



Configuring Avaya Modular Messaging with Avaya IP Office 6.0 (81006), Avaya Aura™ Session Manager 5.2 and Avaya Aura™ Communication Manager 5.2.1 as a Feature Server – Issue 1.0

Abstract

These Application Notes present a sample configuration for a network consisting of a Centralized Avaya Modular Messaging Solution supporting Avaya Aura™ Communication Manager as a Feature Server and Avaya IP Office. These three systems are connected via a common Avaya Aura™ Session Manager.

Testing was conducted via the Internal Interoperability Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The purpose of this interoperability Application Notes is to validate Avaya Modular Messaging for Avaya IP Office with SIP integration via Avaya Aura™ Session Manager. Avaya IP Office users have mailboxes defined in Modular Messaging which they can access via a dedicated pilot number. The sample network is shown in **Figure 1**, where Avaya Aura™ Communication Manager supports the Avaya 9620 IP Telephone (SIP). Avaya IP Office supports the Avaya 4610 IP Telephone (H.323) and the Avaya 2420 Digital Phone. Avaya Modular Messaging consists of Avaya Messaging Application Server and Avaya Message Storage Server. SIP trunks are used to connect these three systems to Avaya Aura™ Session Manager. All inter-system calls are carried over these SIP trunks. Avaya Aura™ Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow for multi-vendor systems to interoperate. Avaya Aura™ Session Manager is managed by a separate Avaya Aura™ System Manager, which can manage multiple Avaya Aura™ Session Managers.

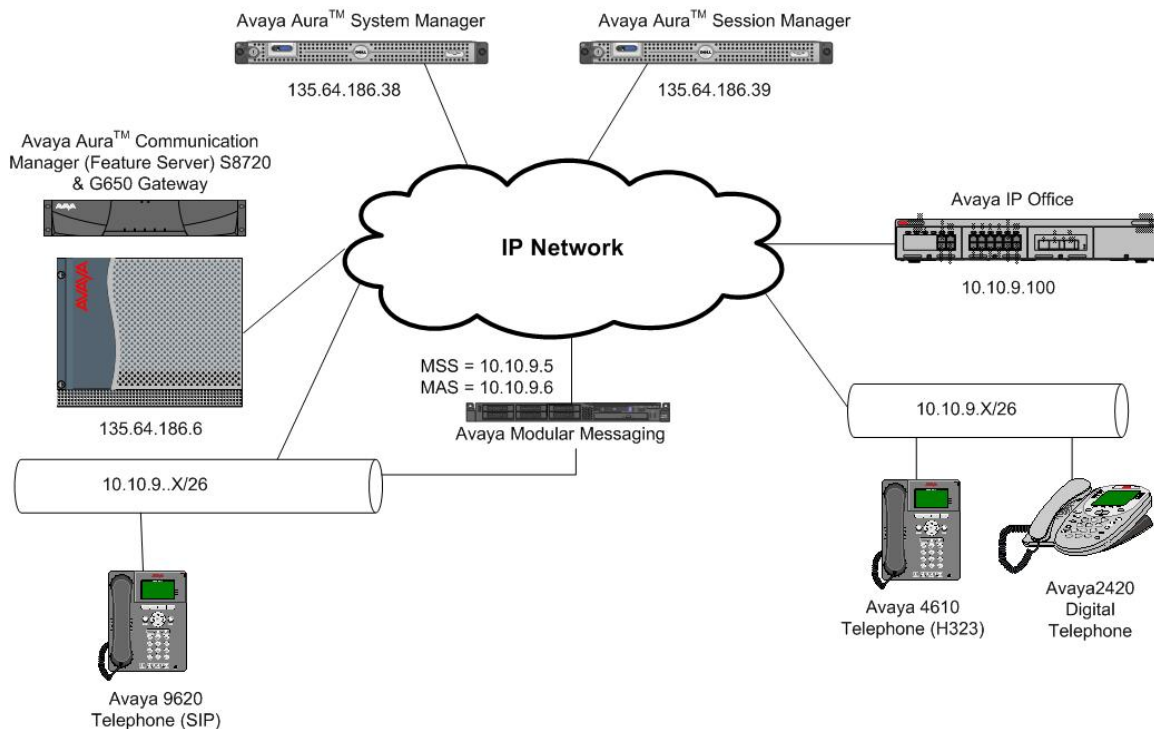


Figure 1: Connection of Avaya Aura™ Communication Manager, Avaya IP Office and Avaya Modular Messaging via Avaya Aura™ Session Manager using SIP Trunks

Avaya telephones are registered to Avaya Aura™ Communication Manager and Avaya IP Office. Avaya Aura™ Communication Manager stations use extensions 320xx. Avaya IP Office registered stations use extensions 701000890xx. One SIP trunk is provisioned from both PBX's to the Avaya Aura™ Session Manager to manage call control for calls between the two systems. One SIP trunk is provisioned to the Avaya Aura™ Session Manager to manage calls to/from Avaya Modular Messaging.

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8720 Media Server	Avaya Aura™ Communication Manager 5.2.1 SP2 (R015x.02.1.016.4)
Avaya G650 Media Gateway <ul style="list-style-type: none"> • TN799DP C-LAN Circuit Pack • TN2312BP IP Server Interface • TN2602AP IP Media Pro 	HW01 FW035 HW15 FW046 HW08 FW054
Avaya S8510 Server with SM100 Card	Avaya Aura™ Session Manager 5.2 SP2
Avaya S8510 Server	Avaya Aura™ System Manager 5.2 SP2
Avaya S8800 Server	Avaya Modular Messaging 5.2 SP2
Avaya 9620 IP Telephone (SIP)	2.6.2.18
Avaya 2420 Digital Phone	-
Avaya 4610 IP Telephone (H.323)	2.9 SP1
Avaya IP Office (IP500 V2)	Avaya IP Office 6.0 (81006)

3. Configure Avaya Aura™ Communication Manager

This section shows the configuration in Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). These Application Notes assumed that the basic configuration has already been administered. For further information on Communication Manager, please consult with references [4] and [5]. 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, Uniform Dial Plan and AAR analysis
- Administer Feature Access Codes
- Administer Hunt Group
- Administer Coverage Path
- Administer SIP Phone
- Save Changes

3.1. Verify Avaya Aura™ Communication Manager License

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

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

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		30	0
Maximum Concurrently Registered IP Stations:		18000	9
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:		10	1
Maximum Video Capable IP Softphones:		10	4
Maximum Administered SIP Trunks:		100	55

3.2. 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			

3.3. 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, **clan1a3** and **135.64.186.6** are entered as **Name** and **IP Address** for the CLAN card in Communication Manager running on the Avaya S8720 Server. In addition, **SM100** and **135.64.186.40** are entered for Session Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
Gateway001	135.64.186.1	
MBTCM	135.64.186.68	
MX6200	135.64.186.15	
SM100	135.64.186.40	
clan1a3	135.64.186.6	
clan1b3	135.64.186.7	
default	0.0.0.0	
mprola2	135.64.186.8	
mprolb2	135.64.186.9	
onexmobile	135.64.186.30	
procr	135.64.186.10	
silstackaes	135.64.186.28	

3.4. 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 3 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 **3** to use ip-codec-set 3.

change ip-network-region 3		Page 1 of 19
IP NETWORK REGION		
Region: 3		
Location:	Authoritative Domain: silstack.com	
Name: To ASM		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 3	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
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		
Keep-Alive Count: 5		

Use the **change ip-codec-set n** command, where **n** is the existing codec set number to configure the desired audio codec.

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

3.5. Administer SIP Signaling Group and Trunk Group

3.5.1. SIP Signaling Group

In the test configuration, Communication Manager acts as a Feature Server. An IMS enabled SIP trunk is required. Use signal group 150 along with trunk group 150 to reach the Session Manager. Use the **add signaling-group n** command, where **n** is the signaling-group number being added to the system. Use the values defined in **Section 3.3** and **3.4** for **Near-end Node Name**, **Far-End Node-Name** and **Far-End Network Region**. The **Far-end Domain** is left blank so that the signaling group accepts any authoritative domain. Set **IMS Enabled** to **y**.

add signaling-group 150

Page 1 of 2

SIGNALING GROUP

Group Number: 150

Group Type: sip

Transport Method: tcp

IMS Enabled? y

IP Video? n

Near-end Node Name: clanla3

Far-end Node Name: SM100

Near-end Listen Port: 5063

Far-end Listen Port: 5063

Far-end Network Region: 3

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? y

Direct IP-IP Early Media? n

Alternate Route Timer(sec): 6

3.5.2. SIP Trunk Group

Use the **add trunk-group n** command, where **n** is the new trunk group number being added to the system. The following screens show the settings used for trunk group 150.

Enter the following:

- **Group Type** **sip**
- **TAC** a numeric value i.e. **150**
- **Service Type** **tie**
- **Signaling Group** the signaling group defined in **Section 3.5.1**, i.e. **150**
- **Number of Members** set to a numeric value, i.e. **10**

```
add trunk-group 150                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 150          Group Type: sip          CDR Reports: y
Group Name: Avaya SIP phones      COR: 1          TN: 1          TAC: 150
Direction: two-way          Outgoing Display? y
Dial Access? n                      Night Service:
Queue Length: 0
Service Type: tie              Auth Code? n
                                     Signaling Group: 150
                                     Number of Members: 10
```

Navigate to **Page 3** and enter **private** for **Numbering Format**.

```
add trunk-group 150                                     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
Show ANSWERED BY on Display? Y
```

Navigate to **Page 4** and enter **120** for **Telephone Event Payload Type**.

```
add trunk-group 150                                     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: 120
```


3.6. Administer Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the **change route-pattern n** command, where **n** is the route pattern number specified in **Section 3.8**. Configure this route pattern to route calls to trunk group number **150** configured in **Section 3.5.2**. Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern.

change route-pattern 150													Page 1 of 3									
Pattern Number: 140 Pattern Name: To ASM																						
SCCAN? n Secure SIP? n																						
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC														
No			Mrk	Lmt	List	Del	Digits	QSIG														
								Intw														
1:	150	0								n	user											
2:								n	user													
3:								n	user													
4:								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							none							
2:	y	y	y	y	y	n	n	rest							none							
3:	y	y	y	y	y	n	n	rest							none							
4:	y	y	y	y	y	n	n	rest							none							

3.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling party number to be sent out through the SIP trunk. In the sample network configuration below, all calls originating from a 5-digit extension beginning with 320 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext	Ext	Trk	Private	Total		
Len	Code	Grp(s)	Prefix	Len		
5	2			5	Total Administered: 4	
5	4			5	Maximum Entries: 540	
5	8			5		
5	320			5		

3.8. Administer Dial Plan, Uniform Dial Plan and AAR analysis

Configure the dial plan for dialing 11-digit extensions beginning with **701000** to stations registered with IP Office. Use the **change dialplan analysis** command to define **Dialed String 701000** as a **udp** Call Type.

change dialplan analysis							Page 1 of 12	
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	Call Type
1	3	dac						
3	5	ext						
701000	11	udp						
9	1	fac						
*	3	fac						
#	3	fac						

Use the **change uniform-dialplan n** command where **n** is the dial string pattern to configure a **udp** entry for **Dialed String 701000**

change uniform-dialplan 7							Page 1 of 2	
UNIFORM DIAL PLAN TABLE								
							Percent Full: 0	
Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num		
701000	11	0		aar		n		

Use the **change aar analysis 0** command to configure an **aar** entry for **Dialed String 701000** to use **Route Pattern 150**. Add another entry to cover calls to the voicemail number **39999**.

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 2	
Dialed String	Total		Route	Call	Node	ANI		
	Min	Max	Pattern	Type	Num	Reqd		
701000	5	5	150	aar		n		
39999	5	5	150	aar		n		
5	7	7	254	aar		n		
6	7	7	254	aar		n		
9	7	7	254	aar		n		

3.9. 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**.

