



Avaya Solution Interoperability Test Lab

Configuring SIP Trunks among Avaya Business Communication Manager 5.0, Avaya Aura™ Session Manager 5.2, and Avaya Modular Messaging 5.2– Issue 1.0

Abstract

These Application Notes describe a sample configuration of a network that uses SIP trunks between Avaya Business Communication Manager Release 5.0, Avaya Aura™ Session Manager Release 5.2, Avaya Modular Messaging 5.2, Avaya Aura™ Communication Manager Access Element Release 5.2.1, and a second Avaya Aura™ Communication Manager operating as a Feature Server.

- Avaya Aura™ Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura™ Communication Manager operates as an Access Element to support H.323, DCP and analog phones. The second Avaya Aura™ Communication Manager operates as a Feature Server for the SIP endpoints which communicates with Avaya Aura™ Session Manager over SIP trunks.
- Avaya Business Communication Manager 5.0 is an all-in-one platform supporting converged voice and data communications for small businesses.
- Avaya Modular Messaging 5.2 provides a centralized voice messaging solution for the Avaya Business Communication Manager with SIP integration via Avaya Aura™ Session Manager. Users on all three systems have mailboxes defined on the Avaya Modular Messaging Message Storage Server (MSS) which they can access via a dedicated pilot number.

These Application Notes provide information for the setup, configuration, and verification of the call flows tested on this solution.

Table of Contents

1.	Introduction	5
2.	Equipment and Software Validated	7
3.	Configure Avaya Aura™ Communication Manager	7
3.1.	Verify System Capabilities and Licensing	8
3.1.1.	Verify SIP Trunk Capacity	8
3.1.2.	Verify AAR/ARS Routing	8
3.1.3.	Verify Private Networking and Uniform Dialing Plan.....	9
3.1.4.	Configure Trunk-to-Trunk Transfers	9
3.2.	Configure IP Codec Type	10
3.3.	Set IP Network Region	11
3.4.	Add Node Names and IP Addresses	11
3.5.	Configure SIP Signaling Group and Trunk Group.....	12
3.5.1.	Add Signaling Group for SIP Trunk	12
3.5.2.	Add SIP Trunk Group	13
3.6.	Configure Route Patterns	15
3.7.	Administer Numbering Plan	15
3.7.1.	Administer Uniform Dialplan	15
3.7.2.	Administer AAR analysis	16
3.7.3.	Administer Locations	16
3.8.	Administer Coverage to Avaya Modular Messaging	17
3.8.1.	Administer Hunt Group	17
3.8.2.	Administer Coverage Path.....	18
3.8.3.	Administer Station for Coverage to Avaya Modular Messaging.....	19
3.9.	Save Translations.....	20
4.	Configure Avaya Aura™ Session Manager	20
4.1.	Administer SIP Domains.....	22
4.2.	Define Locations	23
4.3.	Specify Listen Port for UDP Connections	24
4.4.	Add Avaya Business Communication Manager.....	25
4.4.1.	Define SIP Entity	25
4.4.2.	Define Entity Links.....	26
4.4.3.	Define Routing Policy	27
4.4.4.	Define Dial Pattern	28

4.5. Add Avaya Modular Messaging	29
4.5.1. Define SIP Entity and Entity Link.....	29
4.5.2. Define Routing Policy	30
4.5.3. Define Dial Pattern	31
5. Configure Avaya Business Communication Manager.....	32
5.1. Run Element Manager Application and Login.....	32
5.2. Add SIP Trunk to Avaya Aura™ Session Manager.....	34
5.2.1. Configure Routing for SIP Trunks.....	35
5.2.2. Configure IP Trunk Settings	36
5.2.3. Configure SIP Settings	36
5.2.4. Configure SIP Media Parameters.....	37
5.3. Define Business Name	38
5.4. Configure Dialing Plan	39
5.4.1. Configure SIP Line Pool	39
5.4.2. Configure Public Network	40
5.4.3. Configure Routing	41
5.4.4. Configure Destination Code	42
5.5. Configure Dialing Plan for Avaya Modular Messaging.....	43
5.6. Configure Stations for Coverage to Avaya Modular Messaging	44
6. Configure Avaya Modular Messaging	45
6.1. Verify Multi-Site Configuration	45
6.2. Configure TCP Port	46
6.3. Administer Avaya Aura™ Session Manager as PBX	47
6.4. Administer Sites.....	50
6.5. Administer Subscribers.....	52
6.6. Configure Message Waiting Indication	53
7. Verification Steps.....	54
7.1. Verify Avaya Aura™ Session Manager Configuration.....	54
7.1.1. Verify Avaya Aura™ Session Manager is Operational	54
7.1.2. Verify SIP Link Status.....	56
7.1.3. Verify Registrations of SIP Endpoints.....	57
7.2. Verify Avaya Business Communication Manager Configuration	58
7.3. Verify Avaya Aura™ Communication Manager Feature Server.....	59
7.4. Verify Status of Avaya Modular Messaging	61

7.5. Call Scenarios Verified	62
7.6. Issues Found and Known Limitations	63
8. Conclusions	63
9. Acronyms.....	64
10. Additional References	65

1. Introduction

These Application Notes describe a sample configuration of a network that uses SIP trunks between Avaya Business Communication Manager Release 5.0, Avaya Aura™ Session Manager Release 5.2, Avaya Modular Messaging 5.2, Avaya Aura™ Communication Manager Access Element Release 5.2.1, and a second Avaya Aura™ Communication Manager operating as a Feature Server.

As shown in **Figure 1**, the Avaya Business Communication Manager Release 5.0 runs on the Business Communication Manager 50 platform and supports the 1230 IP and T7316E digital phones. Business Communication Manager is connected over a SIP trunk to Avaya Aura™ Session Manager, using the SM-100 (Security Module) network interface on the Session Manager.

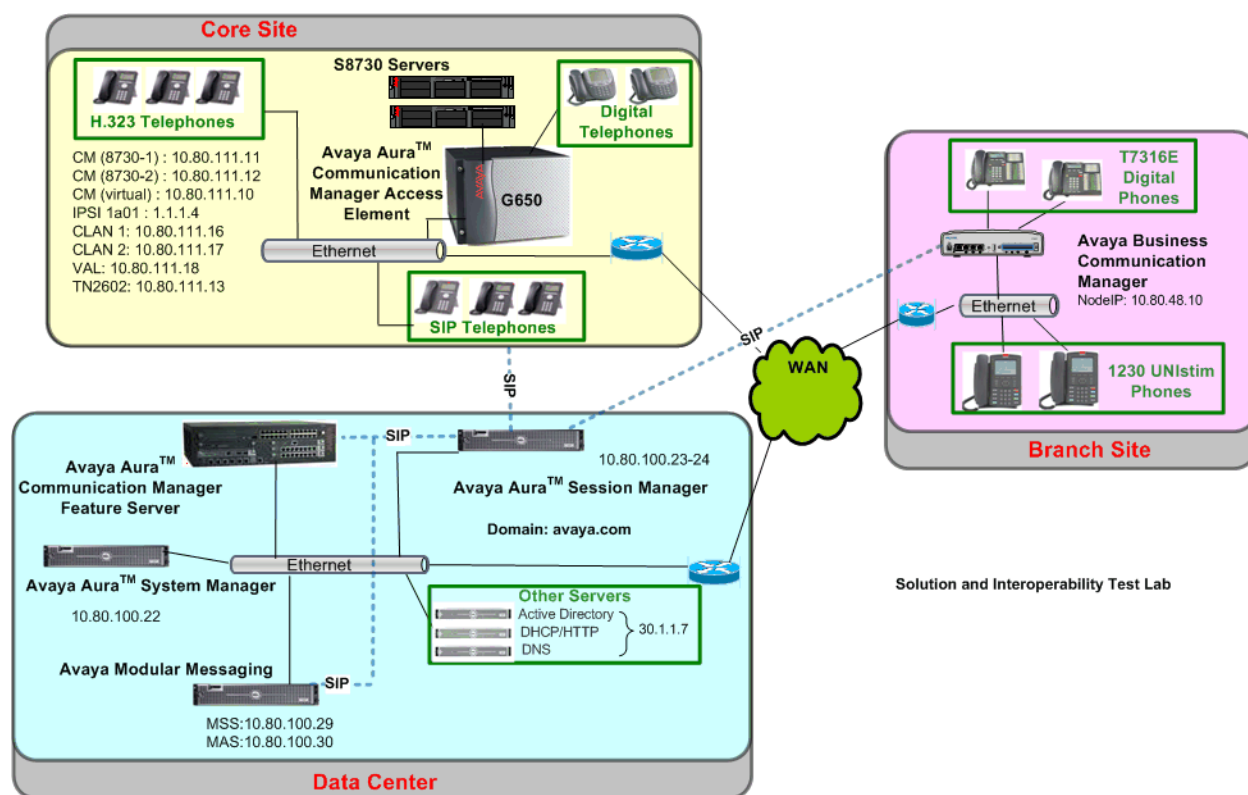


Figure 1 – Sample Configuration

Avaya Aura™ Communication Manager Access Element supports Avaya 9600 Series IP Telephone (H.323) and 2420 Digital Telephone and is also connected over a SIP trunk to Session Manager.

Avaya 9630 IP Telephones configured as SIP endpoints utilize the Session Manager User Registration feature and require an Avaya Aura™ Communication Manager operating as a Feature Server. Communication Manager Feature Server only supports IMS-SIP users that are

registered to Session Manager. The Communication Manager Feature Server is connected to Session Manager via an IMS-enabled SIP signaling group and associated SIP trunk group.

Avaya Modular Messaging Release 5.2 consists of Avaya Messaging Application Server (MAS) and Avaya Message Storage Server (MSS) running on a single server. Avaya Modular Messaging is connected over a SIP trunk to Session Manager.

All inter-system calls are carried over these SIP trunks

Session Manager is managed by Avaya Aura™ System Manager. For the sample configuration, System Manager and Session Manager run on separate Avaya S8510 Servers. Communication Manager Access Element runs on a pair of duplicated Avaya S8730 Servers with an Avaya G650 Media Gateway.

The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Communication Manager.

These Application Notes will focus on the configuration of the SIP trunks and call routing needed to test calls between Avaya Business Communication Manager, Communication Manager Access Element, Avaya Modular Messaging or SIP stations registered to Session Manager. Detailed administration of Communication Manager Feature Server, SIP endpoints, or SIP users will not be described (see the appropriate documentation listed in **Section 10**).

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Component	Software Version
Avaya Aura™ Session Manager on Avaya S8510 server	Release 5.2.1.1.521012-01-14-2010
Avaya Aura™ System Manager	Release 5.2, Load: 5.2.0.8.27
Avaya Aura™ Communication Manager Access Element <ul style="list-style-type: none">• Duplicated Avaya S8730 Servers• Avaya G650 Media Gateway	Release 5.2.1, SP1 Load: R015x.02.1.016.4-17959
Avaya Aura™ Communication Manager Feature Server <ul style="list-style-type: none">• Avaya S8300 Server	Release 5.2.1, SP1 Load: R015x.02.1.016.4-17959
Avaya IP Telephones: <ul style="list-style-type: none">• 4621SW• 9620	FW: 2.90 FW:3.0
Avaya SIP Phones <ul style="list-style-type: none">• 9630	FW: 2.5.0
Avaya Digital Telephones (2420D)	N/A
Avaya Business Communication Manager <ul style="list-style-type: none">• Avaya Business Communication Manager 50 platform	Release 5 Version: 9.0.1.22.524 Update: BCM050.R500.SU.System-004.201004-1
• 1230 IP Telephone	FW: 062AC6R
• T7316E Digital Telephone	N/A
Avaya Modular Messaging	Release 5.2

3. Configure Avaya Aura™ Communication Manager

This section describes the necessary configuration in Communication Manager for routing calls to Avaya Business Communication Manager or for coverage to Avaya Modular Messaging. This configuration applies to either the Access Element or Feature Server. For information on how to administer other aspects of Communication Manager Access Element or Feature Server, please see references in **Section 10**.

This section describes the administration of Communication Manager using a System Access Terminal (SAT). Some administration screens have been abbreviated for clarity.

The following administration actions are described:

- Verify System Capabilities and Communication Manager Licensing
- Administer IP Codec Set
- Administer IP Network Region
- Administer IP Node Names

- Administer SIP Trunk group and associated Signaling Group
- Administer Route Pattern
- Administer Numbering Plan
- Administer Locations
- Administer Hunt Group
- Administer Coverage Path
- Administer a station for coverage to Modular Messaging

After completing these steps, the **save translation** command should be performed.

3.1. Verify System Capabilities and Licensing

This section describes the procedures to verify the correct system capabilities and licenses have been configured. If there is insufficient capacity or a required features is not available, contact an authorized Avaya sales representative to make the appropriate changes.

3.1.1. Verify SIP Trunk Capacity

Issue the **display system-parameters customer-options** command to verify that an adequate number of SIP trunk members are administered for the system as shown below:

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES			USED	
Maximum Administered H.323 Trunks:			500	0
Maximum Concurrently Registered IP Stations:			18000	4
Maximum Administered Remote Office Trunks:			0	0
Maximum Concurrently Registered Remote Office Stations:			0	0
Maximum Concurrently Registered IP eCons:			0	0
Max Concur Registered Unauthenticated H.323 Stations:			100	0
Maximum Video Capable Stations:			0	0
Maximum Video Capable IP Softphones:			0	0
Maximum Administered SIP Trunks:			50	20

3.1.2. Verify AAR/ARS Routing

To simplify the dialing plan for calling stations on the Business Communication Manager, verify that the **ARS**, **ARS/AAR Partitioning** and **ARS/AAR Dialing without FAC** parameters are enabled on **Page 3** of **system-parameters customer options** command.

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
A/D Grp/Sys List Dialing Start at 01? n		CAS Main? n		
Answer Supervision by Call Classifier? n		Change COR by FAC? n		
ARS? y		Computer Telephony Adjunct Links? y		
ARS/AAR Partitioning? y		Cvg Of Calls Redirected Off-net? y		
ARS/AAR Dialing without FAC? y		DCS (Basic)? y		
ASAI Link Core Capabilities? y		DCS Call Coverage?		

3.1.3. Verify Private Networking and Uniform Dialing Plan

Verify that the **Private Networking** and **Uniform Dialing Plan** parameters are enabled on **Page 5** of **system-parameters customer options** command.

display system-parameters customer-options		Page	5 of	11
OPTIONAL FEATURES				
Multinational Locations? n	Station and Trunk MSP? y			
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? n			
Multiple Locations? y	System Management Data Transfer? n			
Personal Station Access (PSA)? n	Tenant Partitioning? n			
PNC Duplication? y	Terminal Trans. Init. (TTI)? y			
Port Network Support? y	Time of Day Routing? n			
Posted Messages? n	TN2501 VAL Maximum Capacity? y			
	Uniform Dialing Plan? y			
Private Networking? y	Usage Allocation Enhancements? y			
Processor and System MSP? y				
Processor Ethernet? y	Wideband Switching? n			
	Wireless? y			

3.1.4. Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. This feature is needed when a call to Modular Messaging from a Communication Manager station is transferred to Business Communication Manager. 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 by increasing the risk of toll fraud, and must be used with caution. To minimize the risk, a COS could be defined to allow trunk-to-trunk transfers for specific trunk group(s). For more information regarding how to configure Communication Manager to minimize toll fraud, see **Reference [8]** in **Section 10**.

change system-parameters features		Page	1 of	18
FEATURE-RELATED SYSTEM PARAMETERS				
Self Station Display Enabled? n				
Trunk-to-Trunk Transfer: all				
Automatic Callback with Called Party Queuing? n				
Automatic Callback - No Answer Timeout Interval (rings): 3				
...				

