in System Manager (covered in **Section 6.5.4**) and ensures egress messages have the hostname **ipc.com** used by IPC, and ingress messages have the hostname **avaya.com** used by Avaya. To add an adaptation, select **Adaptations** on the left panel menu and then click on the **New** button (not shown). Under **General**:

- In the **Adaptation Name** field enter an informative name
- In the **Module Name** field select **<click to add module>** from the drop down list and enter “DigitConversionAdapter” in the resulting **New Module Name** field
- In the **Module Parameter** field enter the modification parameters to be used. In this configuration the modification parameters used are: “odstd=ipc.com iodstd=avaya.com”. Appendix A provides an overview of the module parameters available for the DigitConversionAdapter module



Asset Management	Adaptation Details General * Adaptation name: <input type="text" value="IPCHostName"/> Module name: <input type="text" value="DigitConversionAdapter"/> Module parameter: <input type="text" value="odstd=ipc.com iodstd=avaya.com"/> Egress URI Parameters: <input type="text"/> Notes: <input type="text"/>
Communication System Management	
User Management	
Monitoring	
Network Routing Policy	
Adaptations	
Dial Patterns	
Entity Links	
Locations	
Regular Expressions	


6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter an IP address of the SM or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity, **Modular Messaging** for a Modular Messaging SIP entity or **Other** for an IPC SIP entity
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for this location

In this configuration there are six SIP Entities.

 Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jan

Home / Network Routing Policy / SIP Entities

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

SIP Entities

Edit New Duplicate Delete More Actions ▼ Commit

6 Items | Refresh

<input type="checkbox"/>	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	AccessElement	▶	10.10.16.23	CM	
<input type="checkbox"/>	Feature Server	▶	10.10.16.42	CM	
<input type="checkbox"/>	IPCESS1	▶	192.168.0.103	Other	
<input type="checkbox"/>	IPCESS2	▶	192.168.0.105	Other	
<input type="checkbox"/>	ModMessaging	▶	10.10.16.26	Modular Messaging	
<input type="checkbox"/>	SessionManager	▶	10.10.16.11	Session Manager	

Select : All, None (0 of 6 Selected)

6.5.1. Avaya Aura™ Session Manager SIP Entity

The following screens show the SIP entity for Session Manager.

AVAYAAvaya Aura™ System Manager 5.2Welcome, **admin** L

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

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

SIP Entity Details

General

* Name:

SessionManager

* FQDN or IP Address:

10.10.16.11

Type:

Session Manager

Notes:

Location:

AvayaLab

Outbound Proxy:

Time Zone:

Europe/Dublin

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

Use Session Manager Configuration

The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row:

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field select from the drop down menu the Avaya domain as the default domain.

Port

AddRemove

3 Items RefreshFilter: Enable

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

Select : All, None (0 of 3 Selected)

6.5.2. Avaya Aura™ Communication Manager SIP Entities

In this configuration two Communication Manager SIP entities are required. The first SIP entity is for an Access Element, the second SIP entity is for a Feature Server, the Feature Server is only required to service SIP handsets. The following screen shows the SIP Entity for the Access Element.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin |

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

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▶ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

SIP Entity Details

General

* Name: AccessElement ▶

* FQDN or IP Address: 10.10.16.23

Type: CM ▼

Notes:

Adaptation: ▼

Location: AvayaLab ▶

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 ▼

The following screen shows the SIP Entity for the Feature Server Communication Manager.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin |

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

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▶ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

SIP Entity Details

General

* Name: Feature Server ▶

* FQDN or IP Address: 10.10.16.42

Type: CM ▼

Notes:

Adaptation: ▼

Location: AvayaLab ▶

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 ▼

6.5.3. Avaya Modular Messaging SIP Entity

The following screen shows the SIP Entity for Modular Messaging.



SIP Entity Details	General
* Name:	ModMessaging
* FQDN or IP Address:	10.10.16.26
Type:	Modular Messaging
Notes:	
Adaptation:	
Location:	AvayaLab
Time Zone:	Europe/Dublin
Override Port & Transport with DNS SRV:	<input type="checkbox"/>
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none
SIP Link Monitoring	Use Session Manager Configuration

6.5.4. IPC SIP Entities

In this configuration IPC have two Enterprise SIP Server's (ESS) for the purpose of redundancy. Each IPC ESS is added as a separate SIP Entity. The following screen shows the SIP Entity IPC ESS1. Note that in addition to the fields already discussed the SIP Entities for IPC ESS also have an entry in the **Adaptation** field.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura™ System Manager 5.2", and a user greeting "Welcome, admin La". Below this is a red breadcrumb trail: "Home / Network Routing Policy / SIP Entities / SIP Entity Details". On the left is a sidebar menu with categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (expanded), Security, Applications, Settings, and Session Manager. Under "Network Routing Policy", sub-items include Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities (highlighted), Time Ranges, and Personal Settings. The main content area is titled "SIP Entity Details" and "General". It contains the following fields: "Name" (IPCESS1), "FQDN or IP Address" (192.168.0.103), "Type" (Other), "Notes" (empty), "Adaptation" (IPHostName, highlighted with a red box), "Location" (IPCLab), "Time Zone" (Europe/Dublin), "Override Port & Transport with DNS SRV" (checkbox), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), "Call Detail Recording" (none), and "SIP Link Monitoring" (Use Session Manager Configuration).