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: #00								
Attendant Access Code:								

```

Auto Alternate Routing (AAR) Access Code: *8
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
Automatic Callback Activation:                     Deactivation:
Call Forwarding Activation Busy/DA: *1      All: *2  Deactivation: *3
Call Forwarding Enhanced Status:             Act:    Deactivation:
Call Park Access Code:
Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
CDR Account Code Access Code:
Change COR Access Code:

```

3.10. Administer Hunt Group

Configure a Hunt Group to be used as the call coverage point for the call coverage path assigned to Modular Messaging subscribers. Use the **add hunt-group n** command where **n** is the hunt group number to be assigned. Configure a **Group Name** and **Group Extension** number to be used as the Modular Messaging pilot name and number. Select **ucd-mia** for **Group Type**.

```

add hunt-group 2                                     Page 1 of 60
                                     HUNT GROUP

Group Number: 2                                     ACD? n
Group Name: VoiceMail                               Queue? n
Group Extension: 39999                               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:

```

Navigate to **Page 2**. Select **sip-adjunct** for **Message Center**. For **Voice Mail Number** and **Voice Mail Handle** use the Group Extension number and Group Name defined on **Page 1** respectively. For **Routing Digits** use the AAR access code defined in **Section 3.9**.

```

add 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)
39999                  VoiceMail                *8

```

3.11. Administer Coverage Path

Configure a coverage path for the MAS subscribers. Use command **add coverage path n** where **n** is the coverage path number to be assigned. Configure **COVERAGE POINTS**, using value **hn** where **n** is the hunt group number defined in **Section 3.10**.

```
add coverage path 2

                                COVERAGE PATH

                                Coverage Path Number: 2
                                Cvg Enabled for VDN Route-To Party? n
                                Next Path Number:
                                Hunt after Coverage? n
                                Linkage

COVERAGE CRITERIA

    Station/Group Status    Inside Call    Outside Call
    Active?                 n             n
    Busy?                   y             y
    Don't Answer?           y             y
    All?                    n             n
    DND/SAC/Goto Cover?     y             y
    Holiday Coverage?       n             n
    Number of Rings: 2

COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
    Point1: h2              Rng: 2    Point2:
    Point3:                  Point4:
    Point5:                  Point6:
```

3.12. Administer SIP Phone

Configure the SIP Phone discussed in **Section 4.12** to allow call coverage to Modular Messaging. Use the command **change station 32007** and on **Page 1** for **Coverage Path 1** use the coverage path defined in **Section 3.11**.

```
change station 32007                                     Page 1 of 6

                                STATION

Extension: 32007                                Lock Messages? n
Type: 9650SIP                                    Security Code:
Port: S00004                                Coverage Path 1: 2
Name: phelan, tom                            Coverage Path 2:
                                                Hunt-to Station:
                                                BCC: 0
                                                TN: 1
                                                COR: 1
                                                COS: 1

STATION OPTIONS

    Loss Group: 19                                Time of Day Lock Table:
                                                Message Lamp Ext: 32007

    Display Language: english                    Button Modules: 0

    Survivable COR: internal
    Survivable Trunk Dest? y                    IP SoftPhone? n
                                                IP Video? n
```

Navigate to **Page 2** and set **MWI Served User Type** to **sip-adjunct** which is the **Message Center** defined in **Section 3.10**. Set **Per Station CPN - Send Calling Number** to **y**.

change station 32007		Page 2 of 6
STATION		
FEATURE OPTIONS		
LWC Reception: spe		Coverage Msg Retrieval? y
LWC Activation? y		Auto Answer: none
CDR Privacy? n		Data Restriction? n
		Idle Appearance Preference? n
		Bridged Idle Line Preference? n
Bridged Call Alerting? n		
Active Station Ringing: single		
H.320 Conversion? n	Per Station CPN - Send Calling Number? y	EC500 State: enabled
MWI Served User Type: sip-adjunct		
		Coverage After Forwarding? s
		Direct IP-IP Audio Connections? y
Emergency Location Ext: 32007	Always Use? n	IP Audio Hairpinning? n

3.13. Save Changes

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

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

4. Configuring Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager. For further information on Session Manager, please consult with references [1], [2] and [3]. 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 Regular Expression
- Administer Avaya Aura™ Session Manager
- Add Avaya Aura™ Communication Manager as a Feature Server
- Add Users for SIP Phones

4.1. Log in to Avaya Aura™ Session Manager

Access the Avaya Aura™ 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.

AVAYA Avaya Aura System Manager 5.2 Help

Home / Log On

Log On

You have successfully logged out.

Username :

Password :

Log On Cancel

Local intranet

By selecting **Network Routing Policy** from the left panel menu, a short procedure for configuring Network Routing Policy is shown on the right panel.

AVAYA

Avaya Aura System Manager 5.2

Welcome, **admin** Last Logged on at Nov. 04, 2009 3:42 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy

▶ 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

Shortcuts

Change Password

Landing Page

Help for Import All Data

Help for Export All Data

Help for Committing configuration changes

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)

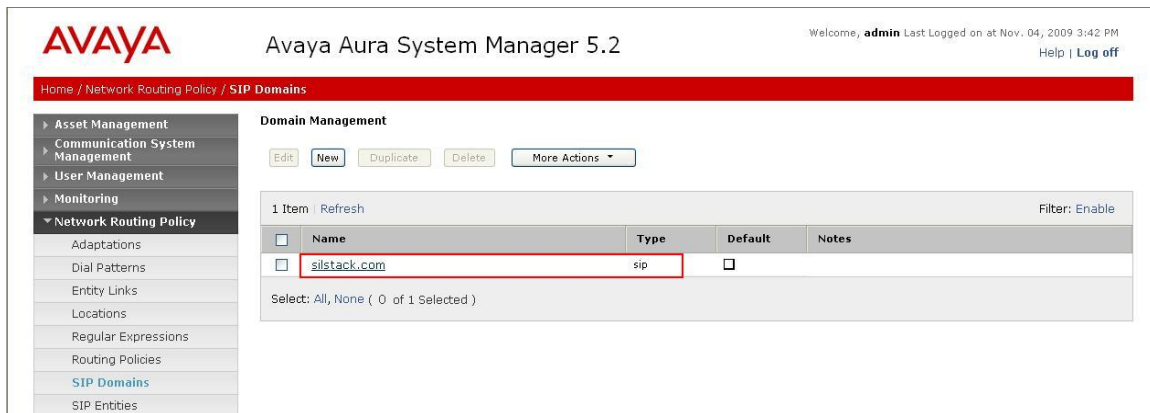
Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

4.2. Administer SIP Domain

Add the SIP domain, for which the communications infrastructure will be authoritative, by selecting **SIP Domains** on the left panel menu and clicking the **New** button (not shown) to create a new SIP domain entry. Complete the following options:

- **Name** The authoritative domain name (e.g., **silstack.com**)
- **Notes** Description for the domain (optional)

Click **Commit** to save changes. Verify the domain is created as in screenshot below.



The screenshot shows the Avaya Aura System Manager 5.2 interface. The top header includes the Avaya logo, the title 'Avaya Aura System Manager 5.2', and a welcome message for user 'admin' logged in on Nov. 04, 2009 at 3:42 PM. The breadcrumb trail is 'Home / Network Routing Policy / SIP Domains'. The left sidebar contains a navigation menu with the following items: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (expanded), Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains (selected), and SIP Entities. The main content area is titled 'Domain Management' and includes buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these buttons is a table with the following columns: Name, Type, Default, and Notes. The table contains one entry: 'silstack.com' with Type 'sip' and Default 'No'. The 'Name' field is highlighted with a red box. Below the table, it says 'Select: All, None (0 of 1 Selected)'.

Note: Since the sample network does not deal with any foreign domains, no additional SIP Domains entry is needed.

4.3. Administer Adaptations

In the sample configuration, multi-site Avaya Modular Messaging represents its subscribers using 11 digit telephone numbers. The 5 digit extension used by Communication Manager is preceded by the 6 digits 120122. DigitConversionAdapter is used in Session Manager to convert between the 5 and 11 digit formats when routing between Modular Messaging and Communication Manager. For the Modular Messaging adaptation (shown on the next page), enter the following information:

Under **General**:

- **Adaptation Name** An informative name for the adaptation e.g. **Voicemail**
- **Module Name** **DigitConversionAdapter**
- **Module Parameter** The domain name, e.g. **silstack.com**

The remaining fields can be left blank.

Under **Digit Conversion for Incoming Calls to SM** and **Digit Conversion for Outgoing Calls from SM**, click **Add** and then edit the fields in the resulting new row as shown below:

- **Matching Pattern** A Regular expression or partial digit string used to match the incoming dialed number
- **Min** Minimum dialed number length
- **Max** Maximum dialed number length
- **Delete Digits** Number of digits to delete from the beginning
- **Insert Digits** Number of digits to insert at the beginning
- **Address to Modify** Chose between **origination**, **destination** or **both**

Adaptation Details

General

* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

1 Item : Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*120122	*11	*11	*6		both	Delete 6 digits

Select : All, None (0 of 1 Selected)

Digit Conversion for Outgoing Calls from SM

2 Items : Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	*	*	*	*			
<input type="checkbox"/>	*3	*5	*5	*0	120122	both	

Click **Commit** to save.

Incoming calls to Communication Manager telephones (SIP INVITE messages) from Modular Messaging that use 11 digit numbers will be converted to the 5 digit form by deleting the first 6 digits. Session Manager will route the call based on the resulting 5 digit extension. Calls routed from Communication Manager to Modular Messaging will have their Request-URI, P-Asserted-Identity, and History-Info headers converted to 11 digit format by insertion of “120122” before being routed to Modular Messaging. See screen below for configuration used.

4.4. Administer SIP Entities

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

Under **General**:

- **Name** An informative name (e.g., **SessionManager**)
- **FQDN or IP Address** IP address of the signaling interface on the Session Manager
- **Type** **Session Manager** for Session Manager, **CM** for Communication Manager, or **Other** for IP Office
- **Time Zone** Time zone for this location

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top header shows the Avaya logo and the title 'Avaya Aura™ System Manager 5.2'. A user status bar indicates 'Welcome, admin Last Logged on at Nov. 11, 2009 8:32 AM' with links for 'Help' and 'Log off'. The breadcrumb trail reads 'Home / Network Routing Policy / SIP Entities / SIP Entity Details'. The left sidebar contains a navigation menu with categories like Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, and Security. 'SIP Entities' is selected under Network Routing Policy. The main content area is titled 'SIP Entity Details' and has 'General' and 'SIP Link Monitoring' tabs. The 'General' tab contains the following fields:

- Name:** SessionManager
- FQDN or IP Address:** 135.64.186.40
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text area)
- Location:** (dropdown menu)
- Outbound Proxy:** (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text area)

 At the top right of the form are 'Commit' and 'Cancel' buttons. The 'SIP Link Monitoring' tab at the bottom shows 'Use Session Manager Configuration' selected from a dropdown menu.

Under **Port**, click **Add**, and then edit the fields in the resulting new row.

- **Port** Port number on which the system listens for SIP requests
- **Protocol** Transport protocol to be used to send SIP requests

The following screen shows the Port definitions for the Session Manager SIP Entity.

The screenshot shows a web interface for managing ports. On the left, there is a 'Shortcuts' sidebar with links: 'Change Password', 'Help for SIP Entity Details fields', and 'Help for Committing configuration changes'. The main area has a 'Port' section with 'Add' and 'Remove' buttons. Below this is a table with 5 items, filtered by 'Enable'. The table has columns: 'Port', 'Protocol', 'Default Domain', and 'Notes'. The data rows are:

Port	Protocol	Default Domain	Notes
5060	TCP	silstack.com	
5061	TLS	silstack.com	
5062	TLS	silstack.com	
5063	TCP	silstack.com	
5064	TLS	silstack.com	

Below the table, it says 'Select: All, None (0 of 5 Selected)'. At the bottom right, there are 'Commit' and 'Cancel' buttons. A red box highlights the 'Port' column header and the first row of data.

The following screen shows the **SIP Entity Details** for Communication Manager.

The screenshot shows the 'Avaya Aura™ System Manager 5.2' interface. The top navigation bar includes the Avaya logo, the product name, and a welcome message for 'admin' logged in on Nov. 11, 2009 at 8:32 AM. The breadcrumb trail is 'Home / Network Routing Policy / SIP Entities / SIP Entity Details'. The left sidebar shows a tree view with categories: 'Asset Management', 'Communication System Management', 'User Management', 'Monitoring', 'Network Routing Policy', 'SIP Entities' (highlighted), 'Time Ranges', 'Personal Settings', 'Security', 'Applications', 'Settings', and 'Session Manager'. The main content area is titled 'SIP Entity Details' and has 'Commit' and 'Cancel' buttons. It is divided into two sections: 'General' and 'SIP Link Monitoring'. The 'General' section contains fields for: 'Name' (AvayaCMtom), 'FQDN or IP Address' (135.64.186.6), 'Type' (CM), 'Notes', 'Adaptation', 'Location', 'Time Zone' (Europe/Dublin), 'Override Port & Transport with DNS SRV' (unchecked), 'SIP Timer B/F (in seconds)' (4), 'Credential name', and 'Call Detail Recording' (none). The 'SIP Link Monitoring' section has a dropdown for 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. A red box highlights the 'Name', 'FQDN or IP Address', and 'Type' fields.