3.2. Configure IP Codec Type

Issue the **change ip-codec-set n** command where **n** is the number used to identify the codec set.

Enter the following values:

- **Audio Codecs:** Enter “**G.711MU**” and “**G.729**” as supported types
- **Silence Suppression:** Retain the default value “**n**”.
- **Frames Per Pkt:** “**2**”
- **Packet Size (ms):** “**20**”
- **Media Encryption:** Enter the value based on the system requirement.
For the sample configuration, “**none**” was used.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
	Audio	Silence	Frames	Packet		
	Codec	Suppression	Per Pkt	Size(ms)		
1:	G.711MU	n	2	20		
2:	G.729	n	2	20		
3:						
Media Encryption						
1:	none					

On **Page 2**, verify the **FAX** field is administered to use “**t.38-standard**” as shown below:

change ip-codec-set 1				Page	2 of	2
IP Codec Set						
Allow Direct-IP Multimedia? n						
	Mode					
FAX	t.38-standard	2				
Modem	off	0				
TDD/TTY	off	0				
Clear-channel	n	0				

3.3. Set IP Network Region

Using the **change ip-network-region 1** command, enter the following values:

- **Intra-region IP-IP Direct Audio:** “yes”
- **Inter-region IP-IP Direct Audio:** “yes”
- **Codec Set:** Enter the IP codec set configured in **Section 3.2**.
- **Authoritative Domain** Enter the correct SIP domain for the configuration.
For the sample configuration, “**avaya.com**” was used

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain: avaya.com	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 16585		

3.4. Add Node Names and IP Addresses

Using the **change node-names ip** command, add the node-name and IP Addresses for the CLANs and the SM-100 interface for the Session Manager, if not previously added.

Note: If Communication Manager is running on an Avaya S8300 server, defining a node name for the CLAN is not necessary since “**procr**” will be added as a node name by default.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
8730-1	10.80.111.11	
8730-2	10.80.111.12	
ASM1	10.80.100.24	
CLAN-1	10.80.111.16	
CLAN-2	10.80.111.17	

3.5. Configure SIP Signaling Group and Trunk Group

3.5.1. Add Signaling Group for SIP Trunk

Use the **add signaling-group n** command, where **n** is an available signaling group number to create a SIP signaling group to connect to Session Manager. In the sample configuration, signaling group “10” and trunk group “10” were used to connect to Session Manager.

Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

Note: TCP was used for the sample configuration. However, TLS would be typically used in a production environment.

- **Group Type:** “sip”
- **Transport Method:** “tcp”
- **IMS Enabled:** “n” for Access Element, or “y” for Feature Server
- **Near-end Node Name:** Enter appropriate node name from **Section 3.4**.
- **Far-end Node Name:** Enter Session Manager node name
- **Near-end Listen Port:** “5060”
- **Far-end Listen Port:** “5060”
- **Far-end Domain:** Enter domain name for **Authoritative Domain** defined in **Section 3.3**
- **DTMF over IP:** “rtp-payload”
- **Session Establishment Timer:** “3”

```
add signaling-group 10                                     Page 1 of 1
                                                           SIGNALING GROUP

Group Number: 10                                           Group Type: sip
                                                           Transport Method: tcp

  IMS Enabled? n
    IP Video? n

    Near-end Node Name: CLAN-1                               Far-end Node Name: ASML
    Near-end Listen Port: 5060                               Far-end Listen Port: 5060
                                                           Far-end Network Region:

Far-end Domain: avaya.com

                                                           Bypass If IP Threshold Exceeded? n
    DTMF over IP: rtp-payload                               Direct IP-IP Audio Connections? y
    Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
    Enable Layer 3 Test? n                                  Direct IP-IP Early Media? n
    H.323 Station Outgoing Direct Media? n                 Alternate Route Timer(sec): 6
```

3.5.2. Add SIP Trunk Group

Add the corresponding trunk group controlled the signaling group defined **Section 3.5.1** using the **add trunk-group n** command, where **n** is an available trunk group number.

Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** Enter a descriptive name.
- **TAC:** Enter an available trunk access code.
- **Direction:** “two-way”
- **Service Type:** “tie”
- **Signaling Group:** Enter number of the signaling group added in **Section 3.5.1**
- **Number of Members:** Enter the number of members in the SIP trunk to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in **Section 3.1.1**).

Once the **add trunk-group** command is completed, trunk members will be automatically generated based on the value in the **Number of Members** field.

add trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: SIP trunk to ASM1	COR: 1	TN: 1	TAC: #10
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 10	
		Number of Members: 10	

On **Page 2**, set the **Preferred Minimum Session Refresh Interval** field to “1200”.

Note: to avoid extra SIP messages, all SIP trunks connected to Session Manager should be configured with a minimum value of “1200”.

add trunk-group 10		Page 2 of 21	
		Group Type: sip	
TRUNK PARAMETERS			
Unicode Name: auto			
		Redirect On OPTIM Failure: 5000	
SCCAN? n		Digital Loss Group: 18	
		Preferred Minimum Session Refresh Interval(sec): 1200	

On **Page 3**, fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Numbering Format** “public”
- **Show ANSWERED BY on Display** “y”

add trunk-group 10		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		
UI Treatment: service-provider		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		
Show ANSWERED BY on Display? y		

On **Page 4**, fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Mark Users As Phone** Enter “y” to send correct user information in SIP INVITE messages
- **Support Request History** “y”
- **Telephone Event Payload Type** “120”

add trunk-group 10		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? y		
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. Configure Route Patterns

This provides the configuration of the route pattern used in the sample configuration for routing calls between Communication Manager, Business Communication Manager and Avaya Modular Messaging.

In the sample configuration, a single route pattern was defined to route calls to Session Manager.

Note: Other methods of routing may be used.

Use the **add route-pattern x** command, when **x** is an available route pattern. In the **Grp No** field, enter the SIP trunk group defined in **Section 3.5.1** to route calls to Session Manager.

In the sample configuration, route pattern “10” was created as shown below:

add route-pattern 10										Page 1 of 3	
Pattern Number: 10 Pattern Name: SIP to ASM1											
SCCAN? n Secure SIP? n											
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC			
No			Mrk	Lmt	List	Del	Digits	QSIG			
								Intw			
1:	10	0							n	user	
2:									n	user	
3:									n	user	

3.7. Administer Numbering Plan

3.7.1. Administer Uniform Dialplan

To enable stations on the Communication Manager to call Modular Messaging, an entry for the pilot number to Modular Messaging was added to the uniform dial plan.

Use the **change uniform-dialplan x** command, where **x** is the first digit of the pilot number.

In the sample configuration, the pilot number for Modular Messaging for extensions on Communication Manager was “666-5000”.

change uniform-dialplan 6							Page 1 of 2		
UNIFORM DIAL PLAN TABLE									
							Percent Full: 0		
Matching				Insert		Node			
Pattern	Len	Del		Digits	Net	Conv	Num		
6663	7	0			aar	n			
6665000	7	0			aar	n			
777	7	0			aar	n			
778	7	0			aar	n			

3.7.2. Administer AAR analysis

This section provides the configuration of the AAR pattern used in the sample configuration for routing calls between Communication Manager and Business Communication Manager.

Note: Depending on the customer network, other methods of routing may be used.

Use the **change aar analysis x** command where **x** is the first digit of the number used to route calls to stations on Business Communication Manager.

In the **Dialed String** field, enter the prefix for dialing stations on Business Communication Manager or the pilot number for Modular Messaging. Enter the appropriate number of digits in the **Total Min** and **Total Max** fields.

In the sample configuration, all calls starting with “**333**” will be routed to Business Communication Manager using Route Pattern “**10**”. Calls to the pilot number for Modular Messaging will also use route Pattern “**10**”.

change aar analysis 3							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 2
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd	
333	6	6	10	aar		n	
522	7	7	10	aar		n	
555	7	7	10	aar		n	
6663	7	7	10	aar		n	
6664	7	7	10	aar		n	
6665000	7	7	10	aar		n	

3.7.3. Administer Locations

This section provides the configuration of the Locations screen. Configuring a default route is necessary to enable stations on Communication Manager to use Modular Messaging features such as Call Sender or Auto-Attendant to place or transfer calls to stations on Business Communication Manager.

Use the **change locations** command to identify a default proxy route. Set the **Proxy Rte** field to use the Route Pattern defined in **Section 3.6**.

change locations										Page 1 of 16
LOCATIONS										
ARS Prefix 1 Required For 10-Digit NANP Calls? y										
Loc No	Name	Timezone Offset	Rule	NPA	ARS FAC	Atd FAC	Disp Parm	Prefix	Proxy Rte	Sel Pat
1:	Main	+ 00:00	0				1		10	
2:			:							
3:			:							

3.8. Administer Coverage to Avaya Modular Messaging

3.8.1. 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 x** command, where **x** is an available hunt-group number. Fill in the indicated fields as shown below. Default values can be used for the remaining fields.

- **Group Name** Enter a descriptive name
- **Group Extension** Enter an available extension number
- **Group Type** “ucd-mia”

In the sample configuration, hunt-group “3” was defined as shown below:

add hunt-group 3	Page 1 of 60
HUNT GROUP	
Group Number: 3	ACD? n
Group Name: SIP coverage to MM	Queue? n
Group Extension: 666-4996	Vector? n
Group Type: ucd-mia	Coverage Path:
TN: 1	Night Service Destination:
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display: grp-name	

On **Page 2**, fill in the indicated fields as shown below.

- **Message Center** “sip-adjunct”
- **Voice Mail Number** Enter the pilot number for the Modular Messaging
- **Voice Mail Handle** Enter the pilot number for the Modular Messaging
- **Routing Digits** Leave field blank since the **ARS/AAR Dialing without FAC** parameter was enabled in **Section 3.1.2**.

Note: Since the values of the **Voice Mail Number** and **Voice Mail Handle** fields will be used in the SIP INVITE message and not the values defined for the **Group Extension** field on **Page 1**, the values defined on this page do not need to be the same number used for the **Group Extension** field.

add hunt-group 3	Page 2 of 60	
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits (e.g., AAR/ARS Access Code)
6665000	6665000	

3.8.2. Administer Coverage Path

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 coverage path x** command, where **x** is an available coverage path. Configure a coverage point, using **“hx”** where **x** is the hunt group number defined in **Section 3.8.1**. Default values can be used for the remaining fields.

In sample configuration, coverage path **“3”** was defined as shown below:

add coverage path 3			Page 1 of 1
COVERAGE PATH			
Coverage Path Number: 3			
Cvg Enabled for VDN Route-To Party? n		Hunt after Coverage? n	
Next Path Number:		Linkage	
COVERAGE CRITERIA			
Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 2
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: h3	Rng: 2	Point2:	
Point3:		Point4:	

3.8.3. Administer Station for Coverage to Avaya Modular Messaging

Configure all phones that are Modular Messaging subscribers to enable coverage to Modular Messaging.

Use the **change station xyz** command, where **xyz** is an existing station number.

On **Page 1**, enter the coverage path defined in **Section 3.8.2** as the value for **Coverage Path 1** field. Verify the extension number defined for the **Message Lamp Ext** field matches the extension number for the station.

In the example below station **“666-4003”** is being configured to cover to Modular Messaging.

change station 6664003		Page 1 of 5
STATION		
Extension: 666-4003	Lock Messages? n	BCC: 0
Type: 9620	Security Code: 123456	TN: 1
Port: S00009	Coverage Path 1: 3	COR: 1
Name: 9620H323	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 666-4003	

On **Page 2**, set **MWI Served User Type** field to **“sip-adjunct”**.

change station 6664003		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number? y	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced		
MWI Served User Type: sip-adjunct	Display Client Redirection? n	
	Select Last Used Appearance? n	
	Coverage After Forwarding? s	

On **Page 4**, if the station has a dedicated **Message** button, use the **Voice Mail Number** defined on **Page 2** of the **hunt-group** form in **Section 3.8.1** to program the button on the station and enable users to directly dial the Modular Messaging system.

change station 6664003	Page 4 of 5
STATION	
...	
BUTTON ASSIGNMENTS	
1: call-appr	4: conf-dsp
2: call-appr	5: fe-mute
3: call-appr	6: call-fwd Ext:
voice-mail Number: 6665000	

3.9. Save Translations

Configuration of Communication Manager is complete. Use the **save translation** command to save these changes.

4. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager to route calls between Business Communication Manager, Avaya Modular Messaging and Communication Manager Access Element or Communication Manager Feature Server.

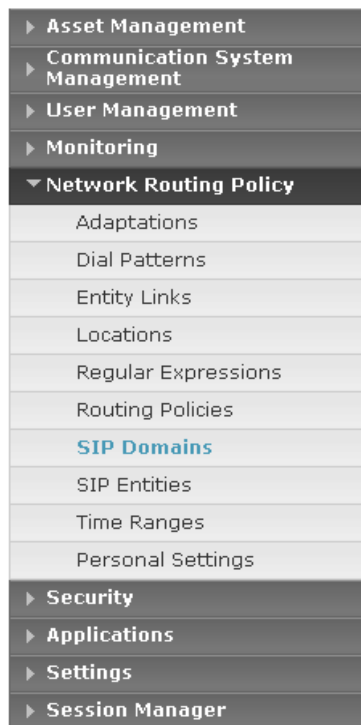
These instructions assume Session Manager has already been configured with the appropriate network connection to System Manager. In addition, other administration activities will be needed such as defining the SIP Entities and associated Entity Links, Routing Policy and Dial Patterns for Communication Manager Access Element and Communication Manager Feature Server and defining the SIP endpoints that will be registered to Session Manager. For more information on these additional administration actions, see the appropriate documentation in **Section 10**.

The following administration activities will be described:

- Administer SIP domain
- Define Logical/physical Locations where SIP Entities will be located
- Specify the Listen Port on Session Manager for UDP connections
- For Business Communication Manager and Modular Messaging,
 - Define SIP Entity
 - Define Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
 - Define Routing Policies, which control call routing between the SIP Entities
 - Define Dial Patterns

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “http://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and accept the Copyright Notice.

Expand the **Network Routing Policy** Link in the Navigation Menu on the left side of the page. Select a specific item such as SIP Domains. When the specific item is selected, the color of the item will change to blue as shown below:



4.1. Administer SIP Domains

Expand **Network Routing Policy** and select **SIP Domains**.

Click **New**. In the *General* Section (Not Shown), enter the following values.

- **Name** Enter the Authoritative Domain Name specified in **Section 3.3**.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.

The screen below shows the resulting domain specified for the sample configuration.