The following screen shows the SIP Entity for IPC ESS2. Note that the same **Adaptation** entry that was used for the first ESS is used in the **Adaptation** field for the second ESS.

This screenshot shows the same Avaya Aura System Manager 5.2 interface as the previous one, but for the SIP Entity "IPCESS2". The breadcrumb trail is "Home / Network Routing Policy / SIP Entities / SIP Entity Details". The sidebar menu is identical, with "SIP Entities" highlighted. The "SIP Entity Details" and "General" section contains the following fields: "Name" (IPCESS2), "FQDN or IP Address" (192.168.0.105), "Type" (Other), "Notes" (empty), "Adaptation" (IPHostName, highlighted with a red box), "Location" (IPCLab), "Time Zone" (Europe/Dublin), "Override Port & Transport with DNS SRV" (checkbox), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), "Call Detail Recording" (none), and "SIP Link Monitoring" (Use Session Manager Configuration).

6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described as an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed (not shown).

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **SessionManager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 4.5**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- In the **Trusted**, tick whether to trust the other system
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in this configuration. Note that there are two entries for each IPC ESS, although the same port is configured they use different protocols, one link is configured for TCP and the other for UDP as both were tested in this configuration. An individual entity link must be set up for each combination of port and protocol.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 09, 2010 11:52 AM [Help](#) | [Log off](#)

Home / Network Routing Policy / **Entity Links**

Entity Links

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) [Commit](#)

7 Items [Refresh](#) Filter: [Enable](#)

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	LinkToAECM	SessionManager	TCP	5060	AccessElement	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	LinkToESS1	SessionManager	TCP	5060	IPCESS1	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	LinkToESS2	SessionManager	TCP	5060	IPCESS2	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	LinkToFSCM	SessionManager	TCP	5060	Feature Server	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	LinkToMM_TCP	SessionManager	TCP	5060	ModMessaging	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	UDP_LinkToESS1	SessionManager	UDP	5060	IPCESS1	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	UDP_LinkToESS2	SessionManager	UDP	5060	IPCESS2	5060	<input checked="" type="checkbox"/>	

Select : All, None (0 of 7 Selected)

6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown). Enter the following:

- Under **General** enter an informative name in the **Name** field
- 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 then select the time range
- Select **Commit** when completed

As an example the following screen shows the routing policy for IPC ESS1

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar contains a menu with categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (selected), Security, Applications, Settings, and Session Manager. Under Network Routing Policy, the sub-items are Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies (selected), SIP Domains, SIP Entities, Time Ranges, and Personal Settings. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button. It has three sections: 'General' with fields for Name (CallsToESS1), Disabled (unchecked), and Notes; 'SIP Entity as Destination' with a 'Select' button and a table showing the selected entity IPCESS1 with FQDN 192.168.0.103 and Type Other; and 'Time of Day' with 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below this is a table with 1 item, showing a time range of 24/7 from 00:00 to 23:59. The bottom of the screen shows 'Shortcuts'.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 09, 2010 11:52 AM

Help | Log off

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

Routing Policy Details [Commit] [Cancel]

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
IPCESS1	192.168.0.103	Other	

Time of Day

1 Item Refresh Filter: Enable

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

Select : All, None (0 of 1 Selected)

The following screen shows all the **Routing Policies** added for this configuration.

The screenshot shows the Avaya Aura System Manager 5.2 interface with the 'Routing Policies' page selected. The left sidebar is the same as the previous screenshot. The main content area is titled 'Routing Policies' and includes buttons for Edit, New, Duplicate, Delete, More Actions, and Commit. Below this is a table with 5 items, showing the list of routing policies: CallsToAECM, CallsToESS1, CallsToESS2, and CallsToMM. The table has columns for Name, Disabled, Destination, and Notes. The bottom of the screen shows 'Select : All, None (0 of 5 Selected)'.

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 09, 2010 11:52 AM

Help | Log off

Home / Network Routing Policy / Routing Policies

Routing Policies [Edit] [New] [Duplicate] [Delete] [More Actions] [Commit]

5 Items Refresh Filter: Enable

Name	Disabled	Destination	Notes
CallsToAECM	<input type="checkbox"/>	AccessElement	
CallsToESS1	<input type="checkbox"/>	IPCESS1	
CallsToESS2	<input type="checkbox"/>	IPCESS2	
CallsToMM	<input type="checkbox"/>	ModMessaging	

Select : All, None (0 of 5 Selected)

6.8. Administer Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. A dial pattern is not needed for SIP extensions as they are registered with the Session Manager and are routed via an application sequence. To configure a dial pattern, select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select **ALL**

Navigate to **Originating Locations and Routing Policies** and select **Add**, in the resulting screen (not shown) Under **Originating Location** select **ALL** and under **Routing Policies** select **AvayaCM**. Click **Select** button to save. The following screen shows an example dial pattern configured for the access element.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Feb. 09, 2010 11:52 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](#) Filter: [Enable](#)

1 Item [Refresh](#)

<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	CallsToAECM	0	<input type="checkbox"/>	AccessElement	