The following screen shows the **SIP Entity Details** for IP Office.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The left sidebar shows a navigation menu with 'SIP Entities' highlighted under 'Network Routing Policy'. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields: Name (IPOffice-Tom), FQDN or IP Address (10.10.9.100), Type (Other), Notes, Adaptation, Location, Time Zone (Europe/Dublin), Override Port & Transport with DNS SRV (unchecked), SIP Timer B/F (4 seconds), Credential name, Call Detail Recording (none), and SIP Link Monitoring (Use Session Manager Configuration). Commit and Cancel buttons are at the top right.

The following screen shows the **SIP Entity Details** for Modular Messaging.

The screenshot displays the Avaya Aura System Manager 5.2 interface. The left sidebar shows a navigation menu with 'SIP Entities' highlighted under 'Network Routing Policy'. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields: Name (Voicemail), FQDN or IP Address (10.10.9.6), Type (Modular Messaging), Notes, Adaptation (MM Adaptation), Location, Time Zone (Europe/Dublin), Override Port & Transport with DNS SRV (unchecked), SIP Timer B/F (4 seconds), Credential name, Call Detail Recording (none), and SIP Link Monitoring (Use Session Manager Configuration). Commit and Cancel buttons are at the top right.

4.5. Administer Entity Links

A SIP trunk between a Session Manager and a telephony system is described by 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.

- **Name** An informative name
- **SIP Entity 1** Select **SessionManager**
- **Port** Port number to which the other system sends its SIP requests
- **SIP Entity 2** The other SIP Entity for this link, created in **Section 4.4**
- **Port** Port number to which the other system expects to receive SIP requests
- **Trusted** Whether to trust the other system
- **Protocol** Transport protocol to be used to send SIP requests

Click **Commit** to save changes. The following screen shows the Entity Links used in the sample network.

AVAYA Avaya Aura System Manager 5.2

Welcome, **admin** Last Logged on at Nov. 04, 2009 3:42 PM
Help | Log off

Home / Network Routing Policy / Entity Links

Entity Links

Edit New Duplicate Delete More Actions Commit

8 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
<input type="checkbox"/>	Avaya	SessionManager	TLS	5062	AvayaCM	5062	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	AvayaTom	SessionManager	TCP	5063	AvayaCMtom	5063	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Branch Office	SessionManager	TLS	5061	Branch CM	5061	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	IPOffice-Tom	SessionManager	TCP	5060	IPOffice-Tom	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Feature Server	SessionManager	TLS	5064	feature	5064	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	MX-S6200	SessionManager	UDP	5065	MX-S6200	5065	<input checked="" type="checkbox"/>	Link to Mx6200
<input type="checkbox"/>	To OCS Mediation	SessionManager	TCP	5060	Stack OCS Mediation Server	5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	VoiceMail	SessionManager	TCP	5060	VoiceMail	5060	<input checked="" type="checkbox"/>	

Select: All, None (0 of 8 Selected)

4.6. Administer Time Ranges

Before adding routing policies (see next step), time ranges must be defined during which the policies will be active. In the sample network, one policy was defined that would allow routing to occur at anytime. To add this time range, select **Time Ranges** from the left panel menu and then click **New** on the right. Fill in the following fields.

- **Name** An informative name (e.g. **Always**)
- **Mo through Su** Check the box under each day of the week for inclusion
- **Start Time** Enter start time (e.g. **00:00** for start of day)
- **End Time** Enter end time (e.g. **23:59** for end of day)

Avaya Aura System Manager 5.2

Welcome, **admin** Last Logged on at Nov. 04, 2009 3:42 PM
Help | Log off

Home / Network Routing Policy / **Time Ranges**

Time Ranges

Edit New Duplicate Delete More Actions Commit

2 Items Refresh Filter: Enable

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

Select: All, None (0 of 2 Selected)

4.7. Administer Routing Policies

Create routing policies to direct how calls will be routed to a system. Two routing policies must be added, one for IP Office and one for Modular Messaging. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- Enter an informative **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 then select the time range configured in the previous step.

The following screen shows the **Routing Policy Details** for IP Office.

Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at July 15, 2010 1:21 PM

Help | Log off

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

Routing Policy Details

Commit Cancel

General

* Name: IPOffice-Tom

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
IPOffice-Tom	10.10.9.100	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

The following screen shows the **Routing Policy Details** for Modular Messaging.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Jan. 14, 2010 3:19 PM
[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
[Select](#)

Name	FQDN or IP Address	Type	Notes
voicemail	10.10.9.6	Modular Messaging	

Time of Day
[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item Refresh Filter: Enable

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

4.8. Administer Dial Patterns

A dial pattern must be defined that will direct calls to the appropriate telephony system. In the sample network, 5-digit extensions beginning with **320** reside on Communication Manager and 11-digit extensions beginning with **701000** reside on IP Office. The 5-digit extension 39999 is for calls to Modular Messaging. To configure IP Office Dial Pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- **Pattern** Dialed number or prefix
- **Min** Minimum length of dialed number
- **Max** Maximum length of dialed number
- **Notes** Comment on purpose of dial pattern
- **SIP Domain** Select **ALL**

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at July 15, 2010 1:21 PM
[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:

Navigate to **Originating Locations and Routing Policy List** and select **Add** (not shown). Under **Originating Location** select **ALL** and under **Routing Policies** select **IPOffice-Tom**. Click **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown previously), select **Commit** button to save.

- 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

Shortcuts
Change Password

Originating Location and Routing Policy List

Select Cancel

Originating Location

4 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	-ALL-	Any Locations
<input type="checkbox"/>	Avaya	
<input type="checkbox"/>	Cisco	
<input type="checkbox"/>	Stack Enterprise	Main Office for Stack Testing

Select : All, None (0 of 4 Selected)

Routing Policies

8 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	AvayaCM	<input type="checkbox"/>	AvayaCM	
<input type="checkbox"/>	AvayaCMtom	<input type="checkbox"/>	AvayaCMtom	
<input type="checkbox"/>	BranchCM	<input type="checkbox"/>	Branch CM	Branch CM
<input checked="" type="checkbox"/>	IPOffice-Tom	<input type="checkbox"/>	IPOffice-Tom	

A dial pattern must be defined that will direct calls to the Modular Messaging system. In the sample network, 5-digit extension 39999 will be used as the pilot number for Modular Messaging. For pilot number configuration perform the following. Select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- **Pattern** Pilot number
- **Min** Minimum length of pilot number
- **Max** Maximum length of pilot number
- **Notes** Comment on purpose of dial pattern
- **SIP Domain** Select **ALL**

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 14, 2010 4:42 PM Help | Log off

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

Dial Pattern Details [Commit] [Cancel]

General

* Pattern: 39999

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: -ALL-

Notes: MM 3rd Party Voicemail Number

Navigate to **Originating Locations and Routing Policy List** and select **Add** (not shown). Under **Originating Location** select all locations by checking the box next to **ALL** and under **Routing Policies** select the Routing Policy created in **Section 4.7**. Click **Select** button to confirm the chosen options and then be returned to the Dial Pattern screen (shown above), select **Commit** button to save.

Originating Location and Routing Policy List [Select] [Cancel]

Originating Location

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	-ALL-	Any Locations
<input type="checkbox"/>	Avaya	
<input type="checkbox"/>	Cisco	
<input type="checkbox"/>	Stack Enterprise	Main Office for Stack Testing

Select : All, None (0 of 4 Selected)

Routing Policies

13 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	AvayaCM	<input type="checkbox"/>	AvayaCM	
<input type="checkbox"/>	AvayaCMtom	<input type="checkbox"/>	AvayaCMtom	
<input type="checkbox"/>	BranchCM	<input type="checkbox"/>	Branch CM	Branch CM
<input type="checkbox"/>	Cisco	<input type="checkbox"/>	Cisco	
<input checked="" type="checkbox"/>	Voicemail	<input type="checkbox"/>	MM 3rd Party	

4.9. Administer Regular Expression

A Regular Expression must be defined for Communication Manager MAS subscribers so that they can communicate with Modular Messaging via Session Manager. The format of the Regular Expression is **voicemail handle**@domain name, where voicemail handle is the handle defined in **Section 3.10**. Select **Regular Expressions** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- **Pattern** Voicemail Handle@Domain Name
- **Rank Order** A unique number
- **Notes** Comment on purpose of Regular Expression

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Jan. 14, 2010 4:42 PM Help | Log off

Home / Network Routing Policy / Regular Expressions / Regular Expression Details

Regular Expression Details

Commit Cancel

General

* Pattern: Voicemail@silstack.com

* Rank Order: 1

Deny: ☐

Notes:

Routing Policy

Add Remove

Navigate to **Routing Policies** and select **Add**. Under **Routing Policies** select the routing policy created in **Section 4.7**. Click **Select** button to confirm the chosen option and then be returned to the **Regular Expression Details** screen (shown above), select **Commit** button to save.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Jan. 14, 2010 4:42 PM Help | Log off

Home / Network Routing Policy / Regular Expressions / Regular Expression Details / Routing Policy Details

Routing Policy List

Select Cancel

Routing Policies

13 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	AvayaCM	<input type="checkbox"/>	AvayaCM	
<input type="checkbox"/>	AvayaCMtom	<input type="checkbox"/>	AvayaCMtom	
<input type="checkbox"/>	BranchCM	<input type="checkbox"/>	Branch CM	Branch CM
<input type="checkbox"/>	Cisco	<input type="checkbox"/>	Cisco	
<input type="checkbox"/>	voicemail	<input type="checkbox"/>	MM 3rd Party	

4.10. Administer 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 Session Manager
- **Default Gateway** Enter the IP address of the default gateway for Session Manager

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

The screenshot displays the 'Add Session Manager' configuration page. The left sidebar shows a navigation tree with 'Session Manager Administration' selected. The main content area is titled 'Add Session Manager' and includes a 'Commit' button. The form is divided into two sections: 'General' and 'Security Module'. The 'General' section contains fields for 'SIP Entity Name' (set to 'Session Manager'), 'Description' (set to 'Session Manager'), 'Management Access Point Host Name/IP' (set to '135.64.186.39'), and a 'Direct Routing to Endpoints' dropdown (set to 'Enable'). The 'Security Module' section contains fields for 'SIP Entity IP Address' (set to '135.64.186.40'), 'Network Mask' (set to '255.255.255.224'), 'Default Gateway' (set to '135.64.186.33'), 'Call Control PHB' (set to '46'), 'QOS Priority' (set to '6'), 'Speed & Duplex' (set to 'Auto'), and a 'VLAN ID' field.

Home / Session Manager / Session Manager Administration / New Session Manager

Add Session Manager

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

General

- *SIP Entity Name: Session Manager
- Description: Session Manager
- *Management Access Point Host Name/IP: 135.64.186.39
- *Direct Routing to Endpoints: Enable

Security Module

- SIP Entity IP Address: 135.64.186.40
- *Network Mask: 255.255.255.224
- *Default Gateway: 135.64.186.33
- *Call Control PHB: 46
- *QOS Priority: 6
- *Speed & Duplex: Auto
- VLAN ID:

4.11. 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.

4.11.1. Create an Application Entity

Select **Applications** → **Entities** on the left. Click on **New** (not shown). Enter the following fields and use defaults for the remaining fields:

- **Name** A descriptive name
- **Type** Select **CM**
- **Node** Select **Other** and enter the IP address for CM SAT access

The screenshot shows 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 bar indicating 'Welcome, admin' and 'Last Logged on at Nov. 16, 2009 1:32 PM'. Below the navigation bar is a red breadcrumb trail: 'Home / Applications / Application Management / Applications Details'. On the left is a sidebar menu with categories like 'Asset Management', 'Communication System Management', 'User Management', 'Monitoring', 'Network Routing Policy', 'Security', 'Applications', and 'Settings'. The 'Applications' category is expanded, showing sub-items: 'FPM', 'MSA', 'NMC', 'Session Manager 5.2', 'SMGR', 'SIP AS 8.0', 'Entities' (highlighted with a red box), and 'Settings'. The main content area is titled 'New CM Instance' and contains a form with the following fields: 'Name' (text input with 'EnterpriseCM' entered, highlighted with a red box), 'Type' (dropdown menu with 'CM' selected, highlighted with a red box, and a 'Reset' link), 'Description' (text area), and 'Node' (dropdown menu with '135.64.186.10' selected, highlighted with a red box). At the top right of the form are 'Commit' and 'Cancel' buttons.

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

Click on **Commit** to save.