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top header includes the Avaya logo, the product name "Avaya Aura™ System Manager 5.2", and a user status bar indicating "Welcome, admin" and "Last Logged on at Jan. 22, 2010 4:05 PM". A navigation sidebar on the left lists various management categories, with "Network Routing Policy" expanded to show "SIP Domains". The main content area, titled "Domain Management", features action buttons (Edit, New, Duplicate, Delete, More Actions) and a table listing the configured domains. One domain, "avaya.com", is listed with type "sip" and a note "Authoritative Domain defined in CM".

	Name	Type	Default	Notes
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	Authoritative Domain defined in CM

Select : All, None (0 of 1 Selected)

4.2. Define Locations

Expand **Network Routing Policy** and select **Locations**. Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Click **New**. In the *General* Section, enter the following values.

- **Name** Enter a descriptive name.
- **Notes** Enter a brief description. [Optional]

In the *Location Pattern* Section, enter the following value.

- **IP Address Pattern** Enter pattern used to logically identify the location

Click **Commit** to save.

The screen below shows the information for Communication Manager Access Element in the sample configuration.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 22, 2010 4:05 PM Help | Log off

Home / Network Routing Policy / Locations / Location Details

Location Details Commit Cancel

General

* Name:

Notes:

Managed Bandwidth:

* Average Bandwidth per Call: Kbit/sec

* Time to Live (secs):

Location Pattern

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* <input type="text" value="10.80.111.*"/>	<input type="text" value="CM Access Element"/>

Select : All, None (0 of 1 Selected)

* Input Required Commit Cancel

Repeat the above steps to define **Locations** for other SIP Entities.

4.3. Specify Listen Port for UDP Connections

Since the Business Communication Manager only supports UDP connections, configure a listen port on Session Manager for UDP connections.

Expand **Network Routing Policy** and select **SIP Entities**

Select Session Manager and Click **Edit**

- In the *Port* Section, Click **Add**
- **Port** Enter: “**5060**”
Note: Session Manager is able to use the same port for both TCP and UDP connections.
- **Protocol** Select “**UDP**” from the drop-down menu
- **Default Domain** Select the domain name defined in **Section 4.1** from the drop-down menu.
Note: the default domain for the listen port must be configured to use the domain name defined in **Section 4.1**.
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save. The screen below shows the addition of using **Port 5060** as the listen port for UDP connections:

Port

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	to Nortel CS 1000e
<input type="checkbox"/>	5060	UDP	avaya.com	to Business Communication Ma
<input type="checkbox"/>	5061	TLS	avaya.com	

Select : All, None (0 of 3 Selected)

*** Input Required**

4.4. Add Avaya Business Communication Manager

The following section captures relevant screens for configuring the SIP Entity associated with the Avaya Business Communication Manager applicable for the sample configuration.

4.4.1. Define SIP Entity

Expand **Network Routing Policy** and select **SIP Entities**

Click **New**. In the *General* Section, enter the following values.

- **Name** Enter an identifier for Business Communication Manager.
- **FQDN or IP Address** Enter the IP address for Business Communication Manager
- **Type** Select “**Other**” from drop-down menu.
- **Notes** Enter a brief description. [Optional]
- **Location:** Select the “**Location**” added in **Section 4.2** from the drop-down menu.

Note: **Location** is not a required field. Select a location if location-based routing will be used. Since location-based routing was not used in the sample configuration, the **Location** field was left blank.

Click **Commit** to save. The following screen shows addition of Business Communication Manager. The **IP Address** used is the IP address of the Business Communication Manager server.

The screenshot displays the Avaya Aura™ System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name, and a user status message: "Welcome, admin Last Logged on at Jan. 14, 2010 4:44 PM". A breadcrumb trail shows the path: Home / Network Routing Policy / SIP Entities / SIP Entity Details. On the left, a sidebar menu lists various management categories, with "Network Routing Policy" expanded to show "SIP Entities". The main content area is titled "SIP Entity Details" and contains a "General" tab. The form fields are as follows: "Name" (BCM-50), "FQDN or IP Address" (10.80.48.10), "Type" (Other), "Notes" (BCM-50 in branch site), "Adaptation" (empty), "Location" (empty), "Time Zone" (America/Denver), "Override Port & Transport with DNS SRV" (unchecked), "SIP Timer B/F (in seconds)" (4), "Credential name" (empty), "Call Detail Recording" (none), and "SIP Link Monitoring" (Use Session Manager Configuration). Below the form is an "Entity Links" section with "Add" and "Remove" buttons. At the bottom, there is a table with columns for "SIP Entity 1", "Protocol", "Port", "SIP Entity 2", and "Port", with a "Filter: Enable" option. The table currently shows 0 items. "Commit" and "Cancel" buttons are located at the top right and bottom right of the form area.

AVAYA Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Jan. 14, 2010 4:44 PM Help | Log off

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

SIP Entity Details

General

* Name: BCM-50 *

* FQDN or IP Address: 10.80.48.10

Type: Other

Notes: BCM-50 in branch site

Adaptation:

Location:

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

0 Items Refresh Filter: Enable

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
--------------	----------	------	--------------	------	---------

* Input Required

Commit Cancel

4.4.2. Define Entity Links

Expand **Network Routing Policy** and select **Entity Link**

Click **New**. Enter the following values.

- **Name** Enter an identifier for the link to Business Communication Manager
- **SIP Entity 1** Select Session Manager from the drop-down menu
Note: Session Manager in sample configuration is “**ASM1-DR**”
- **SIP Entity 2** Select the SIP Entity added for Business Communication Manager in **Section 4.4.1** from the drop-down menu.
- **Protocol** After selecting both SIP Entities, select “**UDP**” as the required protocol from the drop-down menu.
- **Port** Verify **Port** for both SIP entities is the default listen port specified in **Section 4.3**.
- **Trusted** Enter ☒
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save.

The following screen shows the entity link defined between the Business Communication Manager and Session Manager.

The screenshot shows the Avaya Aura System Manager 5.2 interface. The top header displays the Avaya logo, the system name "Avaya Aura™ System Manager 5.2", and user information: "Welcome, admin Last Logged on at Jan. 14, 2010 4:44 PM". A sidebar on the left contains navigation links: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (selected), Adaptations, Dial Patterns, Entity Links (highlighted), Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities, Time Ranges, Personal Settings, Security, and Applications. The main content area is titled "Entity Links" and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The row shows: Name: BCM-S0 to ASM1, SIP Entity 1: ASM1-DR, Protocol: UDP, Port: 5060, SIP Entity 2: BCM-S0, Port: 5060, Trusted: checked, Notes: empty. Below the table, there is a red asterisk and the text "Input Required". At the top right of the main content area, there are "Commit" and "Cancel" buttons. At the bottom right, there are also "Commit" and "Cancel" buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
BCM-S0 to ASM1	ASM1-DR	UDP	5060	BCM-S0	5060	<input checked="" type="checkbox"/>	

4.4.3. Define Routing Policy

Expand **Network Routing Policy** and select **Routing Policies**

Click **New**. In the *General* Section, enter the following values.

- **Name** Enter an identifier for the link to Business Communication Manager
- **Notes** Enter a brief description. [Optional]

In the *SIP Entity as Destination* Section, click **Select**.

The **SIP Entity List** page opens.

- Select the entry of the Business Communication Manager added in **Section 4.4.1** and click **Select**
- The selected SIP Entity displays on the **Routing Policy Details** page.

Click **Commit** to save.

The following screen shows the routing policy defined for routing calls to the Business Communication Manager.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 22, 2010 4:05 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
BCM-50	10.80.48.10	Other	BCM-50 in branch site

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
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None (0 of 1 Selected)

Dial Patterns

Add Remove

1 Item Refresh Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
333	6	7	<input type="checkbox"/>	-ALL-	-ALL-	Calls to 333-xxx should route to BCM-50

Select : All, None (0 of 1 Selected)

Shortcuts

- Change Password
- Help for Routing Policy Details fields
- Help for SIP Entity List
- Help for Time Range List
- Help for Pattern List
- Help for Regular Expressions List
- Help for Committing configuration changes

4.4.4. Define Dial Pattern

Expand **Network Routing Policy** and select **Dial Patterns**

Click **New**. In the *General* Section, enter the following values.

- **Pattern** Add dial patterns for any extension numbers associated with stations on Business Communication Manager.
- **Min** Enter the minimum number of digits that must be dialed.
- **Max** Enter the maximum number of digits that may be dialed.
- **SIP Domain** Select the SIP Domain added in **Section 4.1** or select “**All**” if Session Manager should accept incoming calls from all SIP domains.
- **Notes** Enter a brief description. [Optional]

In the *Locations and Routing Policies* Section, click **Add**.

The **Originating Locations and Routing Policy List** page opens.

- In **Originating Locations** table, select “**ALL**”
Note: select a specific location in the **Originating Locations** table if location-based routing is being used.
- In **Routing Policies** table, select the routing policy defined for Business Communication Manager in **Section 4.4.3**
- Click **Select** to save changes and return to **Dial Patterns Details** page.

Click **Commit** to save. The following screen shows the dial pattern defined for routing calls to the Business Communication Manager.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 22, 2010 4:05 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:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to BCM-50	0	<input type="checkbox"/>	BCM-50	333-xxxx

Select : All, None (0 of 1 Selected)

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

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

* Input Required Commit Cancel

4.5. Add Avaya Modular Messaging

The following section captures the relevant screens for configuring the SIP Entity associated with Avaya Modular Messaging to enable stations on either Communication Manager or Business Communication Manager to access the Modular Messaging system.

4.5.1. Define SIP Entity and Entity Link

Expand **Network Routing Policy** and select **SIP Entities**.

Click **New**. In the *General* Section, enter the following values.

- **Name** Enter an identifier for Modular Messaging
- **FQDN or IP Address** Enter the IP address of the Messaging Application Server (MAS) of the Avaya Modular Messaging system
- **Type** Select “**Other**” from drop-down menu.
- **Notes** Enter a brief description. [Optional]
- **Location** Select the appropriate Location from **Section 4.2**

In the *Entity Links* Section, click **Add** (not shown). Enter the following values.

- **Name** Enter an identifier for Modular Messaging
- **SIP Entity 1** Select Session Manager
- **SIP Entity 2** Select SIP Entity for Modular Messaging as “**Trusted**”
- **Protocol** After selecting both SIP Entities, select “**TCP**”
- **Port** Verify **Port** for both entities is “**5060**”
- **Notes** Enter a brief description [Optional]

Click **Commit** to save. The following screen shows the addition of Modular Messaging for the sample configuration.

The screenshot displays the Avaya Aura System Manager 5.2 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura™ System Manager 5.2', and a user status 'Welcome, admin Last Logged on at Apr. 20, 2010 11:09 AM' with links for 'Help' and 'Log off'.

The main content area is titled 'Home / Network Routing Policy / SIP Entities / SIP Entity Details'. On the left is a sidebar menu with categories: Asset Management, Communication System Management, User Management, Monitoring, Network Routing Policy (expanded), Security, Applications, Settings, and Session Manager. Under 'Network Routing Policy', options include Adaptations, Dial Patterns, Entity Links, Locations, Regular Expressions, Routing Policies, SIP Domains, SIP Entities (selected), Time Ranges, and Personal Settings. A 'Shortcuts' section at the bottom of the sidebar lists 'Change Password', 'Help for SIP Entity Details fields', 'Help for Committing configuration changes'.

The 'SIP Entity Details' form is divided into two sections: 'General' and 'SIP Link Monitoring'.
General Section:
- * Name: SIL-DR-MAS1
- * FQDN or IP Address: 10.80.100.30
- Type: Other (dropdown)
- Notes: MM Single Server
- Adaptation: (dropdown)
- Location: 10_80_100 (dropdown)
- Time Zone: America/Denver (dropdown)
- Override Port & Transport with DNS SRV: ☐
- * SIP Timer B/F (in seconds): 6
- Credential name: (text field)
- Call Detail Recording: none (dropdown)
SIP Link Monitoring Section:
- SIP Link Monitoring: Use Session Manager Configuration (dropdown)

Below the form is the 'Entity Links' section, which includes 'Add' and 'Remove' buttons. It contains a table with 1 item, showing a link between 'SIP Entity 1' (ASM1-DR) and 'SIP Entity 2' (SIL-DR-MAS1) using 'TCP' protocol on port '5060'. The 'Trusted' checkbox is checked. The table has columns for SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and Trusted. Below the table, it says 'Select : All, None (0 of 1 Selected)'. At the bottom of the form are 'Commit' and 'Cancel' buttons.

4.5.2. Define Routing Policy

Expand **Network Routing Policy** and select **Routing Policies**

Click **New**. In the *General* Section, enter the following values.

- **Name** Enter an identifier to define the routing policy for Modular Messaging
- **Notes** Enter a brief description. [Optional]

In the *SIP Entity as Destination* Section, click **Select**. The **SIP Entity List** page opens.

- Select the entry for Modular Messaging added in **Section 4.5.1** and click **Select**.
- The selected SIP Entity displays on the **Routing Policy Details** page.

Click **Commit** to save. The following screen shows the routing policy defined for routing calls to Avaya Modular Messaging.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, admin Last Logged on at Apr. 20, 2010 11:09 AM
[Help](#) | [Log off](#)

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

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

Security

Applications

Settings

Session Manager

Shortcuts

Change Password

Help for Routing Policy Details fields

Help for SIP Entity List

Help for Time Range List

Help for Pattern List

Help for Regular Expressions List

Help for Committing configuration changes

Routing Policy Details

CommitCancel

General

* Name: to SIL-MAS1

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SIL-DR-MAS1	10.80.100.30	Other	MM Single Server

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: 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

Select : All, None (0 of 1 Selected)

Dial Patterns

AddRemove

4 Items RefreshFilter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	6665000	7	7	<input type="checkbox"/>	-ALL-	-ALL-	CM MM access
<input type="checkbox"/>	6665001	7	7	<input type="checkbox"/>	avaya.com	-ALL-	Nortel MM Access
<input type="checkbox"/>	6665002	7	7	<input type="checkbox"/>	avaya.com	-ALL-	BCM MM Access
<input type="checkbox"/>	7775000	7	7	<input type="checkbox"/>	-ALL-	-ALL-	

Select : All, None (0 of 4 Selected)

4.5.3. Define Dial Pattern

Expand **Network Routing Policy** and select **Dial Patterns**

Click **New**. In the *General* Section, enter the following values.

- **Pattern** Add dial pattern for pilot numbers to Modular Messaging.
- **Min** Enter the minimum number digits that must be dialed.
- **Max** Enter the maximum number digits that may be dialed.
- **SIP Domain** Select the SIP Domain from drop-down menu or select “**All**” if Session Manager should accept incoming calls from all SIP domains.
- **Notes** Enter a brief description. [Optional]

In the Locations and Routing Policies Section, click **Add**.

The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select “**ALL**”
- In **Routing Policies** table, select the Routing Policy defined for Modular Messaging in **Section 4.5.2**
- Click **Select** to save changes and return to **Dial Patterns Details** page.