Select : All, None (0 of 1 Selected)

The following screen shows the dial pattern configured for the Modular Messaging pilot number.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 09, 2010 11:52 AM

Help | Log off

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

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

Dial Pattern Details

Commit Cancel

General

* Pattern: 888

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: -ALL-

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	CallsToMM	0	<input type="checkbox"/>	ModMessaging	

Select : All, None (0 of 1 Selected)

The following screen shows an example dial pattern configured for IPC. For IPC two routing policies are associated with the dial pattern, the first routing policy routes to ESS1 and the second to ESS2. As the routing policies are of equal priority, SIP messaging will be shared between the routing policies; if one ESS is unavailable then the routing policy for the alternate ESS will be used.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 09, 2010 11:52 AM

Help | Log off

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

▶ Asset Management

▶ Communication System Management

▶ User Management

▶ Monitoring

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

Dial Pattern Details

Commit Cancel

General

* Pattern: 330

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items 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	CallsToESS1	0	<input type="checkbox"/>	IPCESS1	
<input type="checkbox"/>	-ALL-	Any Locations	CallsToESS2	0	<input type="checkbox"/>	IPCESS2	

Select : All, None (0 of 2 Selected)

6.9. Administer Feature Server as an Application on Avaya Aura™ System Manger

In order for Communication Manager to provide configuration and Feature Server support to SIP phones when they register to Session Manager, the feature server must be added as an application. From the left panel menu, select **Applications → Entities** and click **New**. Select **CM** for the type of application from the drop down menu (not shown) in the resulting screen under the **Application** heading, enter values in the following fields and use defaults for the remaining fields:

- In the **Name** field enter a descriptive name
- In the **Node** field select **Other** from the drop-down menu
- In the resulting **Other Node** field enter the IP address of the Communication Manager (the IP address that is used for the SAT login)

Under the **Attributes** heading enter values in the following fields and use defaults for the remaining fields:

- In the **Login** field enter a login name for Communication Manager (SAT SSH login)
- In the **Password** field enter Password for Communication Manager (SAT SSH password)

Select **Commit**, this causes System Manager to synchronize with the Communication Manager in the background.



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

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Other Applications

Session Manager 5.2

SMGR

SIP AS 8.0

Entities

Settings

Session Manager

Shortcuts

Change Password

Application Instance Fields

New CM Instance

CommitCar

Application | Port | Access Point | Attributes |
Expand All | Collapse All

Application

* NameFSCMApp

* TypeCMReset

Description

* NodeOther..

* Other Node10.10.16.17

Port

Access Point

Attributes

* Logindadmin

Password*****

Confirm Password*****

Is SSH Connection☒

* Port5022

6.10. Create a Feature Server Application

From the left panel menu, select **Session Manager** → **Application Configuration** → **Applications** and click on **New**. Enter the following fields and use defaults for the remaining fields:

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Feature Server Communication Manager.

Select **Commit**

The screenshot shows the Avaya Aura™ System Manager 5.2 interface. The left sidebar contains a menu with options: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, Security, Applications, Settings, and Session Manager. The main area is titled "Application Editor" and contains a "Commit" button. Below the title, there is a section "Application Editor" with the following fields: "Name" (FSCMApp), "SIP Entity" (Feature Server), and "Description".

6.11. Administer Feature Server Application sequence

From the left panel menu, select **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New**.

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes select **Commit**

The screenshot shows the Avaya Aura™ System Manager 5.2 interface. The left sidebar contains a menu with options: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, Security, Applications, Settings, and Session Manager. The main area is titled "Application Sequence Editor" and contains a "Commit" button. Below the title, there is a section "Sequence Name" with the following fields: "Name" (FSCMSeq) and "Description". Below this, there is a section "Applications in this Sequence" with buttons "Move First", "Move Last", and "Remove". Below this, there is a table with 1 item:

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
1	FSCMApp	Feature Server	<input checked="" type="checkbox"/>	

Below the table, there is a text "Select : All, None (0 of 1 Selected)". Below this, there is a section "Available Applications" with a table:

Name	SIP Entity	Description
FSCMApp	Feature Server	

6.12. Administer SIP Extensions

SIP extensions are registered with the session manager and use the Feature Server for their feature and configuration settings. To add a SIP user, select **User Management** → **User Management** and select **New**.

Under the **General** section,

- Enter the user's name in the **Last Name** and **First Name** fields.



Avaya Aura™ System Manager 5.2

Home / User Management / User Management / New User

- ▶ Asset Management
- ▶ Communication System Management
- ▼ User Management
 - Manage Roles
 - User Management
 - ▶ Global User Settings
 - Group Management
- ▶ Monitoring
- ▶ Network Routing Policy
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

Shortcuts

[Change Password](#)
[Help for Create User](#)
[Help for New Private Contact](#)

New User Profile

[General](#) | [Identity](#) | [Communication Profile](#) | [Roles](#) | [Override Permissions](#) | [Group Memberships](#)
[Expand All](#) | [Collapse All](#)

General

* Last Name:

* First Name:

Middle Name:

Description:

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

User Type: ☐ supervisor
☐ resident_expert
☐ service_technician
☐ lobby_phone

Under the **Identity** section,

- In the **Login Name** field enter a unique system login name in the form of user@domain (e.g. “6630@avaya.com”) where the extension is used to log into the SIP phone.
- The **Authentication Type** should be **Basic**
- In the **SMGR Login Password** field enter an alphanumeric password and confirm it
- In the **Shared Communication Profile Password** enter a numeric password; this is the password that is used when logging in to the phone
- In the **Localized Display Name** field enter the name to be displayed as the calling party
- Re-enter the name of the user for **Endpoint Display Name**

Identity ▼

* **Login Name:**

* **Authentication Type:** ▼

SMGR Login Password:

* **Password:**

* **Confirm Password:**

Shared Communication Profile Password:

Confirm Password:

Localized Display Name:

Endpoint Display Name:

Honorific:


Language Preference: ▼

Time Zone: ▼

Click on the show/hide button for **Communication Profile** then Click on the show/hide button for **Communication Address**.

- Select **New** and in the **SubType** field, select username from the drop-down menu
- Click the **New** button and in the resulting fields (not shown)
- Select **sip** from the drop-down menu for **Type** if it is not set already
- In the **SubType** field, select **username** from the drop-down menu
- In the **Fully Qualified Address** field, enter an extension number

Click the **Add** button to commit.


Communication Profile 

Name
Primary

Select : None

* Name:

Default : ☒


Communication Address 

<input type="checkbox"/>	Type	SubType	Handle	Domain
<input type="checkbox"/>	sip	username	6630	avaya.com

Select : All, None (0 of 1 Selected)

Click the show/hide button next to **Session Manager**

- Make sure the **Session Manager** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Session Manager Instance** field
- Select the appropriate application name from the drop-down menu in the **Origination Application Sequence** field
- Select the appropriate application name from the drop-down menu in the **Termination Application Sequence** field

☒ **Session Manager** 

* **Session Manager Instance**

Origination Application Sequence

Termination Application Sequence

Click the show/hide button next to **Station Profile** and Make sure the **Station Profile** check box is checked.

- Select the Communication Manager application from the **System** drop-down menu
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- For the **Port** field select **IP**
- Select the **Delete Station on Unassign of Station from User** box
- Select **Commit** (not shown) to save changes and the System Manager will add the Communication Manager Feature Server configuration automatically

☒ **Station Profile** ▼

* **System**

Use Existing Stations ☐

* **Extension**

* **Template**

Set Type

Security Code

* **Port**

Delete Station on Unassign of Station from User ☒

7. Configure Avaya Modular Messaging

This section provides the procedures for configuring Modular Messaging. The procedures include the following areas:

- Configure Avaya Message Application Server
- Configure Avaya Message Storage Server

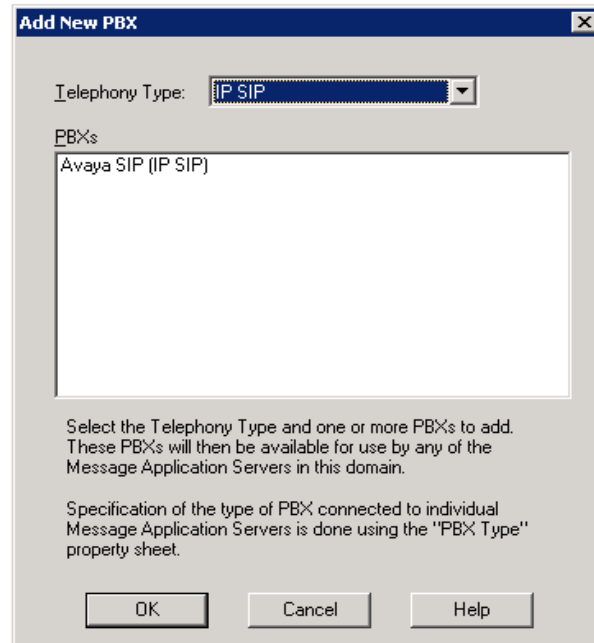
7.1. Configure Avaya Message Application Server

7.1.1. Add New PBX

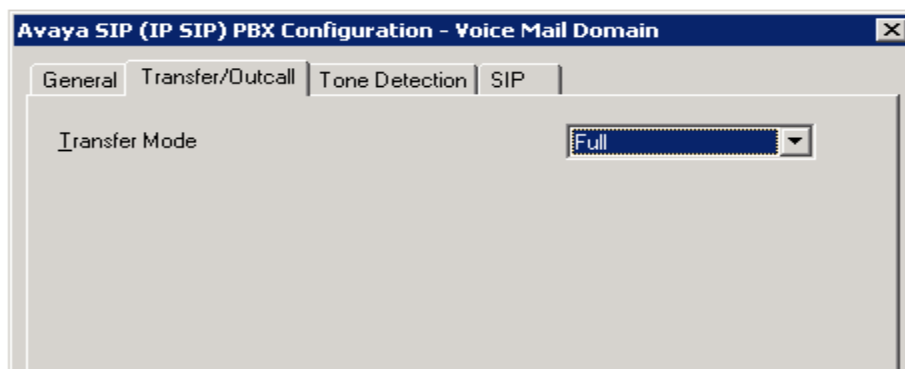
Select **Start → Programs → Avaya Modular Messaging → Voice Mail System Configuration – AVAYAMAS1**. Expand **Voice Mail Domains** and the administered domain name (**DCVMD** in the screenshot below). Right-click on **PBXs** and select **Add New PBX Type...**



On the **Add New PBX** screen, select **IP SIP** from the **Telephony Type** drop down box, then select **Avaya CM (IP SIP)** from the **PBXs** box. Select **OK** when completed.