The screenshot shows a web interface for configuring system attributes. The 'Attributes' tab is selected and highlighted with a red box. Below the tab, there are several input fields: '* Login', 'Password', and 'Confirm Password', all of which are highlighted with red boxes. Below these are checkboxes for 'Is SSH Connection' (checked) and 'Is ASG Enabled' (unchecked). There are also input fields for '* Port' (containing '5022'), 'RSA SSH Fingerprint (Primary IP)', 'RSA SSH Fingerprint (Alternate IP)', 'Alternate IP Address', 'ASG Key', 'Confirm ASG Key', and 'Location'. At the bottom left, there is a '* Required' label. At the bottom right, there are 'Commit' and 'Cancel' buttons, with the 'Commit' button highlighted by a red box.

4.11.2. Create a Feature Server Application

Select **Session Manger** → **Application Configuration** → **Applications** on the left. Click on **New** (not shown). Enter following fields and use defaults for the remaining fields and click on **Commit** to save.

- **Name** A descriptive name
- **SIP Entity** Select the CM SIP Entity defined in **Section 4.4**

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Nov, 16, 2009 1:32 PM Help Log off

Home / Session Manager / Application Configuration / Application Editor

Application Editor [Commit] [Cancel]

Application Editor

* Name [Feature]

* SIP Entity [AvayaCMtom]

Description []

Application Attributes (optional)

Name	Value
Application Handle	[]
URI Parameters	[]

*Required [Commit] [Cancel]

4.11.3. Create a Feature Server Application Sequence

Select **Session Manager** → **Application Configuration** → **Application Sequences** on the left. 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.

Application Sequence Editor [Commit] [Cancel]

Sequence Name

* Name [App Sequence]

Description []

Applications in this Sequence

[Move First] [Move Last] [Remove]

	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		feature	feature	<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"/>	feature	feature	

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

AVAYA Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Nov. 16, 2009 1:32 PM Help | Log off

Home / Communication System Management / Telephony / System

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"/>	EnterpriseCM	135.64.186.10	Nov 16, 2009 02:00:28 AM +0000	Incremental	Failed		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

4.12. 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 Nov. 16, 2009 1:32 PM Help | Log off

Home / User Management / User Management / New User

New User Profile Commit Cancel

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

General ▼

* Last Name: phelan
* First Name: tom
Middle Name:
Description:

User Type:
☐ administrator
☐ communication_user
☐ agent
☐ supervisor
☐ resident_expert
☐ service_technician
☐ lobby_phone

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

- **Login Name** The desired phone extension number@domain.com where domain was defined in **Section 4.2**
- **Password** Password for user to log into System Manager (SMGR)
- **Shared Communication Profile Password** Password to be entered by the user when logging into the phone.

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:

Navigate to and click on **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

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: 32007 @ silstack.com ▾

Add

Cancel

Navigate to and click on **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 4.11.3**. Click on **Station Profile** to expand that section. Enter the following fields and use defaults for the remaining fields:

- **System** Select the CM Entity
- **Extension** Enter a desired extension number
- **Template** Select a telephone type template
- **Port** Select **IP**

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

The screenshot displays a web-based configuration interface. The 'Session Manager' section is expanded, showing three dropdown menus: 'Session Manager Instance' (set to 'SessionManager'), 'Origination Application Sequence' (set to 'App_sequence'), and 'Termination Application Sequence' (set to 'App_sequence'). Below this, the 'Messaging Profile' section is collapsed. The 'Station Profile' section is expanded, showing several fields: 'System' (dropdown set to 'EnterpriseCM'), 'Use Existing Stations' (checkbox), 'Extension' (text input with '32007'), 'Template' (dropdown set to 'DEFAULT_9650SIP'), 'Set Type' (text input with '9650SIP'), 'Security Code' (text input), 'Port' (dropdown set to 'IP'), and 'Delete Station on Unassign of Station from User' (checkbox). Red boxes highlight the 'Session Manager', 'Station Profile', and the individual fields mentioned in the instructions.

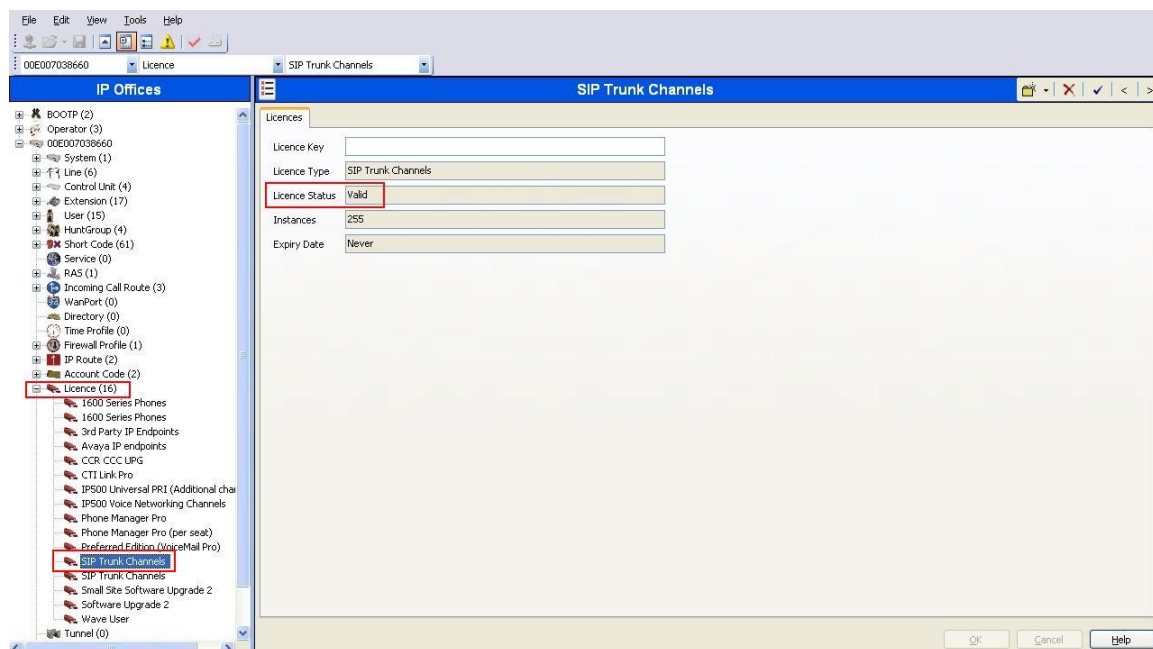
5. Configure Avaya IP Office

This section provides the procedures for configuring Avaya IP Office. The procedures include the following areas:

- Verify Avaya IP Office License
- Obtain LAN IP Address
- Administer Network Topology
- Administer SIP Registrar
- Administer Codec Preference
- Administer SIP Trunk to Avaya Aura™ Session Manager
- Administer Voicemail
- Administer Branch Prefix
- Administer Short Codes
- Administer Voicemail on End Users
- Save Configuration

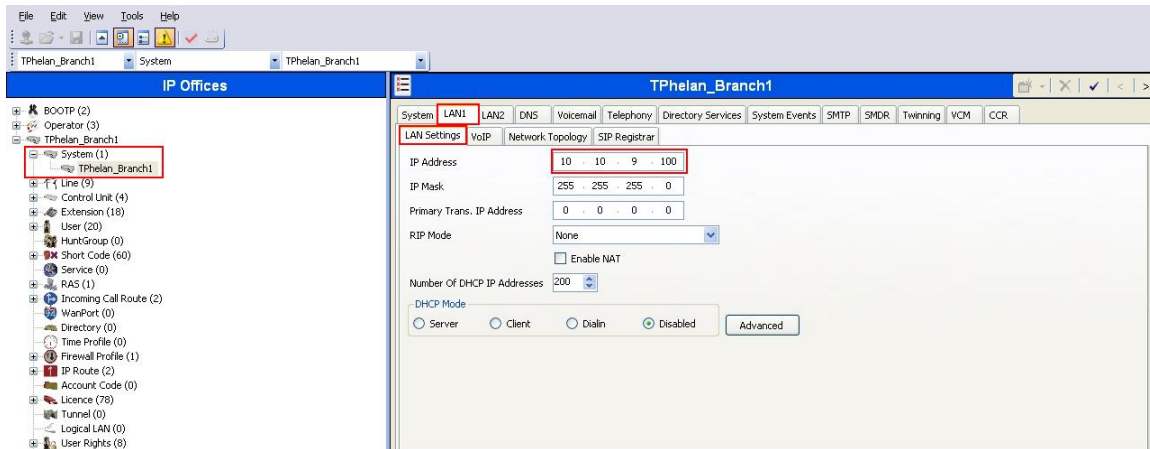
5.1. Verify Avaya IP Office License

From a PC running the Avaya IP Office Manager application, select **Start → Programs → IPOffice → Manager** to launch the Manager application. Select the proper IP Office system, and log in with the appropriate credentials. The **Avaya IP Office Manager** screen is displayed. From the configuration tree in the left pane, select **License → SIP Trunk Channels** to display the **SIP Trunk Channels** screen in the right pane. Verify that the **License Status** is **Valid** and if not contact your Avaya representative.



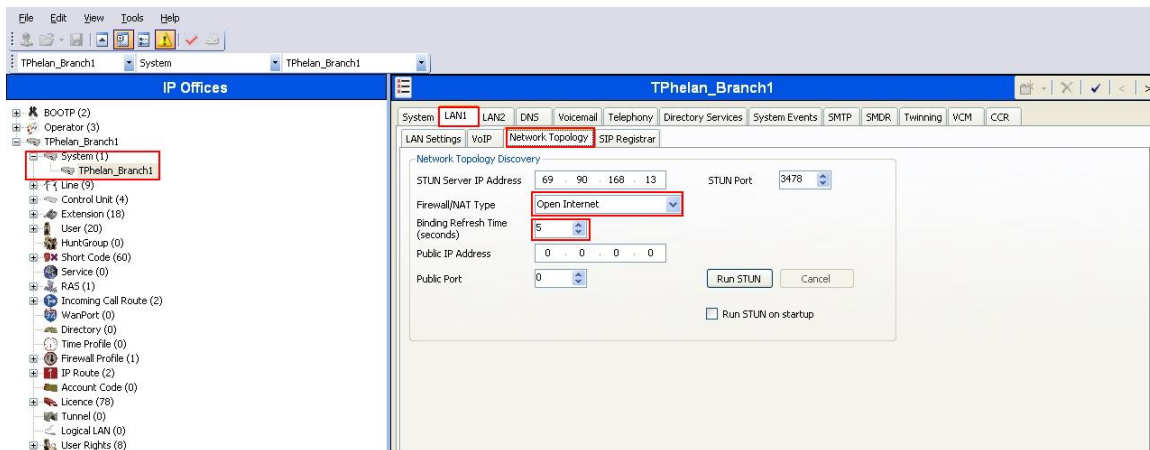
5.2. Obtain LAN IP Address

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab. The **IP address** will be the one defined for the IP Office SIP Entity in **Section 4.4** Note that IP Office can support SIP trunks on the LAN1 and/or LAN2 interfaces, and the sample configuration used the LAN1 interface.



5.3. Administer Network Topology

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **LAN1** tab, followed by the **Network Topology** sub-tab. Configure **Firewall/NAT Type** to **Open Internet** and **Binding Refresh Time** to **5**. Click **OK** (not shown).