Click **Commit** to save. The following screen shows the dial pattern defined for routing calls to Avaya Modular Messaging mailboxes associated with stations on Business Communication Manager.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, **admin** Last Logged on at Apr. 20, 2010 11:09 AM [Help](#) [Log off](#)

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

Dial Pattern Details Commit Cancel

General

* Pattern: 6665002

* Min: 7

* Max: 7

Emergency Call: ☐

SIP Domain: avaya.com

Notes: BCM MM Access

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to SIL-MAS1	0	<input type="checkbox"/>	SIL-DR-MAS1	

Select : All, None (0 of 1 Selected)

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

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

* Input Required Commit Cancel

5. Configure Avaya Business Communication Manager

This section describes the relevant configuration of the SIP Trunks and call routing between Business Communication Manager and Session Manager.

In addition to the steps described in this section, other configuration activities will be needed such as verifying licensing, configuring digital and IP stations, and defining the associated Target Lines for each station on Business Communication Manager. For more information on these additional actions, see the appropriate documentation in **Section 10**.

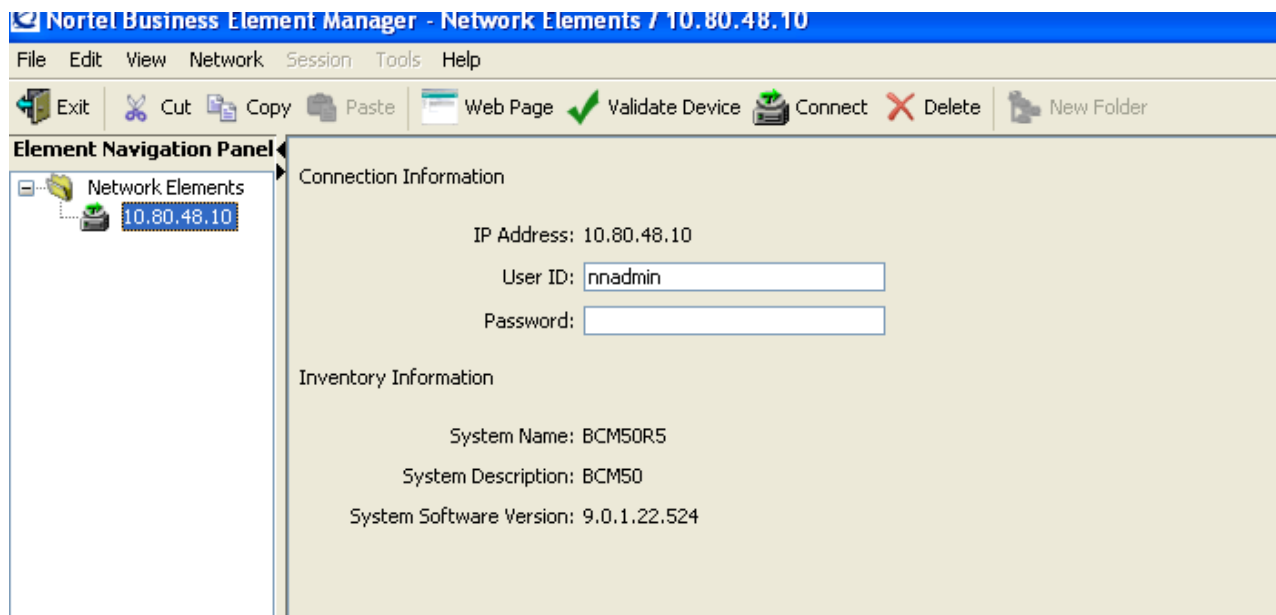
Business Communication Manager is configured using the Business Element Manager GUI.

5.1. Run Element Manager Application and Login

Select the **Business Element Manager** from the BCM applications list and select the **Run** button to download the application to the desktop.

Enter the default user name and password to log into the **Business Element Manager**.

The following screen is displayed:

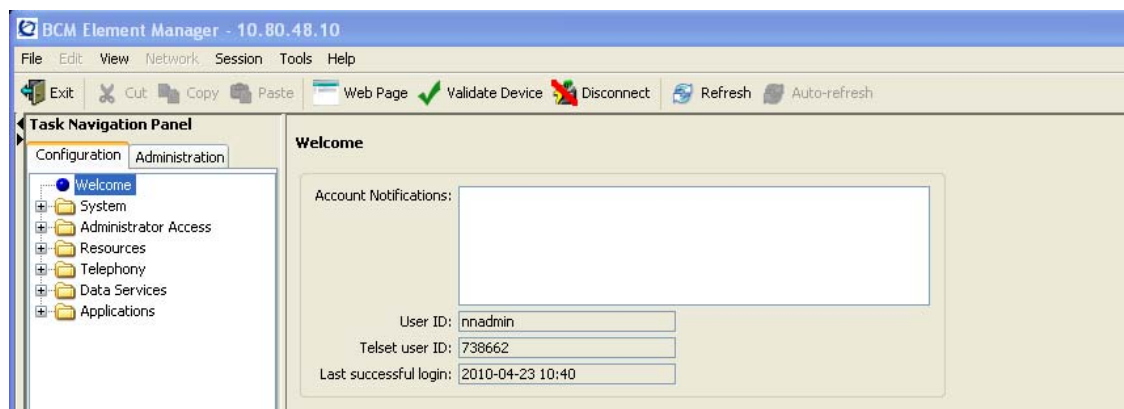


Select the IP address of the appropriate Business Communication Manager server on the **Element Navigation Panel** on the left side of the page. In the sample configuration, the Business Element Manager is used to manage a single Business Communication Manager server.

Enter the appropriate credentials on the **Connection Information** page shown above and select the **Connect** button in the Toolbar.

After connecting to Business Communication Manager, the initial **Business Element Manager** screen appears as shown below.

Note: on the screen below, the **Element Navigation Panel** has been collapsed.



Use the **Task Navigation Panel** on the left side of the page to navigate to specific configuration tasks.

5.2. Add SIP Trunk to Avaya Aura™ Session Manager

Navigate to **Resources** → **Telephony Resources** task in the **Task Navigation Panel**.

Select the **IP Trunks** row in the **Telephony Resources** table. Wait for the configuration details of IP Trunks to be displayed in the lower section of the screen as shown below:

The screenshot shows the BCM Element Manager interface. The Task Navigation Panel on the left has 'Telephony Resources' selected. The main area displays a table of Telephony Resources. The 'Internal' row for 'IP Trunks' is selected. Below the table, the 'Details for Module: Internal IP Trunks' section is visible, showing tabs for 'Routing Table', 'IP Trunk Settings', 'H323 Settings', 'H323 Media Parameters', 'SIP Settings', 'SIP Proxy', 'SIP Media Parameters', 'SIP URI Map', and 'SIP Authentication'. The 'Routing Table' tab is active, showing a table with columns: Description, Destination Digits, Domain, IP Address, Port, GW Type, and MCDN Protocol.

Location	Configured Device	Bus	State	Low	High	Active	Busy
Internal	IP Trunks	N/A	Enabled	001	012	8	0
Internal	IP Sets	1	Enabled	301	332	2	0
Internal	Applications	1	Enabled	333	396	9	N/A
Main	GAT14	3	Enabled	061	064	4	0
Main	DS112	4	Enabled	221	232	0	0
Main	GAS14	4	Enabled	233	236	4	0
Expansion 1	DTM-PRI	5.1	Enabling...	065	087	0	0
Expansion 2	None	7.1	N/A	N/A	N/A	N/A	N/A

Details for Module: Internal IP Trunks

Routing Table | IP Trunk Settings | H323 Settings | H323 Media Parameters | SIP Settings | SIP Proxy | SIP Media Parameters | SIP URI Map | SIP Authentication

Description	Destination Digits	Domain	IP Address	Port	GW Type	MCDN Protocol
-------------	--------------------	--------	------------	------	---------	---------------

Add... Delete

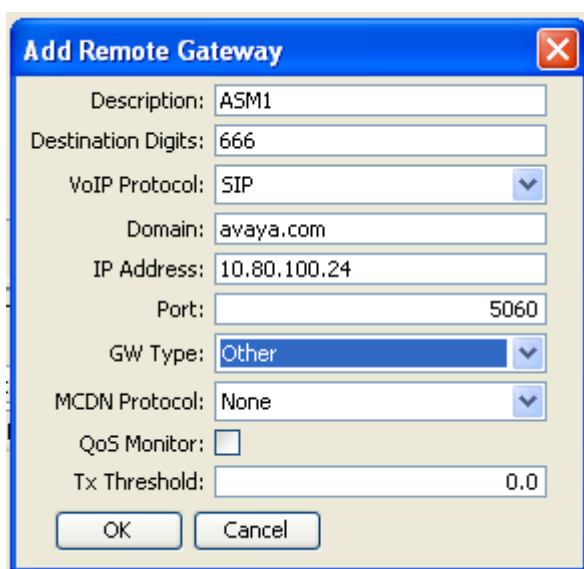
5.2.1. Configure Routing for SIP Trunks

Under the **Routing Table** tab, click **Add** to add a SIP Trunk to Session Manager

Enter the following values in the **Add Remote Gateway** dialog:

- **Description:** Enter a logical name for the trunk destination
- **Destination Digits:** Enter the set of digits or dial pattern to identify outgoing calls
- **VoIP Protocol:** Select “**SIP**” from drop-down menu.
- **Domain:** Enter the same SIP Domain name as defined in **Section 4.1**.
- **IP Address:** Enter IP address for the SM-100 card for Session Manager
- **Port:** Enter the same UDP port number as defined in **Section 4.3**.
- **GW Type:** Select “**Other**” from the drop-down menu
- **MCDN Protocol:** Select “**None**” from the drop-down menu
- **QoS Monitor:** Leave unchecked
- **Tx Threshold:** Leave this field at its default value of 0.0

The following dialog shows the values entered for the sample configuration.

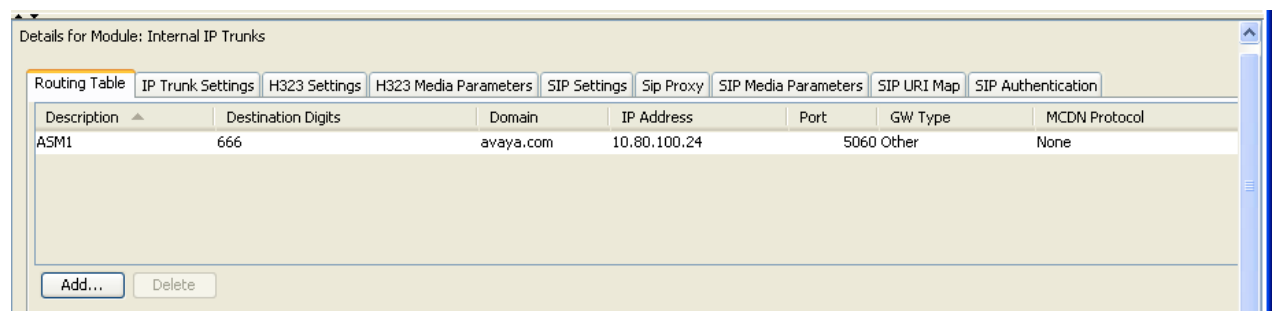


The 'Add Remote Gateway' dialog box contains the following fields and values:

- Description: ASM1
- Destination Digits: 666
- VoIP Protocol: SIP
- Domain: avaya.com
- IP Address: 10.80.100.24
- Port: 5060
- GW Type: Other
- MCDN Protocol: None
- QoS Monitor: ☐
- Tx Threshold: 0.0

Buttons: OK, Cancel

Click **OK** to save changes. The following screen shows the details of the **Routing Table** for the sample configuration:



Details for Module: Internal IP Trunks

Description	Destination Digits	Domain	IP Address	Port	GW Type	MCDN Protocol
ASM1	666	avaya.com	10.80.100.24	5060	Other	None

Buttons: Add..., Delete

5.2.2. Configure IP Trunk Settings

Under the **IP Trunk Settings** tab, configure the following parameters as shown below:

- **Forward redirected OLI** Enter ☒
- **Remote capability MWI** Enter ☒
- **Send name display** Enter ☒
- **Ignore in-band DTMF in RTP:** Leave blank

Details for Module: Internal IP Trunks

Routing Table | **IP Trunk Settings** | H323 Settings | H323 Media Parameters | SIP Settings | Sip Proxy | SIP Media Parameters | SIP URI Map | SIP Authentication

Telephony Settings

Forward redirected OLI: ☒ Send name display: ☒
Remote capability MWI: ☒ Ignore in-band DTMF in RTP: ☐

5.2.3. Configure SIP Settings

Under the **SIP Settings** tab, enter the following values in the *Telephony Settings* section.

- **Fallback to circuit-switched:** Select “**Enabled-All**” from the drop-down menu

Configure the following fields in the *RFC2833* section:

- **Dynamic Payload:** Enter value defined in **Telephone Event Payload Type** on the SIP Trunk Group form in **Section 3.5.2**
For the sample configuration, “**120**” was used.

Configure the following fields in the *SIP Settings* section:

- **Local Domain:** Enter the domain name defined in **Section 4.1**
- **Disable maddr in Contact** Enter ☒
- **Disable OPTIONS Caps** Enter ☒
- **Disable PRACK** Enter ☒
- **Call signaling port:** Enter Port from SIP Entity Link in **Section 4.4.2**
In the sample configuration, “**5060**” was used.

The following screen shows the details of the **SIP Settings** tab for the sample configuration:

Details for Module: Internal IP Trunks

Routing Table | IP Trunk Settings | H323 Settings | H323 Media Parameters | **SIP Settings** | Sip Proxy | SIP Media Parameters | SIP URI Map | SIP Authentication

Telephony Settings

Fallback to circuit-switched: Enabled-All

RFC2833

Dynamic Payload: 120

SIP Settings

Local Domain: avaya.com

Disable maddr in Contact: ☒
Disable OPTIONS Caps: ☒

Service Impacting SIP Settings

Call signaling port: 5060
Disable PRACK: ☒
Modify...

RTP Keepalives

Scope: None

Status: Gateway is running

5.2.4. Configure SIP Media Parameters

Under the **SIP Media Parameters** tab, configure the Business Communication Manager to use the same set of IP Codecs specified for Communication Manager in **Section 3.2**.

In the *Preferred Codecs* section on the left side of the page,

- Select **G.711-uLaw**, **G.729** from the **Available List** table and click **Add** to move these two codec choices to the **Selected List** table.
- Configure **G.711-uLaw** as the first choice by moving **G.711-ulaw** to top of list.

In the *Settings* section on the right side of the page, configure the following fields:

- **Enable Voice Activity Detection** Leave blank
- **G.729 payload size (ms):** Select “**20ms**” from the drop-down menu
- **G.711 payload size (ms):** Select “**20ms**” from the drop-down menu
- **Fax transport** Select “**T.38**” from the drop-down menu
- Use default values for remaining fields

The screen below shows the details of the **SIP Media Parameters** for the sample configuration:

The screenshot shows a web-based configuration interface titled "Details for Module: Internal IP Trunks". It features several tabs: "Routing Table", "IP Trunk Settings", "H323 Settings", "H323 Media Parameters", "SIP Settings", "Sip Proxy", "SIP Media Parameters" (which is the active tab), "SIP URI Map", and "SIP Authentication".