On the **Voice Mail System Configuration – AVAYAMAS1** screen double-click on **PBXs**. On the **Avaya CM (IP SIP) PBX Configuration** screen, select the **Transfer/Outcall** tab, in the **Transfer Mode** field select **Full** from the drop down menu.



Select the **SIP** tab and enter the following fields.

- In the **Address/FQDN** field enter the IP address of the session manager interface
- In the **Protocol** field select the protocol Modular messaging will use for communication to the Session Manager
- Select the **MWI** check box
- In the **SIP Domain** field enter the sip domain that is being used by Session Manager and that Modular Messaging will become part of.
- Click **OK** when completed

The screenshot shows the 'asm PBX Configuration - Voice Mail Domain' dialog box with the 'SIP' tab selected. The 'Gateways' section contains a table with one entry: 10.10.16.11, TCP, MWI checked, and SRTP set to None. Below the table are fields for 'SIP Domain' (avaya.com), 'P-Asserted-Identity', and 'PBX Address'. A 'Phone Number Translation Rules' section includes a 'Configure...' button and a note that translation rules are effective only after MultiSite has been enabled. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Address/FQDN	Protocol	MWI	SRTP
10.10.16.11	TCP	<input checked="" type="checkbox"/>	None

SIP Domain: avaya.com

P-Asserted-Identity:

PBX Address:

Phone Number Translation Rules

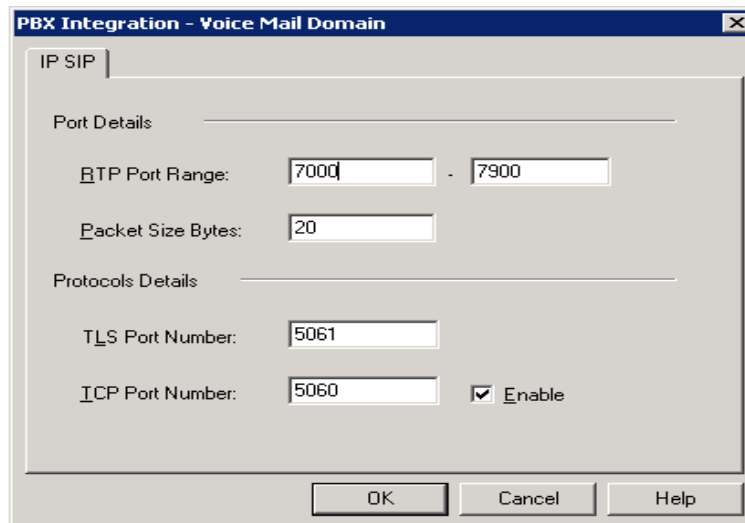
Click 'Configure' to set incoming and outgoing phone number translation rules. [Configure...](#)

Translation rules are effective only after MultiSite has been enabled.

OK Cancel Help

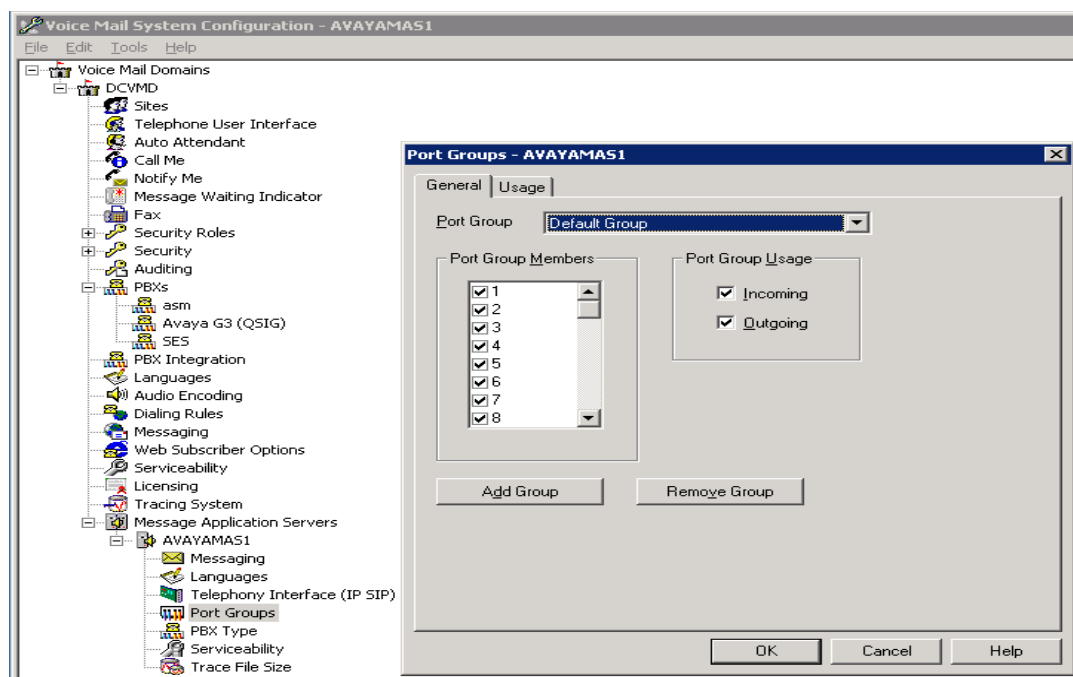
7.1.2. PBX Integration

On the **Voice Mail System Configuration – AVAYAMAS1** screen, double-click on **PBX Integration**. Confirm the default settings below and check the **Enable** check box if TCP is to be used. Click **OK** when completed.