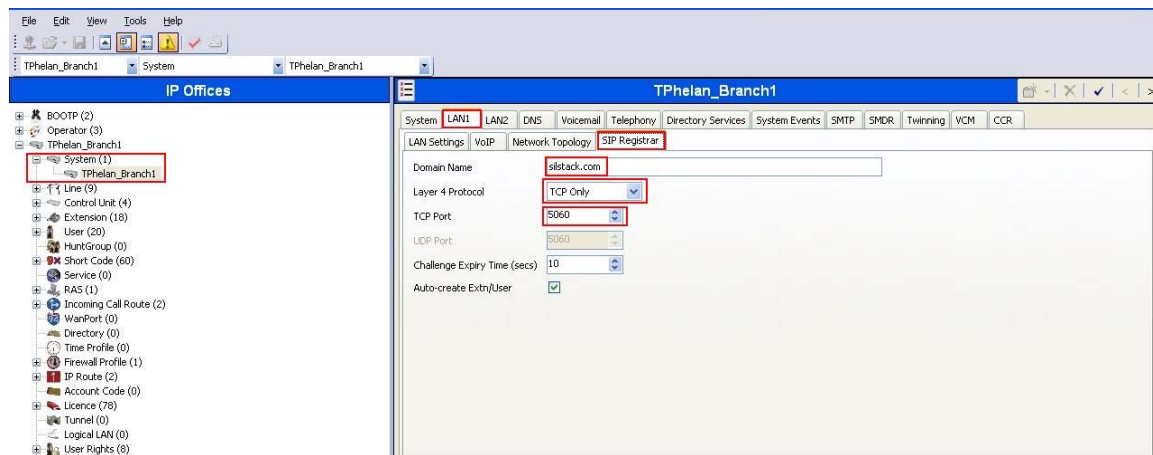


5.4. Administer SIP Registrar

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **LAN1** tab, followed by the **SIP Registrar** sub-tab in the right pane and enter following values:

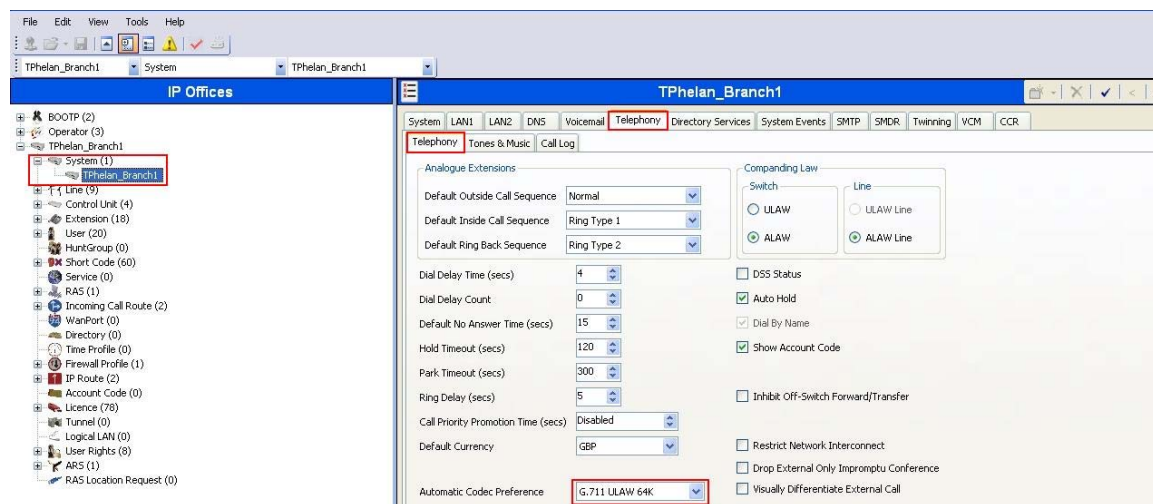
- **Domain Name** Enter a valid Domain Name
- **Layer 4 Protocol** Select **TCP only**
- **TCP Port** Select **5060**

Click **OK** (not shown).



5.5. Administer Codec Preference

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **Telephony** tab followed by the **Telephony** sub-tab in the right pane. Configure **Automatic Codec Preference** to **G.711 ULAW 64K**. Click **OK** (not shown).



5.6. Administer SIP Trunk to Avaya Aura™ Session Manager

From the configuration tree in the left pane, right-click on **Line** and select **New → SM Line** to add a new SIP Trunk towards Session Manager. Select the **Session Manager** tab and enter the following values:

- **Line Number** Select a unique Line Number
- **SM Domain** Enter a Domain Name
- **SM Address** Enter the IP address for SM-100 card

Retain default values for all other fields. Click **OK** (not shown).

The screenshot shows the Avaya Aura configuration interface. On the left, a tree view shows the configuration hierarchy: IP Offices > TPhelan_Branch1 > System (1) > Line (9). Line 17 is selected. The main pane shows the 'SM Line - Line 17' configuration. The 'Session Manager' tab is active. Fields are as follows:

Field	Value
Line Number	17
SM Domain Name	silstack.com
SM Address	135 . 64 . 186 . 40
Inactivity Timeout (seconds)	0
Outgoing Group ID	99999
Prefix	
Max Calls	10
Layer 4 Protocol	TCP
Send Port	5060
Listen Port	5060

Select the **VoIP** tab and enter the following values:

- **DTMF Support** **RFC2833**
- **Fax Transport Support** Tick the box
- **Allow Direct Media Path** Tick the box
- **Re-invite Supported** Tick the box

Retain default values for all other fields. Click **OK** (not shown).

The screenshot shows the Avaya Aura configuration interface. On the left, the same tree view is shown. The main pane shows the 'SM Line - Line 17' configuration. The 'VoIP' tab is active. Fields are as follows:

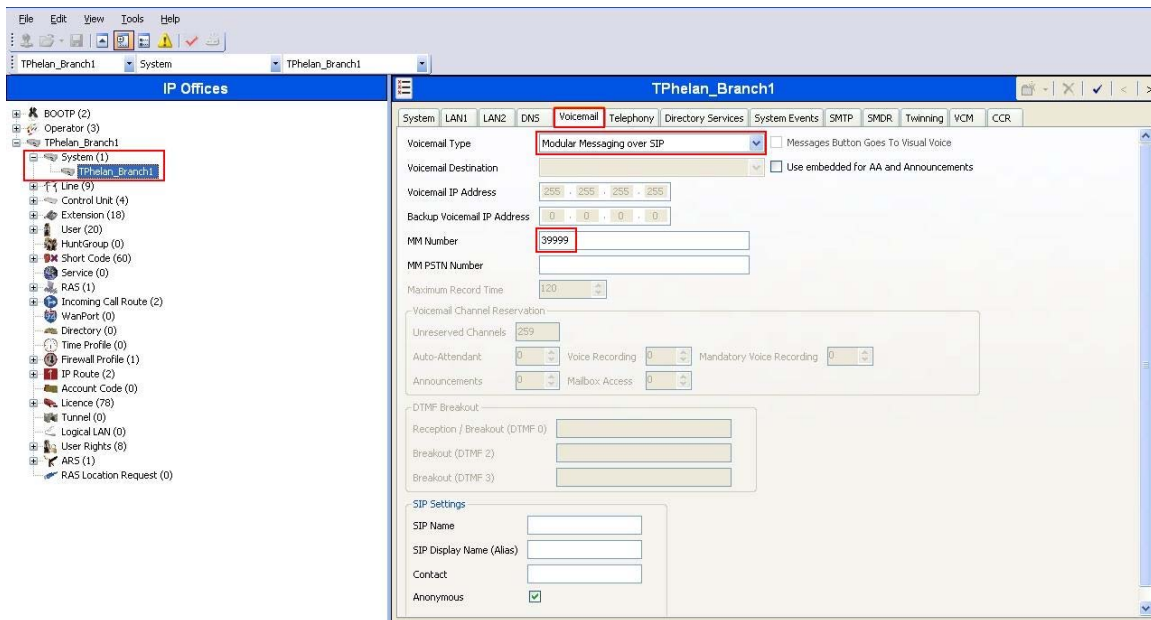
Field	Value
Compression Mode	Advanced
Call Initiation Timeout (s)	4
DTMF Support	RFC2833
VoIP Silence Suppression	<input type="checkbox"/>
Fax Transport Support	<input checked="" type="checkbox"/>
Allow Direct Media Path	<input checked="" type="checkbox"/>
Re-invite Supported	<input checked="" type="checkbox"/>
Use Offerer's Preferred Codec	<input type="checkbox"/>

5.7. Administer Voicemail

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **Voicemail** tab and enter the following values:

- **Voicemail Type** **Modular Messaging over SIP**
- **MM Number** Enter the MM Pilot number

Retain default values for all other fields. Click **OK** (not shown).

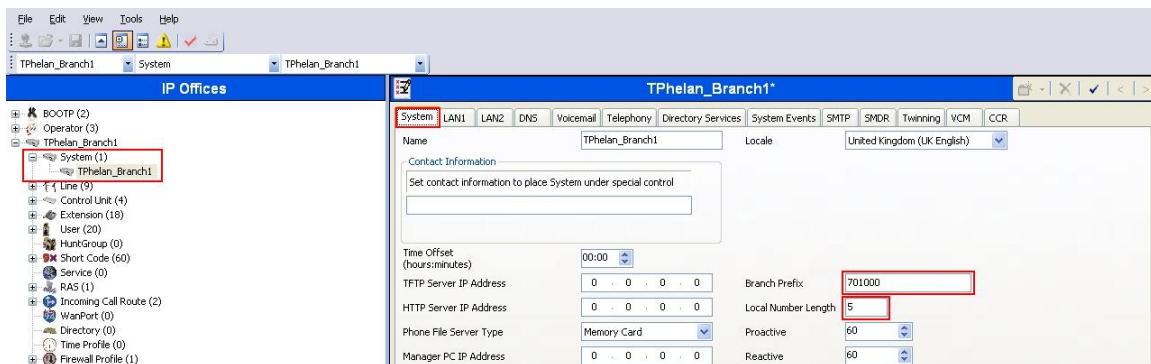


5.8. Administer Branch Prefix

From the configuration tree in the left pane, select **System** to display the system screen in the right pane. Select the **System** tab and enter the following values:

- **Branch Prefix** Enter a desired Branch Prefix
- **Local Number Length** Enter a desired Local Number Length

Retain default values for all other fields. Click **OK** (not shown).

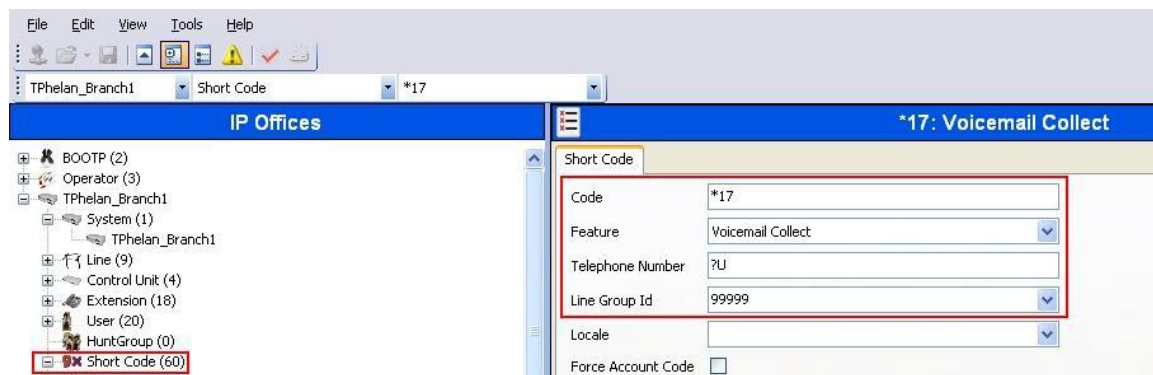


5.9. Administer Short Codes

From the configuration tree in the left pane, right-click on **Short Code**, and select **New**. Enter the following details to define a short code to access Voicemail:

- **Code** Enter a dialing string that will be used to dial Voicemail
- **Feature** Select **Voicemail Collect**
- **Telephone Number** Enter **?U**
- **Line Group ID** Select **Outgoing Group ID** from **Section 5.6**

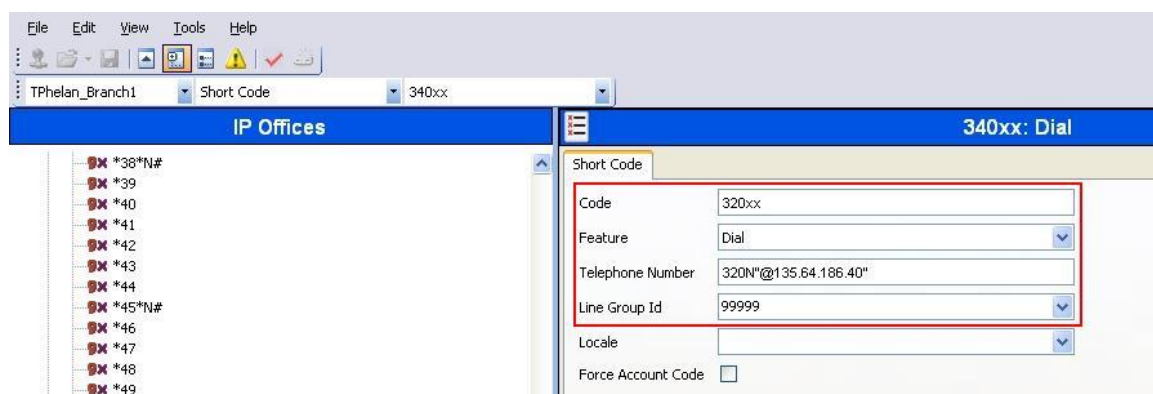
Retain default values for all other fields. Click **OK** (not shown).