The "SIP Media Parameters" tab is divided into two main sections:

- Preferred Codecs:** This section contains two lists. The "Available list" on the left includes "G.723" and "G.711-aLaw". The "Selected list" on the right includes "G.711-uLaw" and "G.729". An "Add" button with a right-pointing arrow is positioned between the lists, and a "Del" button with a left-pointing arrow is below it. A vertical double-headed arrow is to the right of the "Selected list".
- Settings:** This section contains several configuration fields:
 - "Enable Voice Activity Detection": An unchecked checkbox.
 - "Jitter buffer": A dropdown menu set to "Auto".
 - "G.729 payload size (ms)": A dropdown menu set to "20".
 - "G.723 payload size (ms)": A dropdown menu set to "30".
 - "G.711 payload size (ms)": A dropdown menu set to "20".
 - "Fax transport": A dropdown menu set to "T.38".
 - "Force G.711 for 3.1k audio": An unchecked checkbox.
 - "Provide in-band ringback": An unchecked checkbox.

5.3. Define Business Name

Navigate to the **Telephony → Global Settings → Features Settings** task.

Enter a name into the **Business Name** field on this page. This name will be sent as part of the user information in SIP messages. If the Business Name field is left blank, Business Communication Manager will not include the station name in the SIP message.

Note: Since Business Communication Manager concatenates the station name to the end of the Business Name in the SIP message and there appears to be a fixed length for this concatenated string, using a short Business Name is recommended.

Default values can be used for other fields on this page.

The following screen shows the **Feature Settings** for the sample configuration:

The screenshot displays the BCM Element Manager web interface. The title bar indicates the URL is 10.80.48.10. The left-hand 'Task Navigation Panel' shows a hierarchical tree structure. Under 'Global Settings', 'Feature Settings' is highlighted. The main panel, titled 'Feature Settings', contains the following configuration options:

- Business Name:** A text input field containing 'BCM'.
- Feature Settings:**
 - Background music: ☐
 - Page tone: ☒
 - Message reply enhancement: ☐
 - Force auto/spd dial over ic/conf: ☐
 - On hold: Tones (dropdown)
 - Held line reminder: Off (dropdown)
 - Delayed ring transfer: After 4 rings (dropdown)
 - Park mode: Lowest (dropdown)
 - Maximum CLI per line: 30 (text input)
 - Answer keys: Basic (dropdown)
 - Receiver volume: Use sys volume (dropdown)
 - Directed pickup: ☒
 - Set relocation: ☐
 - Alarm set: 221 (text input)
- Timers:**
 - Camp timeout (sec.): 45 (dropdown)
 - Park timeout (sec.): 45 (dropdown)
 - Page timeout (sec.): 180 (dropdown)
 - Transfer callback timeout: After 4 rings (dropdown)
 - Host delay (ms.): 1000 (dropdown)
 - Link time (ms.): 600 (dropdown)

5.4. Configure Dialing Plan

5.4.1. Configure SIP Line Pool

Navigate to the **Telephony → Dialing Plan → Line Pool** task.

Select “**BlocA**” from the **Line Pools** table. In the *Details for Line Pool: BlocA* Section at the bottom of the page, click **Add**. Enter **DN** of each station to allow access to the SIP trunk.

Note: BlocA Line Pool is automatically configured as a VoIP Trunk Type. The screen below shows results for the sample configuration.

BCM Element Manager - 10.80.48.10

File Edit View Network Session Tools Help

Exit Cut Copy Paste Web Page Validate Device Disconnect Refresh Auto-refresh

Task Navigation Panel

Configuration Administration

- Welcome
- System
- Administrator Access
- Resources
- Telephony
 - Global Settings
 - Sets
 - Lines
 - Loops
 - Scheduled Services
 - Dialing Plan
 - General
 - DNs
 - Public Network
 - Private Network
 - Line Pools**
 - Routing
 - Ring Groups
- Call Security
 - Hospitality
 - Hunt Groups
 - Call Detail Recording
 - Call Recording
- Data Services
- Applications

Dialing Plan - Line Pools

Pool	Access Code
A	
B	
C	
D	
E	
F	
G	
H	
I	
J	
K	
L	
M	
N	
O	
BlocA	N/A
BlocB	N/A
BlocC	N/A
BlocD	N/A
BlocE	N/A
BlocF	N/A

Details for Line Pool: BlocA

DNs Call by Call Limits

DNs with Access to Line Pool

DN

- 221
- 222
- 301
- 302

Add... Delete

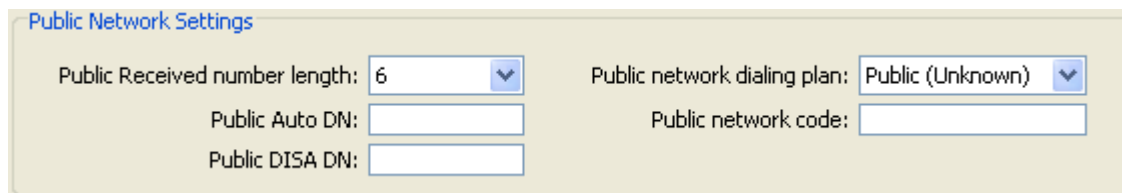
5.4.2. Configure Public Network

Navigate to the **Telephony → Dialing Plan → Public Network** task.

In the *Public Network Settings* section, configure the following fields:

- **Public Received number length:** Select the correct number of digits for received calls from drop-down menu
- **Public network dialing plan:** Select “**Public (Unknown)**” from drop-down menu
- Leave remaining fields blank

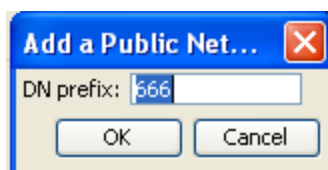
The screen below shows the settings for the sample configuration:



Public Network Settings

Public Received number length:	<input type="text" value="6"/>	Public network dialing plan:	<input type="text" value="Public (Unknown)"/>
Public Auto DN:	<input type="text"/>	Public network code:	<input type="text"/>
Public DISA DN:	<input type="text"/>		

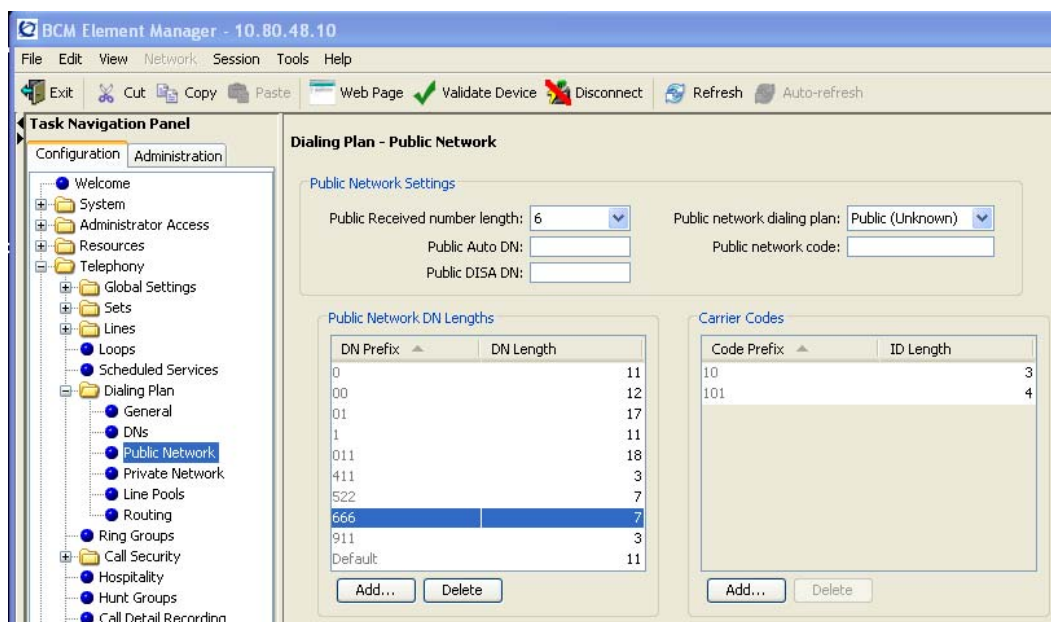
In the *Public Network DN Length* section, click **Add** to define a dialed number prefix pattern. In the sample configuration, received calls contain 6 digits and outgoing calls routed to Session Manager will start with the digits “666” as shown by the **Add a Public Network** dialog below:



Add a Public Net...

DN prefix:

Click **OK** to enter the new prefix. To avoid delays in placing outgoing calls, select the new row in the **Public Network DN Lengths** table and modify the **DN Length** field to match the number of digits in the dialed number as shown below:



BCM Element Manager - 10.80.48.10

File Edit View Network Session Tools Help

Exit Cut Copy Paste Web Page Validate Device Disconnect Refresh Auto-refresh

Task Navigation Panel

Configuration Administration

- Welcome
- System
- Administrator Access
- Resources
- Telephony
 - Global Settings
 - Sets
 - Lines
 - Loops
 - Scheduled Services
 - Dialing Plan
 - General
 - DNs
 - Public Network**
 - Private Network
 - Line Pools
 - Routing
 - Ring Groups
 - Call Security
 - Hospitality
 - Hunt Groups
 - Call Detail Recording

Dialing Plan - Public Network

Public Network Settings

Public Received number length:	<input type="text" value="6"/>	Public network dialing plan:	<input type="text" value="Public (Unknown)"/>
Public Auto DN:	<input type="text"/>	Public network code:	<input type="text"/>
Public DISA DN:	<input type="text"/>		

Public Network DN Lengths

DN Prefix	DN Length
0	11
00	12
01	17
1	11
011	18
411	3
522	7
666	7
911	3
Default	11

Carrier Codes

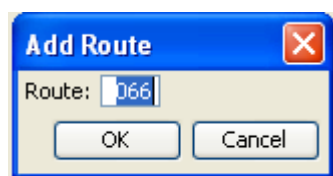
Code Prefix	ID Length
10	3
101	4

Move the cursor to save the change. **Note:** This change may take several seconds to finish.

5.4.3. Configure Routing

Navigate to the **Telephony → Dialing Plan → Routing** task.

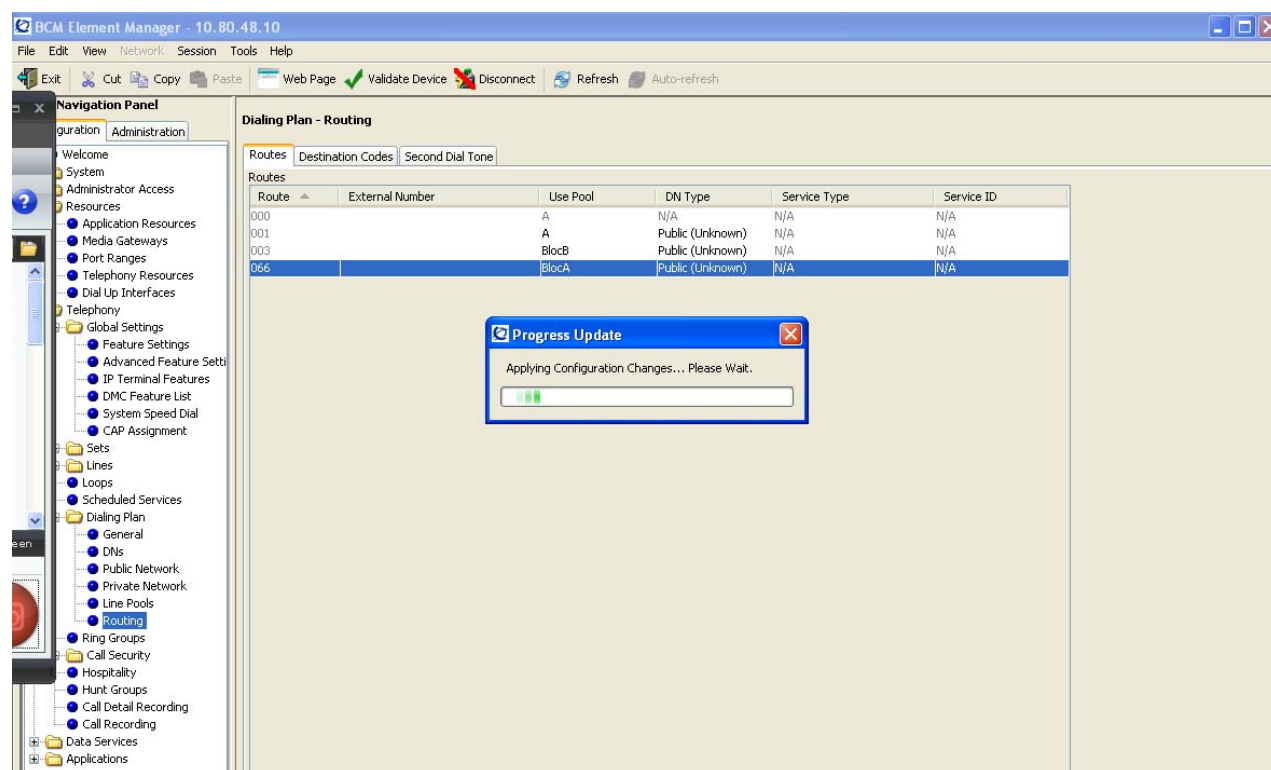
Under the **Routing** tab, click **Add** to create a route for routing calls to Session Manager. Enter an available route number in the **Add Route** dialog as shown below:



Click **OK** to add the route.

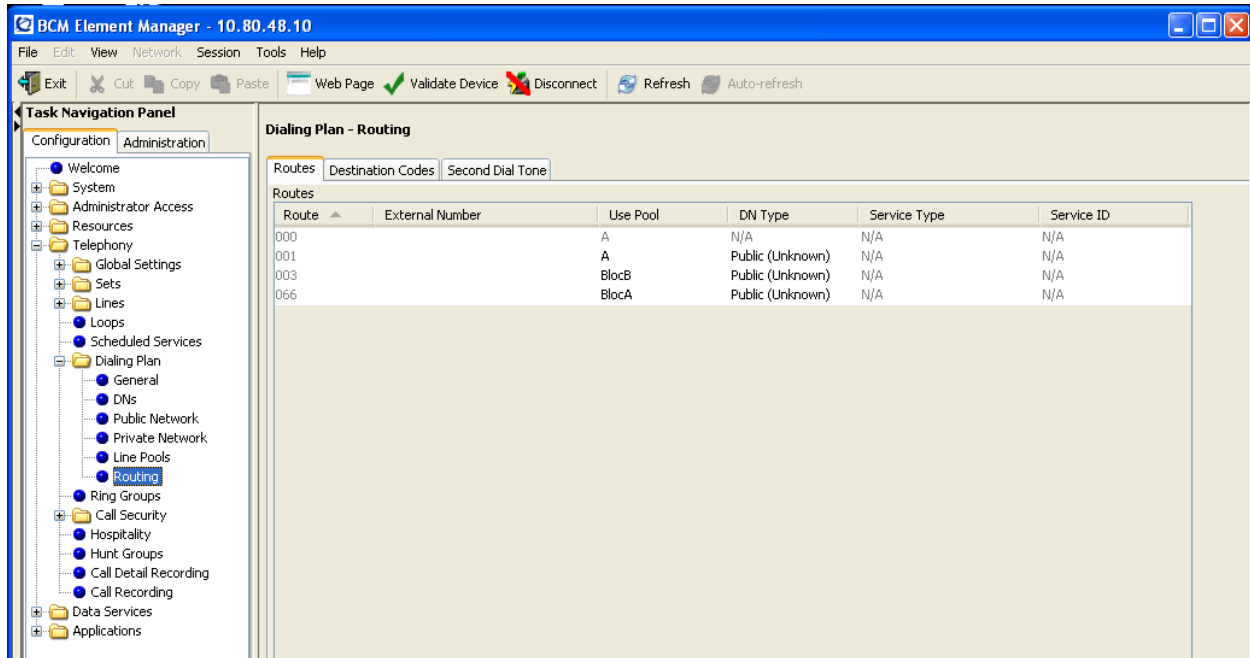
Select the row associated with the new route in the **Routes** table and select "**BlocA**" from the drop-down menu associated with the **Use Pool** column.