7.1.3. Port Groups

On the **Voice Mail System Configuration – AVAYAMAS1** screen, expand **Message Application Servers** and expand the appropriate MAS server. Double click **Port Groups** and confirm all the **Port Group Members** and both the **Incoming** and **Outgoing** check boxes are selected. Click **OK** when completed



7.2. Configure Avaya Message Storage Server

7.2.1. Class of Service

From a Web browser, navigate to <http://<ip-addr>> where *<ip-addr>* is the IP address of the Avaya MSS. After logging in with an appropriate login and password, the main page appears. (not shown). Select **Messaging Administration** → **Classes-of-Service** from the left pane. From the **Manage Classes-of-Service** screen that is presented, select a Class of Service (COS) that will be used by subscribers using IPC turrets (in this example **class00** is selected). Click **Edit the Selected COS** button

Help Log Off

Messaging Administration

- Subscriber Management
- Activity Log Configuration
- Messaging Attributes
- Classes-of-Service**
- Enhanced-Lists
- Sending Restrictions
- System Administration
- Request Remote Update
- Networked Machines
- Trusted Servers

Server Administration

- Configure Using DCT
- TCP/IP Network Configura
- External Hosts
- MAS Host Setup
- MAS Host Send
- Windows Domain Setup
- Console Reboot Option
- Date/Time/NTP Server
- Syslog Server
- Modem/Terminal Display
- Modem/Terminal Configur
- Modem/Terminal Removal
- TCP/IP Service Settings

IMAP/SMTP Administration

- SMTP Options
- Mail Options
- IMAP/SMTP Status

Server Information

- Server Status
- Alarm Summary
- Disk Information
- Server Notes
- CMOS Settings
- RAID Status
- Rebuild RAID Status
- Reboot Interval

Utilities

- Rebuild RAID 1 Array
- CP/DPD Monitor

Manage Classes-of-Service

Server Name: 10.10.16.25 Number of Classes-of-Service: 512

COS Name	COS Number
class00	0
class01	1
class02	2
class03	3
class04	4
class05	5
class06	6
class07	7
ELA	8
class09	9
class10	10
class11	11
class12	12
class13	13
class14	14

Sort By Name

Display Report of COSs Edit the Selected COS

In the **Edit a Class-of-Service** screen that follows, select **yes** from the drop-down menu for the **Message Waiting Indication Allowed** field. Scroll down to the bottom of the screen and click the **Save** button (not shown).

Edit a Class-of-Service

Class of Service Number: 0		Class of Service Name class00	
MESSAGE RETENTION SETTINGS			
Retain New Messages (days)	<input type="checkbox"/> Forever 45	Retain Saved Messages (days)	<input type="checkbox"/> Forever 45
Retain Filed Messages (days)	<input type="checkbox"/> Forever 45		
MAILBOX AND MESSAGE SIZES			
Maximum Mailbox Size	36 Minutes	Maximum Call Answer Message	5 Minutes
Maximum Voice Mail Message	5 Minutes		
SUBSCRIBER FEATURES and SERVICES			
Time Zone	Use System Timezone		
Message Waiting Indication Allowed	yes	Call Me Allowed	no
Find Me Allowed	yes	Notify Me Allowed	no
Call Handling	yes	Call Screening	yes
Outbound Fax Calls	no	Extended Absence Greeting Allowed	yes
Inbound Fax	yes	Aria TUI Date & Time Playback	Never
Page via PBX	no	Record Mailbox Greetings	yes
Caller Application Announcement Recording	no	Caller Application	(none)
Telephone User Interface	MM Aria	Restrict Client Access	yes
Personal Operator Configuration	no	Unsent Message Allowed	no
Allow message after EAG	Always		
<input type="button" value="Back"/> <input type="button" value="Save"/> <input type="button" value="Help"/>			

7.2.2. Add Subscribers

Select **Messaging Administration** → **Subscriber Management** in the left pane. The **Manage Subscribers** page appears, as shown below. In the **Local Subscriber Mailbox Number** field, enter the extension of the desired IPC turret or Avaya extension and click the **Add or Edit** button.