Add another Short Code to dial Communication Manager extensions using the following details:

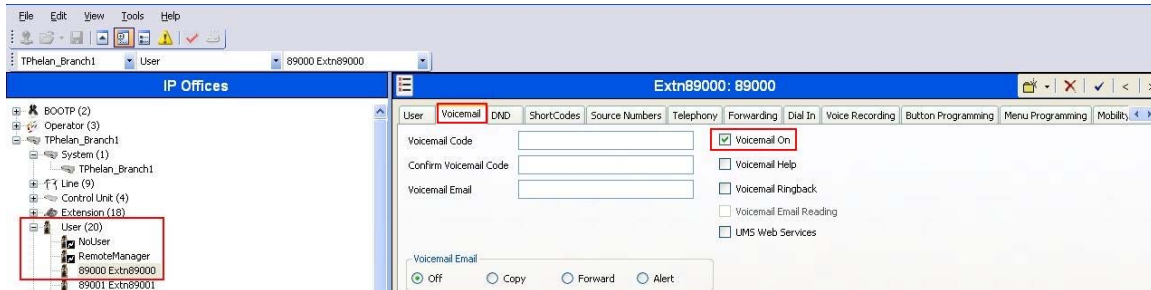
- **Code** Enter a dialing string used to call CM phones
- **Feature** Select **Dial**
- **Telephone Number** Enter the phone number appended with “@<ip-address of SM-100 card>”
- **Line Group ID** Select **Outgoing Group ID** from **Section 5.6**

Retain default values for all other fields. Click **OK** (not shown).



5.10. Administer Voicemail on End Users

From the configuration tree in the left pane, select **User**. Select a user and in the right-pane under the **Voicemail** tab, tick the box next to **Voicemail On**. Click **OK** to save (not shown).



5.11. Save Configuration

Select **File → Save Configuration** to save and send the configuration to the IP Office server.

6. Configure Avaya Modular Messaging

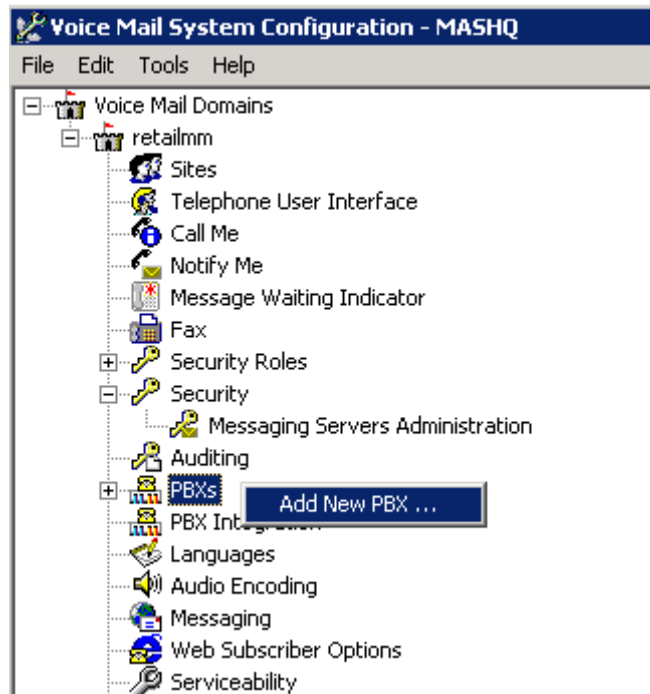
In sample configuration, the Communication Manager and IP Office telephone systems were added as sites to a multi-site Modular Messaging system, which was modified to support their subscribers and communication with Session Manager. The procedures include the following areas:

- Administer PBXs
- Administer Sites
- Administer Subscribers

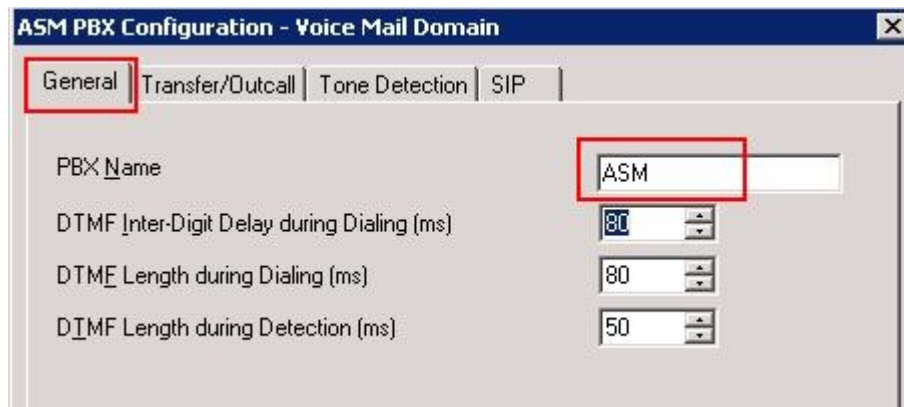
See references [6] to [8] in **Section 9** for standard installation and configuration information. General knowledge of the configuration tools and interfaces is assumed.

6.1. Administer PBXs

The aggregate Session Manager, Communication Manager and IP Office systems are defined to Modular Messaging as a PBX. In the MAS, open the **Voice Mail System Configuration** program, select **PBXs**, and right-click on the mouse to select **Add New PBX**, as shown below.



On the **General** tab of the resulting displayed window, enter an appropriate **PBX Name**. Defaults can be used for the remaining fields.



The screenshot shows the 'ASM PBX Configuration - Voice Mail Domain' window with the 'General' tab selected. The 'PBX Name' field is highlighted with a red box and contains the text 'ASM'. Below it, the 'DTMF Inter-Digit Delay during Dialing (ms)' is set to 80, 'DTMF Length during Dialing (ms)' is set to 80, and 'DTMF Length during Detection (ms)' is set to 50. The 'Transfer/Outcall', 'Tone Detection', and 'SIP' tabs are also visible.

On the **Transfer/Outcall** tab, select **Full** for **Transfer Mode**.



The screenshot shows the 'ASM PBX Configuration - Voice Mail Domain' window with the 'Transfer/Outcall' tab selected. The 'Transfer Mode' dropdown menu is highlighted with a red box and shows 'Full' selected. The 'General', 'Tone Detection', and 'SIP' tabs are also visible.

Default values can be used for the **Tone Detection** tab. On the **SIP** tab navigate to the **Gateways** section, click on the + icon and add the Session Manager's Asset Card IP address under **Address/FQDN**, **TCP** for **Protocol**, and click the MWI box so message waiting notifications will be sent. Fill in **SIP Domain** with the domain from **Section 4.2**. Click on **Configure** to specify number translation rules for translating between the local dial plans of the Communication Manager and IP Office telephone systems and the canonical 11 digit form used by Modular Messaging.

ASM PBX Configuration - Voice Mail Domain

General | Transfer/Outcall | Tone Detection | **SIP**

Gateways

Address/FQDN	Protocol	MWI	SRTP
<input checked="" type="checkbox"/> 135.64.186.40	TCP	<input checked="" type="checkbox"/>	None

SIP Domain:

P-Asserted-Identity:

PBX Address:

Phone Number Translation Rules

Click 'Configure' to set incoming and outgoing phone number translation rules.

In the right pane, create the appropriate rules to translate between the 5-digit (Communication Manager) and 11-digit (IP Office) extensions dialed and the canonical 11 digit numbers used by Modular Messaging. For the sample configuration, three rules are required and were added by selecting **Add**. As described in **Section 4.3**, Session Manager will translate between 11-digit numbers used by Modular Messaging and 5-digit numbering used by the Communication Manager telephone system. The **Avaya CM 11-digit** and **IP Office 11-digit** Incoming and Outgoing translation rules specify that Modular Messaging will change the number to/from the canonical form. Modular Messaging, when configured for Multi-Site, requires the number to be in canonical form (a number with a + prefix). The **Avaya ext** rule supports features such as extension dialing by subscribers while accessing Modular Messaging and translate the 5-digit extension format into canonical 11-digit format. Proper operation of the rules can be verified by adding **Test inputs** in the left pane and viewing the resulting output in the corresponding rule in the right pane. Click on **OK** when finished, then again on **OK** in the original **Add new PBX** window (see previous screen).

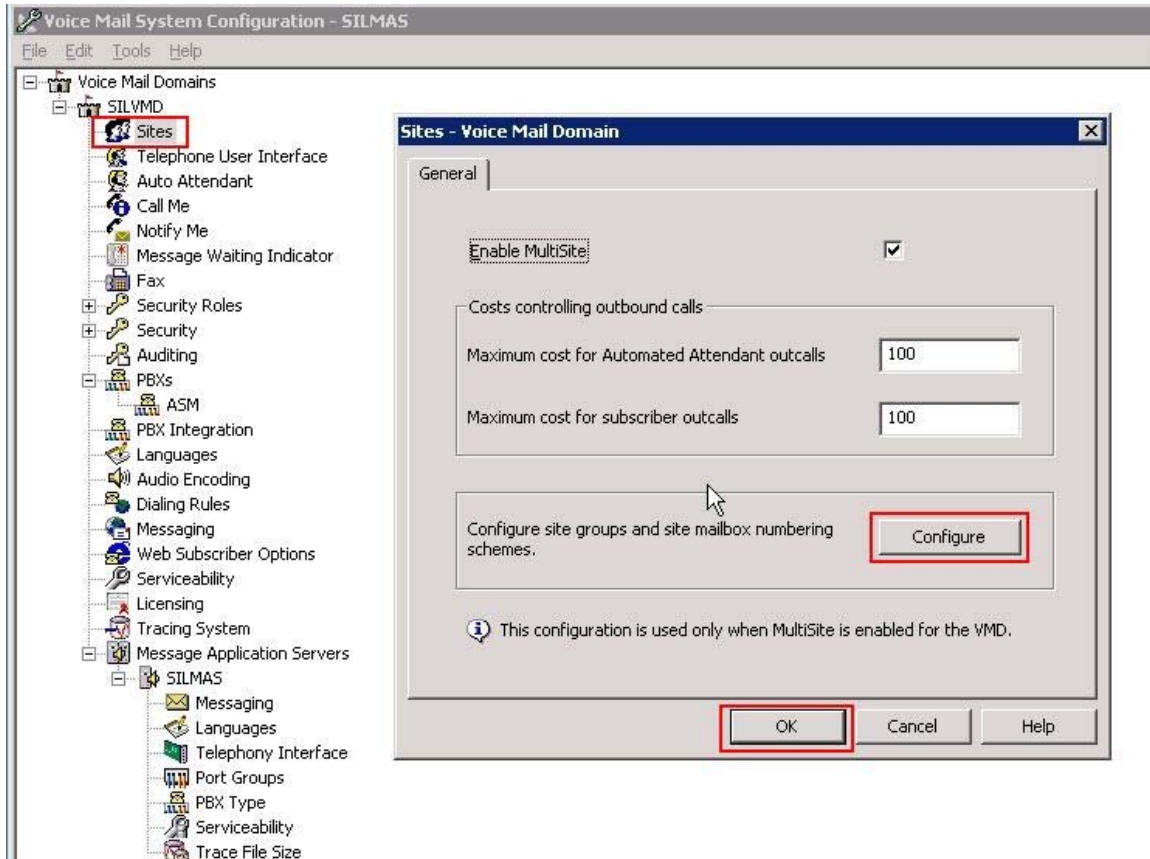
Incoming translation rule		Outgoing translation rule	
Description	Match	Output	Canonical Test
Avaya 11-digit (SIP)	^(12012234\d(3))\$	+\$1	^(120122(34\d(3))\$
Avaya 11-digit	^(12012232\d(3))\$	+\$1	^(120122(32\d(3))\$
Cisco 11-digit	^(12012235\d(3))\$	+\$1	^(120122(35\d(3))\$
Avaya ext (SIP)	^34(\d(3))\$	+12012234\$1	
Avaya ext	^32(\d(3))\$	+12012232\$1	
Cisco ext	^35(\d(3))\$	+12012235\$1	
IP Office 11-digit	^(70100089\d(3))\$	+\$1	^(701000(89\d(3))\$