This change may take several seconds to complete as shown below:



After the **Use Pool** change completes under the **Routes** tab, select "**Public (Unknown)**" from drop-down menu associated with the **DN type** column.

The following screen shows the additional route defined for routing calls to Session Manager in the sample configuration:

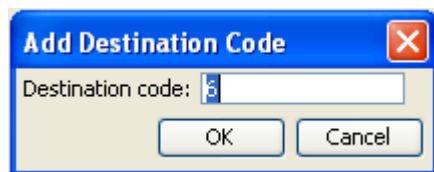


5.4.4. Configure Destination Code

Navigate to the **Telephony → Dialing Plan → Routing** task.

Under the **Destination Code** tab, click **Add** to create a destination code for routing calls to Session Manager.

Enter the first digit of the number used for outgoing calls to Session Manager in the **Add Destination Code** dialog as shown below:



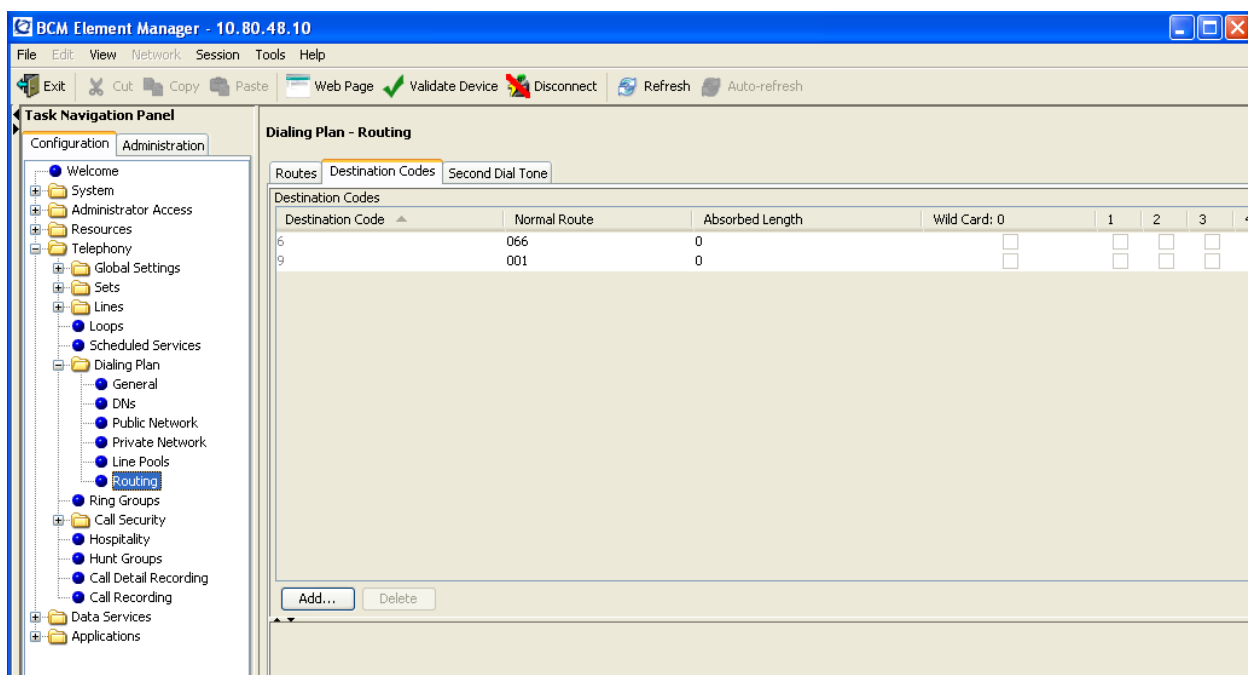
Click **OK** to save the new destination code.

Select the row associated with the new destination code in the **Destination Codes** table and configure the following fields.

- **Normal Route:** Enter the route number defined in **Section 5.4.3**
- **Absorbed Length:** Select “0” from the drop-down menu since the number used as the destination code is the first digit in the outgoing dialed number.

Note: The values defined for the **Destination Code** and **Absorbed Length** fields depend on the specific deployment. Other values in the **Destination Codes** table may be appropriate for different customer networks.

The screen below shows the details of the **Destination Codes** table for the sample configuration:



5.5. Configure Dialing Plan for Avaya Modular Messaging

Since calls to Avaya Modular Messaging are also routed through Session Manager, it may not be necessary to configure additional routing policies in Business Communication Manager.

For example, the pilot number for stations on Business Communication Manager to access Modular Messaging in the sample configuration is “666-5002”. Since all calls starting with the digits “666” will be routed to Session Manager, it was not necessary to configure any other routing rules.

5.6. Configure Stations for Coverage to Avaya Modular Messaging

Navigate to the **Telephony → Sets → Active Sets** task.

Select the row associated with an installed station to configure coverage to Modular Messaging for the station. Enter the pilot number of the Modular Messaging system in both the **Fwd No Answer** and **Fwd Busy** fields. Enter the number of rings in the **Fwd Delay** field.

In the sample configuration, the pilot number for Modular Messaging was “**6665002**” and the **Fwd Delay** was set to “**2**”. The screen below shows the configuration for coverage to Modular Messaging in the sample configuration:

The screenshot displays the BCM Element Manager web interface. The left-hand 'Task Navigation Panel' shows a tree structure with 'Sets' expanded and 'Active Sets' selected. The main content area, titled 'Active Sets', contains a table with columns for DN, Model, Name, Port, Pub. OLI, Priv. OLI, Fwd No Answer, Fwd Delay, and Fwd Busy. The table lists several entries, with row 236 highlighted in blue. The interface also includes a menu bar at the top and a toolbar with icons for Exit, Cut, Copy, Paste, Web Page, Validate Device, Disconnect, Refresh, and Auto-refresh.

DN	Model	Name	Port	Pub. OLI	Priv. OLI	Fwd No Answer	Fwd Delay	Fwd Busy
221	T7316E	Jane DT	0401	221	221	6665002	2	6665002
222	T7316E	Bill DT	0402	222	222	6665002	2	6665002
233	Analog	Fax	0413	233	233		N/A	
234	Analog	234	0414		234		N/A	
235	Analog	235	0415		235		N/A	
236	Analog	236	0416		236		N/A	
301	1230	Tom IP	0101	301	301	6665002	2	6665002
302	1230	Deb IP	0109	302	302	6665002	2	6665002

6. Configure Avaya Modular Messaging

This section describes the relevant configuration of the SIP Trunk between Avaya Modular Messaging and Session Manager, and any administration necessary to add Voice Mail mailboxes for stations on Business Communication Manager. In addition to the steps described in this section, other installation and initial configuration actions will be needed. For more information on these additional actions, see the appropriate documentation in **Section 10**.

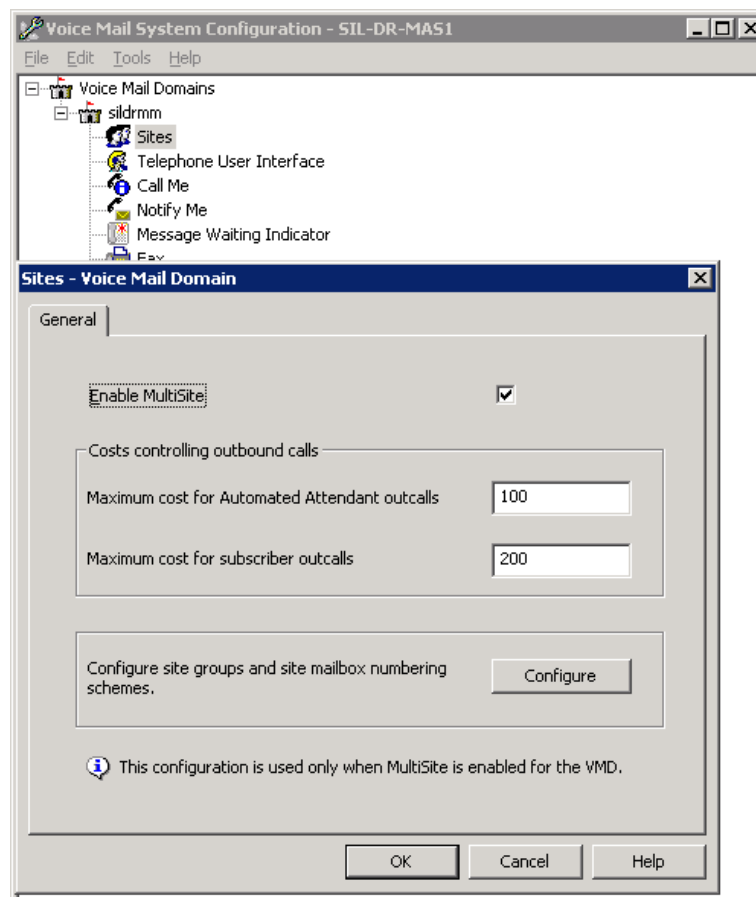
In the sample configuration, Session Manager was added as a PBX. Communication Manager Access Element, Communication Manager Feature Server and Business Communication Manager were added as sites, using the Avaya Modular Messaging Multi-Site feature.

Unless otherwise indicated, the administration steps described in this section were completed on the Messaging Application Server (MAS) via the Voice Mail System Configuration (VMSC) console. Log into the MAS server and launch the VMSC console application.

6.1. Verify Multi-Site Configuration

Double-click on the **Sites** icon in the VMSC console window. Under the **General** tab, verify MultiSite is enabled as shown below:

- **Enable MultiSite** Enter ☒

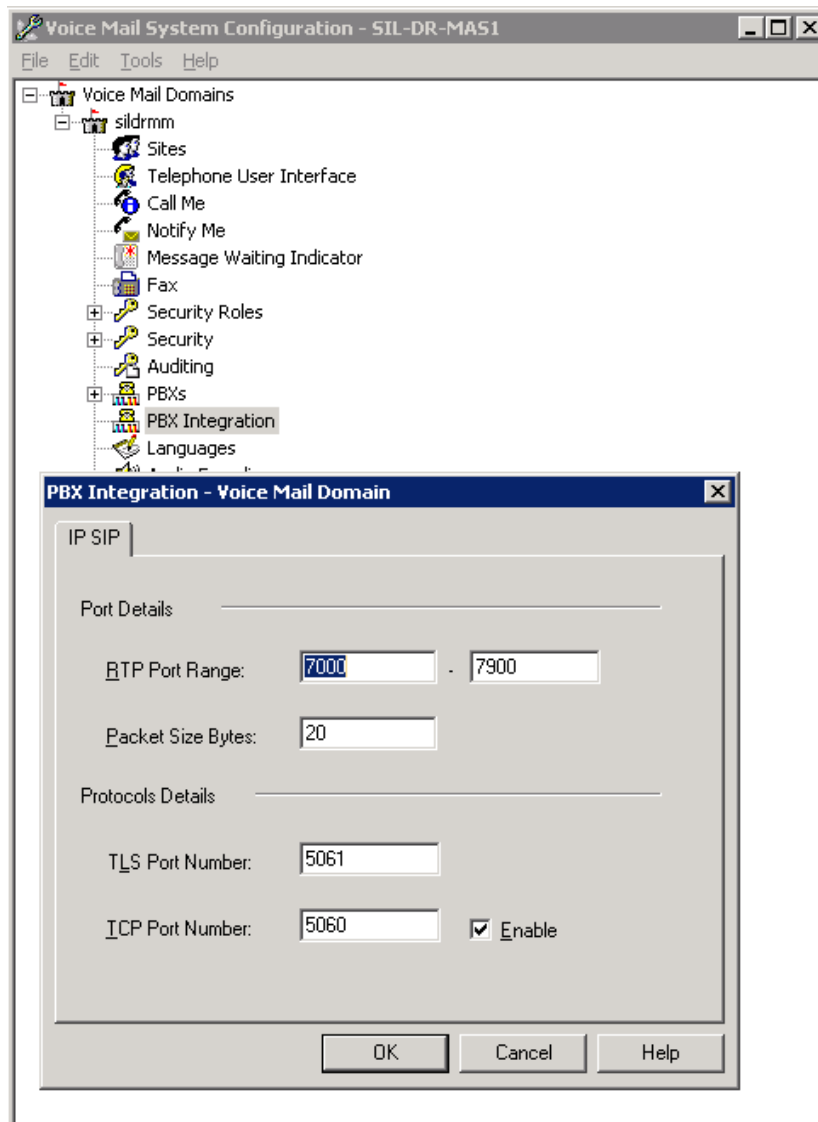


6.2. Configure TCP Port

As described in **Section 4.5.1**, the Entity Link between Avaya Modular Messaging and Session Manager was configured as a TCP link using Port 5060. To configure Modular Messaging to use the same protocol and port number, double-click the **PBX Integration** icon in the VMSC console window.

In the *Port Details* section on the **IP SIP** tab, configure the following fields as shown below:

- **TCP Port Number:** Enter “5060”
- **Enable** Enter ☒

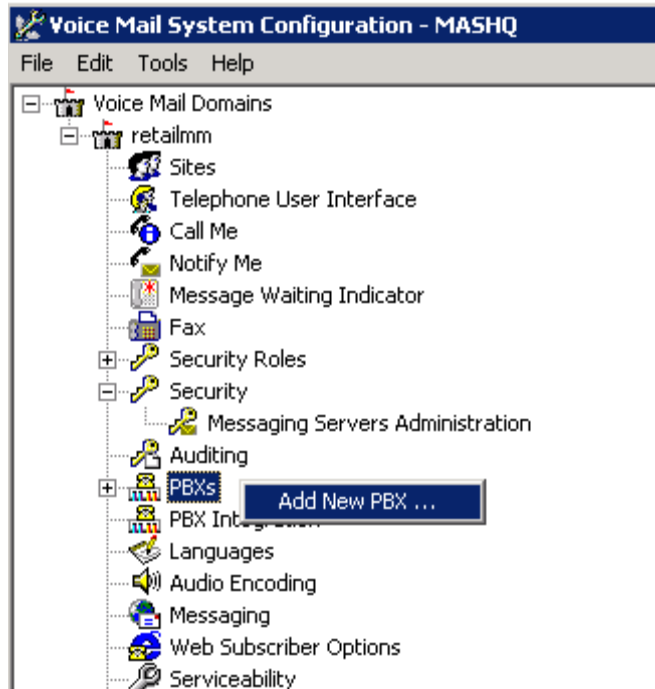


Click **OK** to save changes.