Help Log Off This server: 10.10.16.25

Manage Subscribers

• Local Subscriber Mailbox Number 3301 [Add or Edit](#)

	Machine Name	Local Subscriber Mailboxes	Total Subscribers	Filtered Subscribers
• Local Subscribers	avayamss	31	32	32
• Remote Subscribers	internet		0	0

[Filter](#) [Manage](#) [Filter](#) [Manage](#) [Help](#)

In the **Add Local Subscriber** screen, fill in the required fields, in this example, IPC extension 3301 is used:

- For **Last Name** and **First Name** fields enter values appropriate for the user
- **Password**: Enter a default password for accessing the subscriber's mailbox, from one to 15 digits
- **Mailbox Number**: Enter a number, from 2 to 10 digits in length, which uniquely identifies the mailbox for the purpose of logging in or addressing messages. It must be within the range of Mailbox Numbers assigned to this system and be a valid length on the local machine
- **Numeric Address**: Enter a unique address in the voice mail network
- **Class of Service**: Select the Class of Service modified in **Section 7.2.1**
- **VoiceMail Enabled**: verify it is set to **yes**

Repeat this step for all desired IPC extensions.

Help Log Off This server: 10.

Add Local Subscriber

BASIC INFORMATION
* (Required Fields)

*Last Name	SIP	First Name	IPC Extension
*Password	*****	*Mailbox Number	3301
*Numeric Address	3301	PBX Extension	3301
*Class Of Service	0 - class00	*Community ID	1

SUBSCRIBER DIRECTORY

Email Handle	@avayamss.avaya.com	Telephone Number	3301
Common Name		ASCII Version of Name	

SUBSCRIBER SECURITY

Immediately Expire Password?	no	Is Mailbox Locked?	no
------------------------------	----	--------------------	----

MAILBOX FEATURES

Personal Operator Mailbox		Personal Operator Schedule	Always Active
VoiceMail Enabled	yes	Intercom Paging	paging is off

Navigation Menu:

- Messaging Administration
 - Subscriber Management
 - Activity Log Configuration
 - Messaging Attributes
 - Classes-of-Service
 - Enhanced-Lists
 - Sending Restrictions
 - System Administration
 - Request Remote Update
 - Networked Machines
 - Trusted Servers
- Server Administration
 - Configure Using DCT
 - TCP/IP Network Configura
 - External Hosts
 - MAS Host Setup
 - MAS Host Send
 - Windows Domain Setup
 - Console Reboot Option
 - Date/Time/NTP Server
 - Syslog Server
 - Modem/Terminal Display
 - Modem/Terminal Configu
 - Modem/Terminal Removal
 - TCP/IP Service Settings
- IMAP/SMTP Administration
 - SMTP Options
 - Mail Options
 - IMAP/SMTP Status
- Server Information
 - Server Status
 - Alarm Summary
 - Disk Information
 - Server Notes
 - CNDS Settings
 - RAID Status
 - Rebuild RAID Status
 - Reboot Interval
- Utilities
 - Rebuild RAID 1 Array
 - CD/DVD Mount
 - CD/DVD Unmount
 - CD/DVD Eject
 - Messaging DB Audits
 - Start Messaging
 - Stop Messaging
 - Shutdown Server
 - Reboot Server
- Logs
 - Administration History

To verify that mailboxes have been created, select **Messaging Administration** → **Subscriber Management**, click the **Manage** button to the right of the **Local Subscribers** entry. In the resulting **Manage Subscribers** screen that is presented (see below), verify that the mailboxes created appear in the list of subscribers.

Manage Local Subscribers

Local Subscriber Mailboxes: 31 Total Subscribers: 32
System Mailboxes: 1 Filtered Subscribers: 32

ASCII Name	Mailbox Number	Numeric Address	COS	CID	Subscriber Name
103, 3	3103	3103	0	1	103, 3
3106, Q-SIG	3106	3106	0	1	3106, Q-SIG
6610, Station	6610	6610	0	1	6610, Station
6630, SIP	6630	6630	0	1	6630, SIP
7200, PSTN	7200	7200	0	1	7200, PSTN
IP Station, second	6621	6621	0	1	1 hundred, 6
IP, Station	6620	6620	0	1	Station, IP
Leah, Princess	1601	1601	0	1	Leah, Princess
Mailbox, Pilot	8889	8889	0	1	Mailbox, Pilot
REM CM, Station	3701	3701	0	1	REM CM, Station
SIP, IPC Extension	3301	3301	0	1	SIP, IPC Extension
Solo, Hans	1602	1602	0	1	Solo, Hans
Station, IPC	3109	3109	0	1	Station, IPC
Station, IPC	3308	3308	0	1	Station, IPC
Station, IPC	3309	3309	0	1	Station, IPC

Buttons: Sort and Filter Subscribers, Display Report of Subscribers, Add a New Subscriber, Launch Subscriber Options, Delete the Selected Subscriber, Edit the Selected Subscriber

8. General Test Approach and Test Results

A simulated enterprise site using an Avaya IP telephony solution was connected to IPC via SIP connection provisioned between the Session Manager and IPC's ESS. The compliance test included the following:

- Incoming calls to the Avaya telephones, calls were made from IPC turrets to Avaya SIP, H.323, digital and analog telephones within the enterprise.
- Outgoing calls from the Avaya telephones, calls were made from Avaya SIP, H.323, digital and analog telephones to IPC turrets
- Calls using G.729A, G.711MU, and G.711A codecs.
- DTMF transmission using RFC 2833 with successful Voice Mail navigation
- User features such as hold and resume from Hold, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones.
- Voicemail coverage and retrieval for endpoints at the enterprise site.