Test inputs: 89000

Buttons: Add, Delete, Move Up, Move Down, OK, Cancel

6.2. Administer Sites

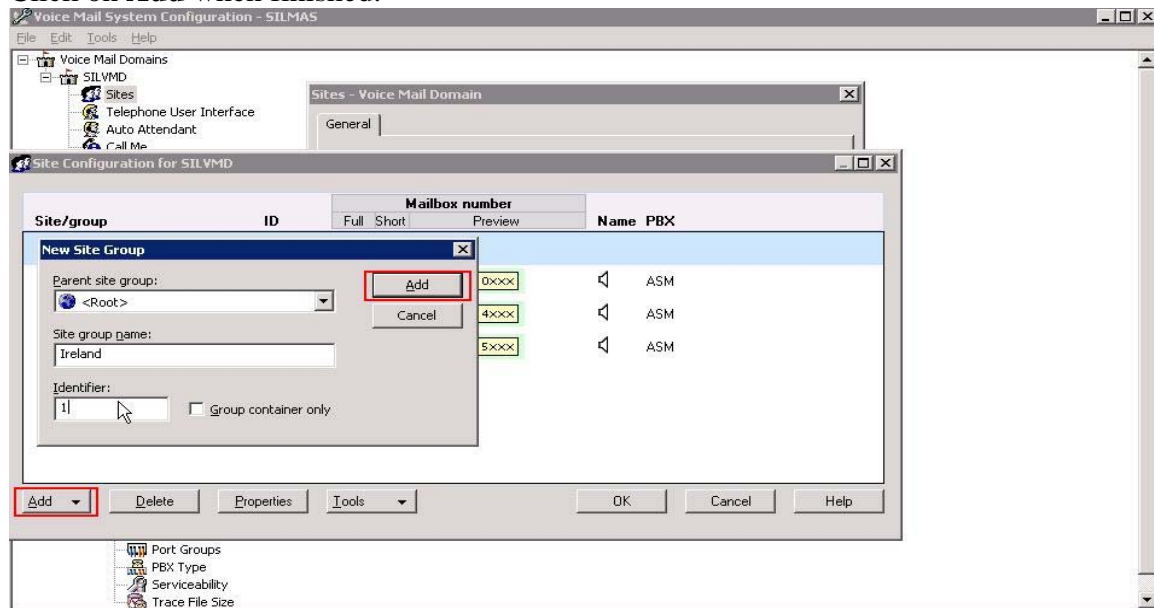
The Communication Manager and IP Office telephone systems must be added as sites in Modular Messaging. This is done by double-clicking **Sites** in the Voice Mail System Configuration tool, as shown below. In the **Sites** window that is displayed, click on **Configure**.



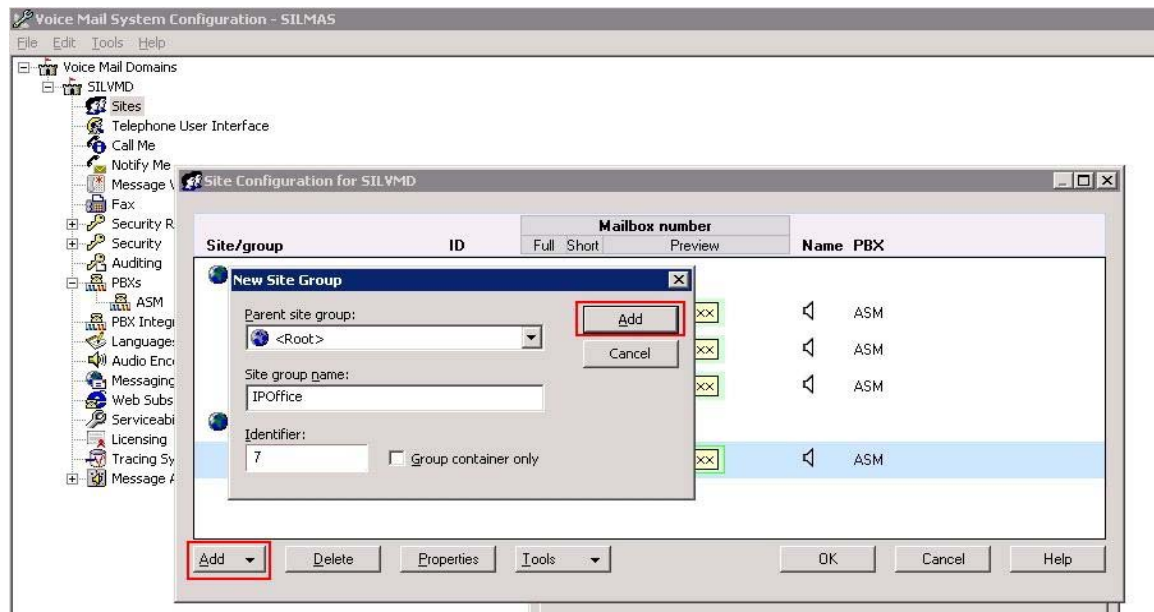
The Site Configuration window is displayed. First create a site group which will be referenced when adding a new site for Communication Manager. Click on **Add** button and select **Group** and enter the following in the **New Site Group** window:

- **Parent site group** Parent site name (default is **Root**)
- **Site group name** Site group name (e.g. **Ireland**)
- **Identifier** A unique number identifying the site group

Click on **Add** when finished.



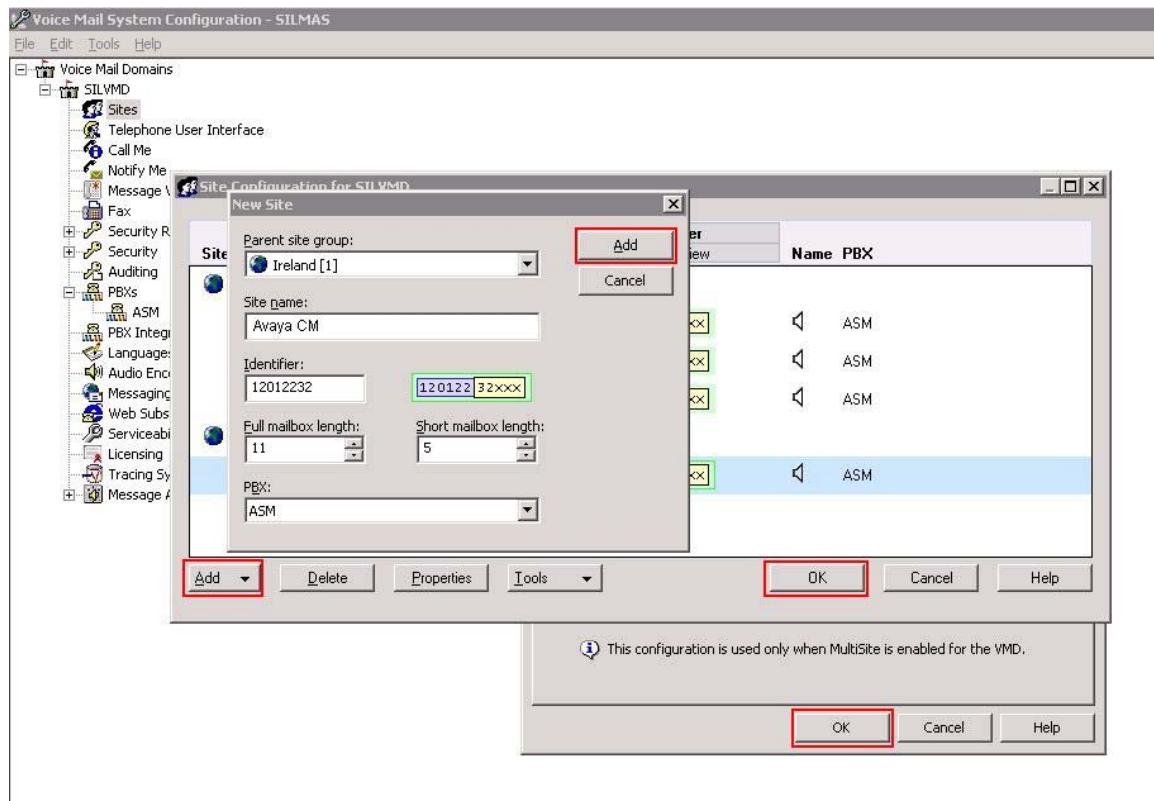
Repeat the above procedure to create a site group which will be referenced when adding a new site for IP Office.

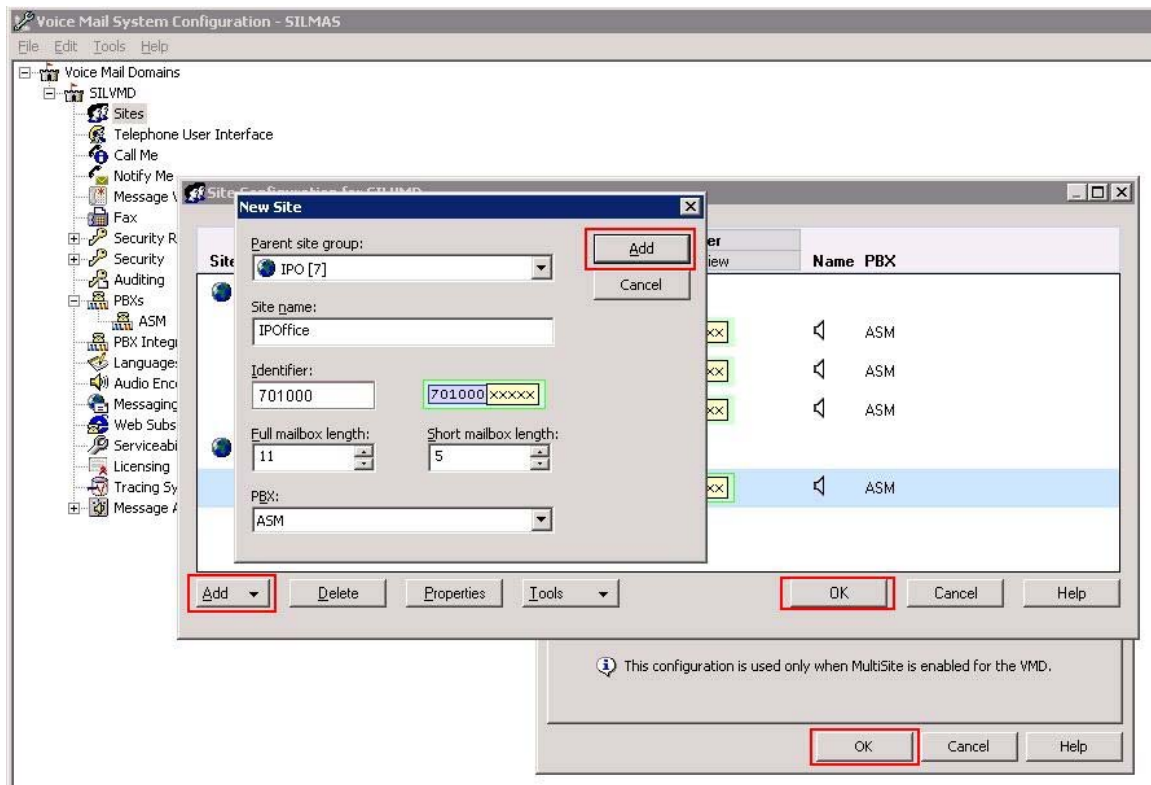


Click on **Add** and select **Site** to add the Communication Manager site, and enter the following in the **New Site** window:

- **Parent site group** Parent site name (e.g., **Ireland**)
- **Site name** Site name
- **Identifier** The unique initial digits of the 11-digit mailbox number, identifying the site
- **Full mailbox length** Enter **11** for the full mailbox number length
- **Short mailbox length** Enter **5** for the extension length
- **PBX** Enter name of the PBX added in the previous **Section 6.1**.

Click on **Add** when finished. The following two screenshots show the adding of the Communication Manager and IP Office sites. When all sites are added, click **OK** in the **Site Configuration** window, and then click on **OK** in the original **Sites** window.





6.3. Administer Subscribers

Log in to the MSS. Select **Messaging Administration → Subscriber Management** from the left pane, to display the **Manage Subscribers** screen. For the **Local Subscriber Mailbox Number** field toward the top of the screen, enter a mailbox number of the subscriber. Click **Add or Edit** box to define more information for the mailbox subscriber.

AVAYA Modular Messaging Messaging Administration This server: 10.10.9.5

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 Configuration
External Hosts
MAS Host Setup
MAS Host Send
Windows Domain Setup
Console Reboot Option
Date/Time/NTP Server
Syslog Server
TCP/IP Service Settings
▼ INAP/SMTP Administration
SMTP Options
Mail Options
INAP/SMTP Status
▼ Server Information
Server Status
Alarm Summary
Server Notes

Manage Subscribers

• Local Subscriber Mailbox Number: 12012232007

	Machine Name	Subscriber Licenses Used	Total Subscribers	Filter	Managed Subscribers
• Local Subscribers	SLMss	5	9	<input type="button" value="Filter"/>	9 <input type="button" value="Manage"/>
• Remote Subscribers	internet		0	<input type="button" value="Filter"/>	0 <input type="button" value="Manage"/>

Page Status:

The **Add Local Subscriber** screen is displayed next. Enter the desired string into the **Last Name, First Name and Password**. In the interoperability testing, the same telephone extensions for the Communication Manager and IP Office subscribers were used for the **Mailbox Number, Numeric Address, and PBX Extension** fields. Scroll down to the bottom of the screen and click **Save** (not shown). Repeat this section to add all subscribers.