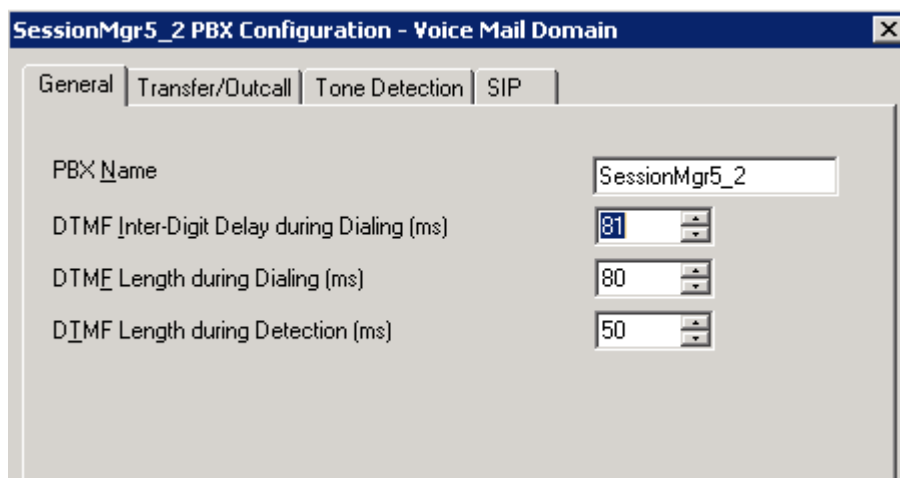
6.3. Administer Avaya Aura™ Session Manager as PBX

From the Modular Messaging perspective, all SIP messages are coming from the Session Manager. Both Business Communication Manager and Communication Manager are defined within Modular Messaging as **sites** whereas Session Manager will be defined as the **PBX**.

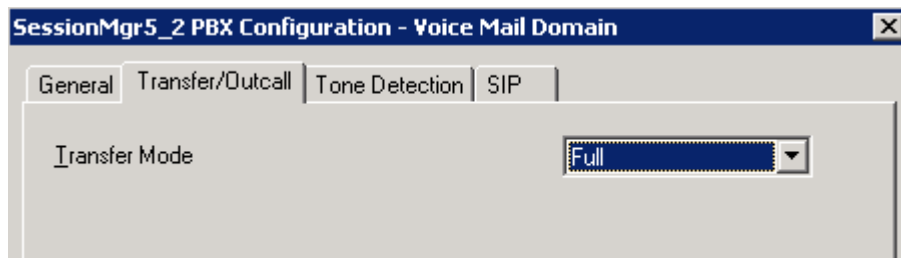
Right-click on the **PBXs** icon in the VPMS console and select **Add New PBX** as shown below:




On the **General** tab, enter an appropriate name for the Session Manager in the **PBX Name** field and use default values for the remaining fields as shown below:

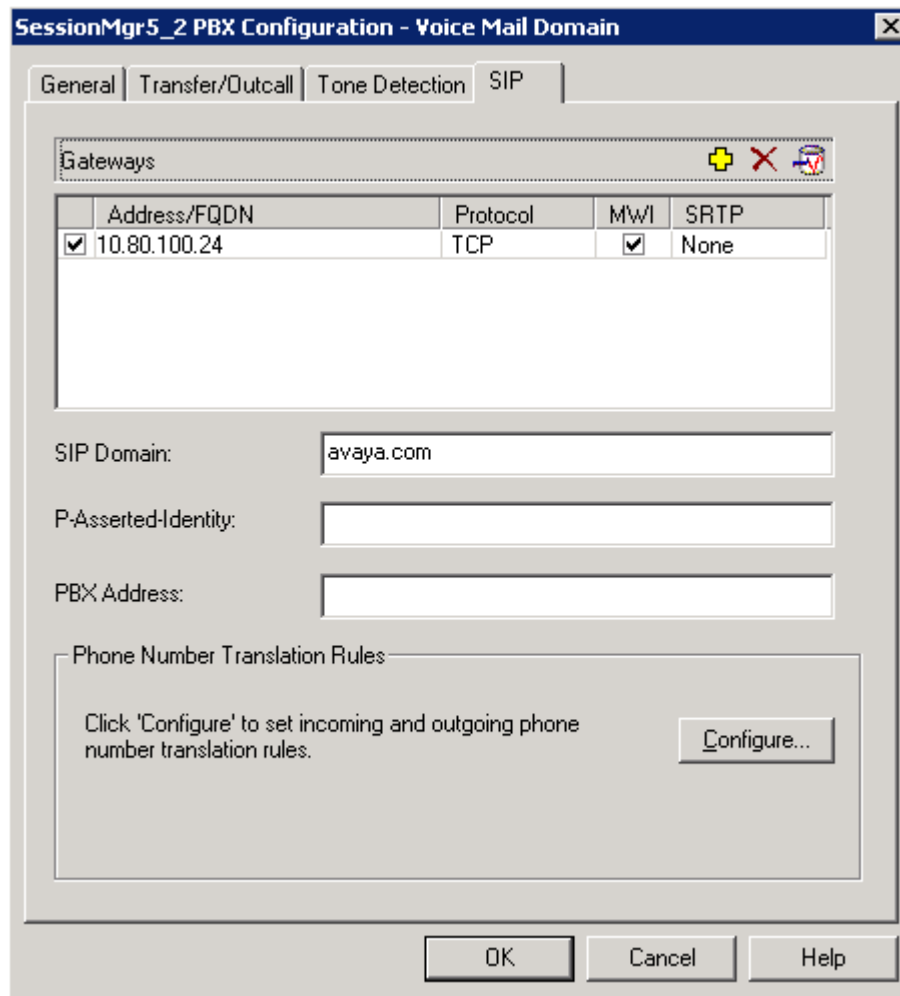


On the **Transfer/Outcall** tab, select “**Full**” from the drop-down menu for **Transfer Mode**:



Under the **SIP** tab, click on the  icon in the *Gateways* section. Enter the IP address of the SM 100 interface for Session Manager under **Address/FQDN** field in the new row. Enter “**TCP**” in the **Protocol** field, and check the **MWI** box so message waiting notifications will be sent.

Enter the domain named defined in **Section 4.1** in the **SIP Domain** field. Leave the other fields blank. The following screen shows the values for the sample configuration:



Click **Configure** at the bottom of the page to define the rules for translating between the local dial plans of either Communication Manager or Business Communication Manager and the normalized 11 digit format used by Modular Messaging. These rules are created using the Modular Messaging regular expression syntax.

Note: For more detailed information on how to use the regular expression syntax to administer the **Translations Rules**, see **References [17] and [18] in Section 10.**

For the sample configuration, two rules were added by selecting **Add** (not shown).

The first rule is used to translate calls from Communication Manager to Business Communication Manager using the 6-digit dialed number format of “**333xxx**”. The second rule is used to translate calls between stations on Business Communication Manager which use 3-digit station numbers format of “**xxx**”.

Proper operation of the rules can be verified by adding **Test inputs** in the table on the left side of the page and viewing the resulting output in the corresponding rule in table on the right side of the page. If the input can be translated, the results will be displayed in green. If the test input fails, the results will be shown in red.

As shown below, entering “**333301**” as a row in **Test inputs** table is successfully translated by Modular Messaging as shown by the green highlighted row in the results table on the right side of the page. Using the first rule, the input of “**333301**” is converted to canonical number “**+1303333301**”.

Translation Rules								
Test inputs	Incoming translation rule				Outgoing translation rule			
	Description	Match	Output	Canonical Test	Match	Output	Switch Test	Cost
✓ +16186663010	Branch1_SRST_1	^(666300[8,9])\$	+1618\$1		^+1618(666300[8,9])\$	\$1		0
✓ +13036624004	Branch_SRST_2	^(666301[0-2])\$	+1618\$1		^+1618(666301[0-2])\$	\$1		0
✓ 19057771088	DID_to_666	^(666\d{4})\$	+1303\$1		^+1303(666\d{4})\$	\$1		0
✓ 7771088	CM_toBCM_calls	^(333\d{3})\$	+13033\$1	+1303333301	^+13033(333\d{3})\$	\$1	333301	0
✓ 333301	BCM_toBCM calls	^(d{3})\$	+13033333\$1					0
✓ +13033333301	To CS1000E				^+1905(777\d{4})\$	\$1		0
✓ 13036664000	x777	^(777\d{4})\$	+1905\$1		^+1905(777\d{4})\$	\$1		0
✓ 301	National Incoming	^(1\d{10})\$	+\$1					0
✓ 222	OutGoingQSIGT1	^(662\d{4})\$	\$1		^+1303(662\d{4})\$	\$1		0
✓ 333222	National Outgoing				^+(1\d{10})\$	9\$1		0
✓ 6663007								

As shown below, entering “301” as a row in **Test inputs** table is also successful and uses the second rule to translate “301” to the same canonical number “+13033333301”.

Translation Rules								
Test inputs	Incoming translation rule				Outgoing translation rule			
	Description	Match	Output	Canonical Test	Match	Output	Switch Test	Cost
✓ +16186663010	Branch1_SRST_1	^(666300{8,9})\$	+1618\$1		^+1618(666300{8,9})\$	\$1		0
✓ +13036624004	Branch_SRST_2	^(666301{0-2})\$	+1618\$1		^+1618(666301{0-2})\$	\$1		0
✓ 19057771088	DID_to_666	^(666\d{4})\$	+1303\$1		^+1303(666\d{4})\$	\$1		0
✓ 7771088	CM_toBCM_calls	^(333\d{3})\$	+13033\$1		^+13033(333\d{3})\$	\$1	333301	0
✓ 333301	BCM_toBCM calls	^(d{3})\$	+13033333\$1	+13033333301				0
✓ +13033333301	To CS1000E				^+1905(777\d{4})\$	\$1		0
✓ 13036664000	x777	^(777\d{4})\$	+1905\$1		^+1905(777\d{4})\$	\$1		0
✓ 301	National Incoming	^(1\d{10})\$	+\$1					0
✓ 222	OutGoingQSIGT1	^(662\d{4})\$	\$1		^+1303(662\d{4})\$	\$1		0
✓ 333222	National Outgoing				^+(1\d{10})\$	9\$1		0
✓ 6663007								

Click **OK** when finished. Click **OK** a second time in the original **Add new PBX** window.

6.4. Administer Sites

This section describes the steps to add Communication Manager and Business Communication Manager as sites in Modular Messaging. **Note:** Since the extensions on the Communication Manager Feature Server are in the same range as those extensions managed by the Communication Manager Access Element, it is not necessary to add the Feature Server as a separate site in the sample configuration. Double-click the **Sites** icon in the VMSC console (not shown) and click **Configure** on the **General** tab.

Sites - Voice Mail Domain

General

☒ Enable MultiSite

Costs controlling outbound calls

Maximum cost for Automated Attendant outcalls: 100

Maximum cost for subscriber outcalls: 200

Configure site groups and site mailbox numbering schemes.

This configuration is used only when MultiSite is enabled for the VMD.

Click **Add** (not shown). Select **Site** from the drop-down menu to add a new site.

Enter the following values in the **New Site** dialog as shown below.

- **Parent site group** Select “<ROOT>” from drop-down menu to add new site to default group
- **Site name** Enter a site name such as BCM 50
- **Identifier** Enter a set of initial digits of the 11-digit mailbox number which will uniquely identify the site.
- **Full mailbox length** Select “11” from the drop-down menu
- **Short mailbox length** Select “3” from the drop-down menu
- **PBX** Select name of the PBX added in **Section 6.3**.

The 'New Site' dialog box contains the following fields and values:









- Parent site group:** <Root>
- Site name:** BCM 50
- Identifier:** 13033333 (with a preview of 13033333xxx)
- Full mailbox length:** 11
- Short mailbox length:** 3
- PBX:** SessionMgr5_2

Buttons for 'Add' and 'Cancel' are located on the right side.

Click **Add** when finished and repeat the above steps to add the Communication Manager site.

For the sample configuration, two new sites were created as highlighted below:

Site Configuration for sildrm

Site/group	ID	Mailbox number			Name	PBX
		Full	Short	Preview		
 BCM 50	13033333	11	3	13033333xxx		SessionMgr5_2
 AvayaAuraCM	1303666	11	7	1303666xxx		SessionMgr5_2
 SRST Branch 1	1618666	11	7	1618666xxx		SessionMgr5_2
 AvayaCS1000E	1905777	11	7	1905777xxx		SessionMgr5_2

Add

Delete

Properties

Tools

OK

Cancel

Help

6.5. Administer Subscribers

Subscriber Management is accomplished using the **Messaging Administration** web interface of the Messaging Storage Server. Enter URL of the Message Storage Server to open the web page.

Log in with the proper credentials and select **Messaging Administration → Subscriber Management** task from the navigation menu.

On the **Manage Subscriber** page shown below, click **Add or Edit** to add a mailbox for stations on both Business Communication Manager and Communication Manager.

Local Subscribers	Machine Name	Local Subscriber Mailboxes	Total Subscribers	Filtered Subscribers	Management
	SIL-DR-MSS1	20	24	24	Filter Manage
Remote Subscribers	Internet	0	0	0	Filter Manage

Under the **BASIC INFORMATION** section on the **Add Local Subscriber** page, configure the following required fields to add a new subscriber:

- **Last Name** Enter Last Name for station user
- **Password** Enter numeric password that will be used to access mailbox
- **Numeric Address** Enter the full 11-digit number for the new mailbox
- **Class Of Service** Select appropriate class of service from drop-down menu
- **Mailbox Number** Enter the full 11-digit number for the new mailbox
- **Community ID** Select “1” from drop-down menu
- Default values can be used for remaining fields.

The screen below shows the details for adding a new subscriber in the sample configuration:

Add Local Subscriber

BASIC INFORMATION * (Required Fields)			
*Last Name	Doe	First Name	Jane
*Password	*****	*Mailbox Number	1303333222
*Numeric Address	1303333222	PBX Extension	<input checked="" type="radio"/> Canonical <input type="radio"/> Switch Native
*Class Of Service	0 - All MM Subs	*Community ID	1

6.6. Configure Message Waiting Indication

For each Subscriber, the Message Waiting Indication needs to be configured for the type of incoming message, include fax documents. Configuring the Messaging Waiting Indication is accomplished using the **Web Subscribers Options** web page.

Log in with the proper credentials and select the **Notification** task from the toolbar.

On the **Notification** page, configure the following fields:

- **Enable Messaging Waiting Indicator** Enter ☒
- **Enable Message Waiting Indicator Rule** Enter ☒

Under the *Message Type* section on the **Notification** page, specify the type of messages as shown below:

- **Voice Messages** Enter ☒
- **Fax Messages** Enter ☒

The screenshot shows the Avaya Modular Messaging Web Subscriber Options interface. The top navigation bar includes 'Caller Experience', 'My Experience', 'Notification' (highlighted), 'Password', 'Options', and 'Logoff'. A left sidebar contains 'MWI', 'Call Me', 'Notify Me', and 'Help Menu'. The main content area is titled 'MWI' and contains the following configuration options:

- ☒ Enable Message Waiting Indicator
- ☒ Enable Message Waiting Indicator Rule
- Message Type**
 - ☒ Voice Messages
 - ☒ Fax Messages
 - ☐ Email Messages
 - ☐ Any Messages
- Message Importance Level**
 - ☐ High Importance
 - ☐ Normal Importance
 - ☐ Low Importance
 - ☒ Any Importance

At the bottom right of the configuration area are 'Apply' and 'Help' buttons.