The following is a list of items that were observed during compliance testing:

- Occasional failures were encountered when diverting a call to Modular Messaging, where the diverting party is a Communication Manager SIP user. This is being investigated by the Avaya team.

- In some instances of the more complex call scenarios for multiple diversions and/or transfers between the two enterprises where the final diversion is to Modular Messaging, inconsistencies were encountered with the last called party mail box or the initial called party mail box being received depending on the specific scenario being run. This is being investigated by the Avaya team.
- Connected name/number privacy is lost when invoked by called party, where the calling party is a Communication Manager SIP user. SIP user sees the connected name and number. This is being investigated by the Avaya team.
- Occasional failures of Communication Manager User screen display updates were encountered when various transfers scenarios between the two enterprise solutions were executed. This is being investigated by the Avaya team.
- Issues were encountered when using the Auto attendant function provided by Modular Messaging. Call failures were seen when Auto attendant transferred calls between two enterprise users. This is being investigated by the Avaya team.

These items were not deemed significant to fail the solution, and are listed here for user awareness. Testing of the sample configuration was completed with successful results for the IPC System Interconnect solution.

9. Verification Steps

The following steps can be used to verify that the required configuration has been correctly administered to support IPC System Interconnect architecture. To verify that any of the trunk groups are up, from the Communication Manager SAT use the **status trunk n** command, where **n** is the number of the trunk group. (Refer to **Sections 4.8, 4.9 and 5.5** for trunk details). Verify for each trunk, that the **Service State** shows in-service/idle.

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no

To ensure that all of the configured SIP entities and their associated links are in service from the system manager web interface click on **Session Manager → System Status → SIP entity monitoring**. Check that zero links are reported down under the **Entity Links Down/Total** heading.



▶ Asset Management
▶ Communication System Management
▶ User Management
▶ Monitoring
▶ Network Routing Policy
▶ Security
▶ Applications
▶ Settings
▼ Session Manager
Session Manager Administration
▶ Network Configuration
▶ Device and Location Configuration
▶ Application Configuration
▼ System Status
System State Administration
▶ SIP Entity Monitoring
Managed Bandwidth

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 - Moni Started
SessionManager	0/5	0	0

All Monitored SIP Entities

[Refresh](#)

5 Items	Filter: Enable
SIP Entity Name	
AccessElement	
Feature Server	
IPCESS1	
IPCESS2	
ModMessaging	

To confirm routing between all devices a number of calls should be made.

- Make a call from an Access Element extension to Feature Server extension and vice versa to confirm routing between them
- Make a call from an Access Element extension to and IPC extension and vice versa to confirm routing between them
- Make a call from a Feature Server extension to an IPC extension and vice versa to confirm routing between them
- Make a call from an Access Element extension to Feature Server extension and vice versa to confirm routing between them
- Make a call from an Access Element extension to Modular Messaging to confirm routing between them
- Make a call from a Feature Server extension to Modular Messaging to confirm routing between them
- Make a call from an IPC extension to Modular Messaging to confirm routing between them

10. Conclusion

These Application Notes describe the steps required to configure the Avaya components to successfully interoperate with IPC System Interconnect architecture using SIP as the transport method between components, Including, Avaya Aura™ Communication Manager Access Element, Avaya Aura™ Communication Manager Feature Server, Avaya Modular Messaging, Avaya Aura™ System Manager and Avaya Aura™ Session Manager.

11. Additional References

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

- [1] *Avaya Aura™ Communication Manager Special Application Features*, 10-Nov-2009
- [2] *Administering Avaya Aura™ Communication Manager*, 04-May-2009, Document Number 03-300509
- [3] *SIP Support in Avaya Aura™ Communication Manager Running on the Avaya S8xxx Servers* 04-May-2009, Document Number 555-245-206
- [4] *Administering Avaya Aura™ Communication Manager as a Feature Server*, 29-Jan-2010
- [5] *Administering Avaya Aura™ Session Manager*, 20-Nov-2009
- [6] *Modular Messaging Release 5.1 with the Avaya MSS - Messaging Application Server (MAS) Administration Guide*, 29-Jun-2009
- [7] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [8] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

APPENDIX A: DigitConversionAdaptor Module Parameters

There are currently 4 Module parameters defined, for the DigitConversionAdaptor two for egress and two for ingress which can be administered using either the full or an abbreviated name. The format of the **Adaptation Module** field is:

<Name of adaptation module> <name1=value1> <name2=value2>,...

For example the adaptation used in **Section 6.4** of this application note was:

DigitConversionAdaptor odstd-ipc.com iodstd=avaya.com

Egress Domain Modification Parameters are:

- **odstd** • (or **overrideDestinationDomain**) replaces the domain in a Request-URI and Notify/message-summary body with the given value for egress only.
- **osrcd** • (or **overrideSourceDomain**): replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for egress only.

Ingress Domain Modification Parameters:

- **iodstd** • (or **ingressOverrideDestinationDomain**): replaces the domain in a Request-URI and Notify/message-summary body with the given value for ingress only.
- **iosrcd** (or **ingressOverrideSourceDomain**): replaces the domain in the P-Asserted-Identity header and calling part of the History-Info header with the given value for ingress only.

©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.