AVAYA Modular Messaging Messaging Administration This server: 10.10.9.5

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 Configuration
External Hosts
MAS Host Setup
MAS Host Send
Windows Domain Setup
Console Reboot Option
Date/Time/NTP Server
Syslog Server
TCP/IP Service Settings
▼ INAP/SMTP Administration
SMTP Options
Mail Options
INAP/SMTP Status
▼ Server Information
Server Status
Alarm Summary
Server Notes

Add Local Subscriber

BASIC INFORMATION * (Required Fields)

*Last Name	phelan	First Name	tom
*Password	****	*Mailbox Number	12012232007
*Numeric Address	12012232007	PBX Extension	12012232007
*Class Of Service	0 - class00	*Community ID	1

7. Verification

This section provides the tests that can be performed on Communication Manager, Session Manager, Modular Messaging and IP Office to verify their proper configuration.

7.1. Verify Avaya Aura™ Communication Manager

Verify the status of the SIP trunk group by using the **status trunk n** command, where **n** is the trunk group number being investigated. Verify that all trunks are in the **in-service/idle** state as shown below.

```
status trunk 150

                                TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                Busy

0150/001 T00036    in-service/idle    no
0150/002 T00037    in-service/idle    no
0150/003 T00038    in-service/idle    no
0150/004 T00039    in-service/idle    no
0150/005 T00040    in-service/idle    no
0150/006 T00041    in-service/idle    no
0150/007 T00042    in-service/idle    no
0150/008 T00043    in-service/idle    no
0150/009 T00044    in-service/idle    no
0150/010 T00045    in-service/idle    no
```

Verify the status of the SIP signaling-group by using the **status signaling-group n** command, where **n** is the signaling group number being investigated. Verify that the signaling group is in the **in-service** state as shown below.

```
status signaling-group 150

                                STATUS SIGNALING GROUP

Group ID: 150                      Active NCA-TSC Count: 0
Group Type: sip                     Active CA-TSC Count: 0
Signaling Type: facility associated signaling
Group State: in-service
```

7.2. Verify Avaya Aura™ Session Manager

Select **Session Manager** → **System Status** → **SIP Entity Monitoring**. Verify as shown below that none of the SIP entities for Communication Manager, Modular Messaging or Avaya IP Office links are down, indicating that they are all reachable for routing.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar contains a navigation menu with categories like Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy, Security, Applications, Settings, and Session Manager. The Session Manager section is expanded, showing options like Session Manager Administration, Network Configuration, Device and Location Configuration, Application Configuration, System Status, and SIP Entity Monitoring. The main content area is titled 'SIP Entity Link Monitoring Status Summary' and includes a 'Refresh' button. Below this is a table showing the status of SIP entity links for all Session Manager instances. The table has five columns: Session Manager Name, Entity Links Down/Total, Entity Links Partially Down, SIP Entities - Monitoring Not Started, and SIP Entities - Not Monitored. The data row shows 'SessionManager' with 0/8 entity links down, 0 partially down, 0 monitoring not started, and 0 not monitored. Below the table is a section titled 'All Monitored SIP Entities' with another 'Refresh' button and a list of 8 items. The list includes AvayaCM, AvayaCMtom, Voicemail, IPOffice-Tom, feature, MX-S6200, Stack OCS Mediation Server, and VoiceMail. The SIP entity names AvayaCMtom, Voicemail, and IPOffice-Tom are highlighted with red boxes.

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
SessionManager	0/8	0	0	0

SIP Entity Name
AvayaCM
AvayaCMtom
Voicemail
IPOffice-Tom
feature
MX-S6200
Stack OCS Mediation Server
VoiceMail

Click on the SIP Entity Names AvayaCMtom, IPOffice-Tom and Voicemail shown in the previous screen and verify that the connection status is **Up**, as shown in screenshots below.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a 'Refresh' button and a 'Summary View' button. Below this is a section titled 'All Entity Links to SIP Entity: AvayaCMtom'. The table shows the connection status for all entity links from all Session Manager instances to a single SIP entity. The table has eight columns: Details, Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The data row shows 'SessionManager' with a resolved IP of 135.64.186.6, port 5063, TCP protocol, and a connection status of 'Up'. The 'Link Status' is also 'Up'. The 'Conn. Status' and 'Link Status' are highlighted with red boxes.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SessionManager	135.64.186.6	5063	TCP	Up	200 OK	Up

Voicemail SIP Entity:

Home / Session Manager / System Status / SIP Entity Monitoring / SIP Entity Link Status

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: **Voicemail**

[Refresh](#) [Summary View](#)

1 Item Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SessionManager	10.10.9.6	5060	TCP	Up	200 OK	Up

IPOffice-Tom SIP Entity:

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at July 15, 2010 4:11 PM [Help](#) [Log off](#)

Home / Session Manager / System Status / SIP Entity Monitoring / SIP Entity Link Status

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: **IPOffice-Tom**

[Refresh](#) [Summary View](#)

1 Item Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SessionManager	10.10.9.100	5060	TCP	Up	200 OK	Up

7.3. Verify Avaya IP Office

IP Office can be debugged with the System Status Application. Log in to the IP Office Manager PC and select **Start → Programs → IP Office → System Status** to launch the application. Log into the application using the appropriate credentials. In the left panel, click on the **Trunks** entry and select the SIP trunk created in **Section 5.6**. Press the **Trace All** button (not shown). The messages on the line are displayed.

AVAYA

IP Office System Status

Help Snapshot LogOff Exit About

System

Alarms (27)

Extensions (11)

Trunks (6)

Line: 1

Line: 2

Line: 3

Line: 17

Line: 18

Line: 19

Active Calls

Resources

Voicemail

IP Networking

Status Utilization Summary Alarms

SIP Trunk Summary

Peer Domain Name: s1stack.com

Gateway Address: 135.64.186.40

Line Number: 19

Number of Administered Channels: 10

Number of Channels in Use: 0

Administered Compression: Auto

Silence Suppression: Off

SIP Trunk Channel Licences: Unlimited

SIP Trunk Channel Licences in Use: 0

SIP Device Features:

Channel Number

URI

Call Gro. Ref

Current State

Time in State

Remote RTP Address

Codec

Connection Type

Caller ID or Dialed Digits

Other Party on Call

Direction of Call

Round Trip Delay

Receive Jitter

Receive Pack Loss Fraction

Transmit Jitter

Transmit Pack Loss Fraction

1			Idle	4 days 00:...										
2			Idle	5 days 01:...										
3			Idle	5 days 02:...										
4			Idle	5 days 20:...										

Trace Output - All Channels:

Trace Clear

Pause

Ping

Call Details

Print...

Save As...

7.4. Verify Avaya Modular Messaging

Make a call from a Communication Manager subscriber to an IP Office subscriber and verify that the call covers to Modular Messaging upon no answer. Leave a voice message for the IP Office subscriber. From the IP Office subscriber, dial the Modular Messaging pilot number to retrieve the message. Verify that the Modular Messaging system identifies the IP Office subscriber as a local subscriber, and that the voice message can be retrieved. Log in to the MSS web interface and **select Logs → Subscriber Activity** from the left pane. Enter the **mailbox number** of the IP Office subscriber (70100089000), enter the appropriate **start date** and **end date** for the above activities, and click **Display**. Verify that a listing of the detailed activities is displayed into the bottom portion of the right hand pane. Verify that there is an entry showing the message left by the Communication Manager subscriber (in this case 12012232007). Also verify that there is an entry showing the message being retrieved.

AVAYA

Help Log Off

Shutdown Server
Reboot Server

▼ Logs

Administration History
Alarm
Backup
ELA Delivery Failures
IMAP/SMTP
Messaging Start-up
MSS DCT Configuration Log
Restore
Server Events
Software Management
Subscriber Activity
Web Server

▼ Reports

IMAP/SMTP Traffic
Messaging Measurements
System Evaluation
TCP/IP Packet Statistics

▼ Diagnostics

Alarm Origination
LDAP Connection
SMTP Connection
POP3 Connection
IMAP4 Connection
Mail Delivery
Ping Another Server
Name Server Lookup

▼ Software Management

Messaging Software Display
Server Software Display
Software Installation
Software Verification
Software Removal
Software Update

▼ Security

Change My Password
Password Rules
Administrative Roles
Local Administrators

Subscriber Activity Log

Mailbox Number: 70100089000

Start Date: January 15, 2010 15:10

End Date: January 15, 2010 15:29

Display Help

Name: Carey, DJ Mailbox Number: 12012235000

Date	Time	Activity	Description
01/15/2010	15:12	received	CA message from 12012232007 new=1(v=1 f=0 e=0 dsn=0) un=0 o=1 d=0 x=0
01/15/2010	15:12	inbox-stat	id=bdf48 port=55143 IP=172.20.10.4 new=1(v=1 f=0 e=0 dsn=0) un=0 o=1 d=0 x=0
01/15/2010	15:12	inbox-sel	id=bdf48 port=55143 IP=172.20.10.4 msgs=2
01/15/2010	15:12	status	changed from new to deleted for message received 1/15/10 at 15:12
01/15/2010	15:12	inbox-stat	id=bdf48 port=55143 IP=172.20.10.4 new=0(v=0 f=0 e=0 dsn=0) un=0 o=1 d=1 x=0
01/15/2010	15:12	status	changed from deleted to removed for message received 1/15/10 at 15:12
01/15/2010	15:12	inbox-dsel	id=bdf48 port=55143 IP=172.20.10.4 msgs=1
01/15/2010	15:20	received	CA message from 12012232007 new=1(v=1 f=0 e=0 dsn=0) un=0 o=1 d=0 x=0
01/15/2010	15:21	inbox-stat	id=bdf4e port=55143 IP=172.20.10.4 new=1(v=1 f=0 e=0 dsn=0) un=0 o=1 d=0 x=0
01/15/2010	15:21	inbox-sel	id=bdf4e port=55143 IP=172.20.10.4 msgs=2
01/15/2010	15:21	status	changed from new to old for message received 1/15/10 at 15:20
01/15/2010	15:21	inbox-stat	id=bdf4e port=55143 IP=172.20.10.4 new=0(v=0 f=0 e=0 dsn=0) un=0 o=2 d=0 x=0
01/15/2010	15:21	inbox-dsel	id=bdf4e port=55143 IP=172.20.10.4 msgs=2

7.5. Verified Scenarios

The verification scenarios for the configuration described in these Application Notes included the following:

- The IP Office subscribers were properly recognized by Modular Messaging upon dialing the Modular Messaging pilot number, and that the IP Office subscribers can log in without entering the mailbox number.
- The IP Office subscribers were properly identified by Modular Messaging as the calling party for voice messages left for other subscribers.
- Modular Messaging turns the message waiting indicator ON and OFF appropriately for voice messages left and retrieved for the IP Office subscribers.
- Modular Messaging appropriately identifies the original dialed endpoint as the called party for scenarios with Multiple Call Forwarding, where a called party has calls forwarded to another party that covers to Modular Messaging upon no answer.

8. Conclusion

As illustrated in these Application Notes, Avaya Aura™ Communication Manager can interoperate with Avaya IP Office using SIP trunks via Avaya Aura™ Session Manager. The following is a list of interoperability items observed:

- Find Me feature does not work properly if the Find Me subscriber and the Find Me destination subscriber are on different PBX's
- Fax sending to Avaya IP Office subscribers does not work properly

9. Additional References

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

- [1] *Avaya AuraTM Session Manager Overview*, Doc # 03-603323, Issue 2
- [2] *Administering Avaya AuraTM Session Manager*, Doc # 03-603324, Issue 2
- [3] *Maintaining and Troubleshooting Avaya AuraTM Session Manager*, Doc # 03-603325, Issue 2
- [4] *SIP Support in Avaya AuraTM Communication Manager Running on Avaya S8xxx Servers*, Doc # 555-245-206, Issue 9
- [5] *Administering Avaya AuraTM Communication Manager*, Doc # 03-300509, Issue 5.0
- [6] *Modular Messaging Admin Guide Release 5.2 with Avaya MSS*
- [7] *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.2 Installation and Upgrades*
- [8] *Avaya S8300/S85x0/S84x0/S87x0 SIP Integration using Avaya Session Manager*
- [9] *Avaya IP Office Manager*, Doc # 15-601011, Issue 24k

©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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com