Click **Apply** to save changes.

7. Verification Steps

7.1. Verify Avaya Aura™ Session Manager Configuration

7.1.1. Verify Avaya Aura™ Session Manager is Operational

Expand the **Session Manager** menu on the left navigational menu and click **System Status** → **System State Administration**.

Verify **Management State** is “**Management Enabled**” and the **Service State** is “**Accept New Service**” as shown below.

System State Administration

This page shows the current service and management state of configured Session Managers. You can use this page to make state changes in the context of an upgrade or necessary maintenance.

Session Manager Instances

2 Items						
<input type="checkbox"/>	Session Manager	Management State	Service State	Last Service State Change	Active Call Count	Version
<input type="checkbox"/>	ASM1-DR	Management Enabled	Accept New Service	No last service state change	0	5.2.1.1.521012 - 01-14-2010
<input type="checkbox"/>	ASM2-DR	Management Enabled	Accept New Service	Tue Jan 19 12:10:26 MST 2010	0	5.2.1.1.521012 - 01-14-2010
Select : All, None (0 of 2 Selected)						

Click **System Status** → **Security Module Status**

Verify the status of the **Security Module Deployment** (SM 100 network interface) is “**Up**” as shown below.

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

Security Module Statistics

Stat Name	ASM1-DR	ASM2-DR
Security Module Deployment	Up	Up

Click **System Status** → **Data Replication Status**

Verify the **Session Manager Downward Data Replication Status** is operational as shown below.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 04, 2010 1:38 PM
[Help](#) [Log off](#)

Home / Session Manager / System Status / Data Replication Status

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

System Status

System Tools

Session Manager Administration

Network Configuration

Device and Location Configuration

Application Configuration

System State Administration

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Data Replication Status

RegistrationSummary

User Registrations

Session Manager Downward Data Replication Status

This page allows you to view Session Manager downward data replication statistics and run tests.

Master Database and Session Manager Replica Database Statistics

Refresh

Stat Name	Master	ASM1-DR (replica)	ASM2-DR (replica)
Records Currently in Database	1077	1077	1077
Records Pending Update	0	0	0
Modifications	1303	11783	27701
Modifications Resulting from Audits	1941	0	0
Failed Modifications (replica only)	N/A	0	0
Failed Modifications Resulting from Audit (replica only)	N/A	0	0
Elapsed Time Since Last Update/Audit (Days H:M:S)	00:00:04	00:12:49	00:15:42
Elapsed Time Since Last Update/Audit Requiring Modifications (Days H:M:S)	00:04:14	20 01:43:06	46 23:36:00
Last JMS Message Sent (master) / Received (replica)	Jan 4, 2010 2:33:56 PM MST	Jan 4, 2010 2:33:56 PM MST	Jan 4, 2010 2:33:56 PM MST
Last JMS Message Received (master) / Sent (replica)	Jan 4, 2010 2:25:21 PM MST	Jan 4, 2010 2:25:21 PM MST	Jan 4, 2010 2:22:28 PM MST
JMS Connection Status	OK	OK	OK
Test String Value	1111	1111	1111
Test String Last Update Time	Dec 22, 2009 2:51:26 PM MST	Dec 22, 2009 2:51:26 PM MST	Dec 22, 2009 2:51:26 PM MST

Shortcuts

Change Password

7.1.2. Verify SIP Link Status

Expand the **Session Manager** menu on the left navigational menu and click **System Status** → **SIP Entity Monitoring**.

Verify all SIP Entity Links are operational as shown below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 22, 2010 4:05 PM
[Help](#) [Log off](#)

Home / Session Manager / System Status / SIP Entity Monitoring

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

Session Manager Administration

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System State Administration

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Data Replication Status

RegistrationSummary

User Registrations

System Tools

Shortcuts

Change Password

Help for SIP Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Refresh

Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
ASM1-DR	0/10	0	0	0
ASM2-DR	0/3	0	0	0

All Monitored SIP Entities

Refresh

11 Items Filter: Enable

SIP Entity Name
ASM1-DR
ASM2-DR
BCM-50
CUCM 5.x
IPO 500
Nortel-Node_Server
S8300-G450-FS
S8730-CH
SIL-DR-MAS1
SIL-DR-MX1
VPMS

Select the corresponding SIP Entity for the Business Communication Manager from the **All Monitored SIP Entities** table and verify the link is up as shown below:

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 22, 2010 4:05 PM
[Help](#) [Log off](#)

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

Asset Management

Communication System Management

User Management

Monitoring

Network Routing Policy

Security

Applications

Settings

Session Manager

Session Manager Administration

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System State Administration

SIP Entity Monitoring

Managed Bandwidth Usage

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: BCM-50

Refresh Summary View

2 Items Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	ASM2-DR	10.80.48.10	5060	UDP	Up	200 OK	Up
Show	ASM1-DR	10.80.48.10	5060	UDP	Up	200 OK	Up

7.1.3. Verify Registrations of SIP Endpoints

Expand **User Management** on left navigation menu to verify SIP users have been created in the Session Manager. For more information on creating SIP users, see the appropriate documentation in **Section 10**.

In the sample configuration, two SIP users were created as shown in the highlighted area below:

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Dec. 15, 2009 2:03 PM
Help : Log off

Home / User Management / User Management

User Management

Users

View Edit New Duplicate Delete More Actions

Advanced Search

5 Items Refresh Filter: Enable

	Status	Name	User Name	Handle	Last Login
<input type="checkbox"/>		Administrator	administrator@avaya.com		December 7, 2009 7:19:23 PM -06:00
<input type="checkbox"/>		Default Administrator	admin		December 15, 2009 10:30:29 PM -06:00
<input type="checkbox"/>		John Smith	6663000@avaya.com	6663000	
<input type="checkbox"/>		Jones, Paul	6663001@avaya.com	6663001	
<input type="checkbox"/>		System User	system		

Select : All, None (0 of 5 Selected)

Verify the associated SIP endpoints are registered with Session Manager as shown below:

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 04, 2010 1:38 PM
Help Log off

Home / Session Manager / System Status / User Registrations

User Registrations

Select to send notifications to AST devices. Click on row to display registration detail.

Refresh AST Device Notifications: Reboot Reload

3 Items Refresh Filter: Enable

	Registered	Address	Login Name	First Name	Last Name	Session Manager	AST Device
<input checked="" type="checkbox"/>	true	6663000@avaya.com	6663000@avaya.com	John	Smith	ASM1-DR	true
<input type="checkbox"/>	true	6663001@avaya.com	6663001@avaya.com	Paul	Jones	ASM1-DR	true
<input type="checkbox"/>	false	Administrator@avaya.com	administrator@avaya.com	SIL	Administrator	ASM1-DR	false

Select : All, None (1 of 3 Selected)

Registration Detail

Login Name: 6663000@avaya.com

Registration Address: 6663000@avaya.com

Registration Time: Wed Dec 16 13:41:47 MST 2009

Event Subscriptions:

- avaya-cm-feature-status
- dialog
- avaya-ccs-profile
- message-summary
- reg

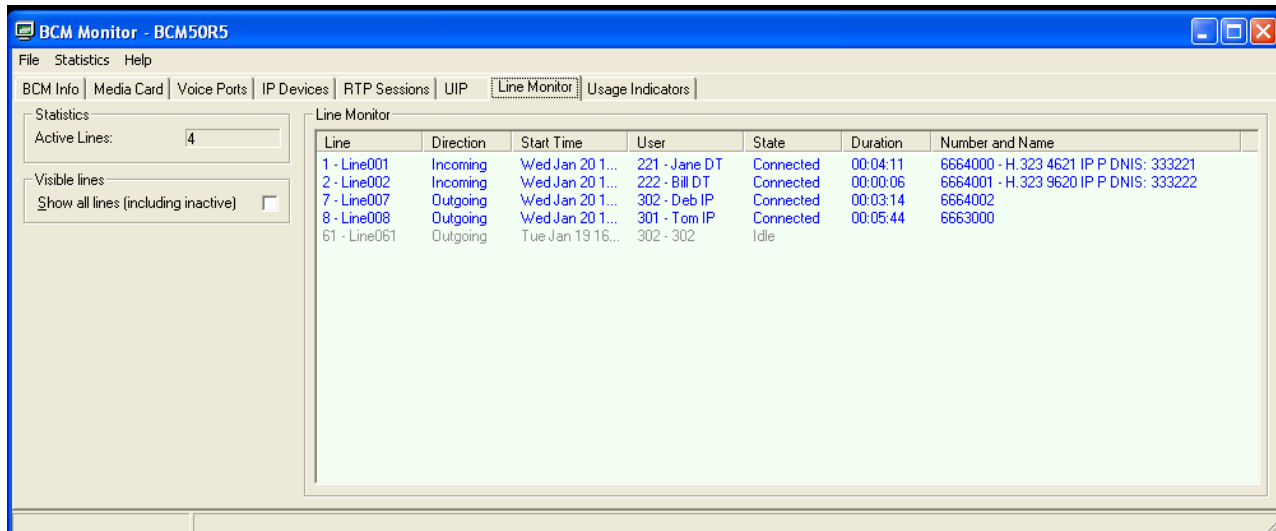
User Communication Profile Addresses: 6663000@avaya.com

7.2. Verify Avaya Business Communication Manager Configuration

The Business Communication Monitor application monitors the status of SIP trunk calls.

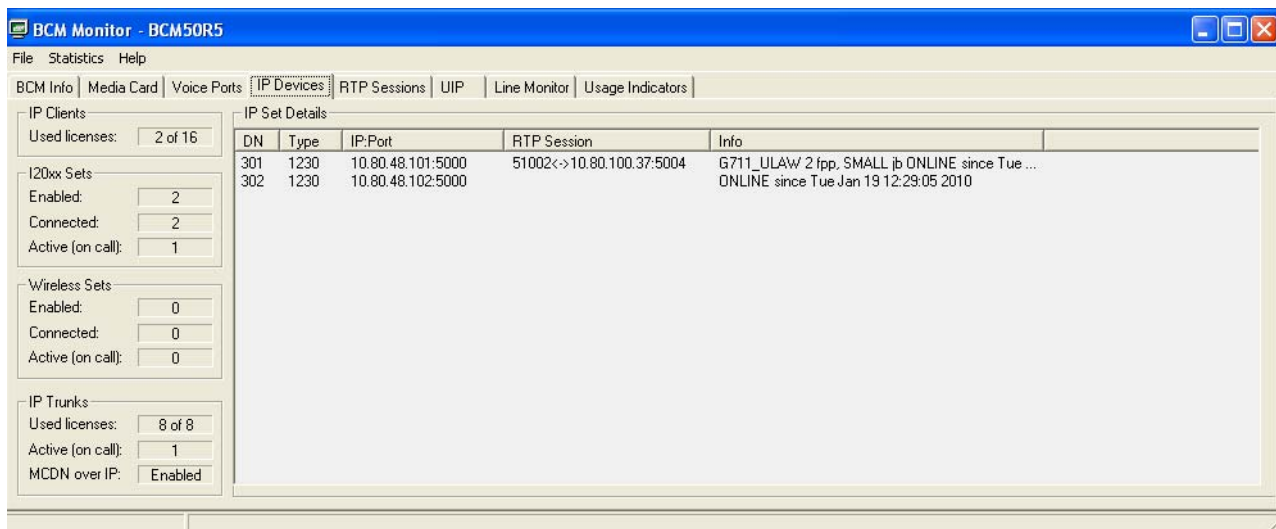
Log in with the appropriate credentials and navigate to the **Line Monitor** tab to see the status of the SIP trunk.

The following screen shows 4 calls active calls between Business Communication Manager and stations on Communication Manager:



Line	Direction	Start Time	User	State	Duration	Number and Name
1 - Line001	Incoming	Wed Jan 20 1...	221 - Jane DT	Connected	00:04:11	6664000 - H.323 4621 IP P DNIS: 333221
2 - Line002	Incoming	Wed Jan 20 1...	222 - Bill DT	Connected	00:00:06	6664001 - H.323 9620 IP P DNIS: 333222
7 - Line007	Outgoing	Wed Jan 20 1...	302 - Deb IP	Connected	00:03:14	6664002
8 - Line008	Outgoing	Wed Jan 20 1...	301 - Tom IP	Connected	00:05:44	6663000
61 - Line061	Outgoing	Tue Jan 19 16...	302 - 302	Idle		

Use the **IP Devices** tab to monitor individual IP stations. For example, the screen below provides status of an active call from a SIP endpoint using extension 6663000 to station 301:



DN	Type	IP:Port	RTP Session	Info
301	1230	10.80.48.101:5000	51002<->10.80.100.37:5004	G711_ULAW/2 fpp, SMALL jb ONLINE since Tue ...
302	1230	10.80.48.102:5000		ONLINE since Tue Jan 19 12:29:05 2010

7.3. Verify Avaya Aura™ Communication Manager Feature Server

Verify the status of the SIP trunk group by using the **status trunk n** command, where **n** is the trunk group number administered in **Section 3.4.2**.

Verify that all trunks are in the “in-service/idle” state as shown below:

status trunk 10			
TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0010/001	T00006	in-service/idle	no
0010/002	T00007	in-service/idle	no
0010/003	T00008	in-service/idle	no
0010/004	T00009	in-service/idle	no
0010/005	T00014	in-service/idle	no
0010/006	T00015	in-service/idle	no
0010/007	T00043	in-service/idle	no
0010/008	T00044	in-service/idle	no
0010/009	T00045	in-service/idle	no
0010/010	T00046	in-service/idle	no

Verify the status of the SIP signaling groups by using the **status signaling-group n** command, where **n** is the signaling group number administered in **Section 3.5.1**.

Verify the signaling group is “in-service” as indicated in the **Group State** field shown below:

status signaling-group 10	
STATUS SIGNALING GROUP	
Group ID: 10	Active NCA-TSC Count: 0
Group Type: sip	Active CA-TSC Count: 0
Signaling Type: facility associated signaling	
Group State: in-service	

Use the SAT command, **list trace tac #**, where **tac #** is the trunk access code to trace trunk group activity for the SIP trunk between Session Manager and Communication Manager Feature Server as shown below:

list trace tac #10		Page 1
LIST TRACE		
time	data	
11:44:50	Calling party station 6663000 cid 0x27f	
11:44:50	Calling Number & Name 6663000 John Smith	
11:44:50	active station 6663000 cid 0x27f	
11:44:59	dial 333301 route:AAR	
11:44:59	term trunk-group 10 cid 0x27f	
11:44:59	dial 333301 route:AAR	
11:44:59	route-pattern 10 preference 1 cid 0x27f	
11:44:59	seize trunk-group 10 member 7 cid 0x27f	
11:44:59	Calling Number & Name NO-CPNumber NO-CPName	
11:44:59	Setup digits 333301	
11:44:59	Calling Number & Name 6663000 John Smith	
11:44:59	Proceed trunk-group 10 member 7 cid 0x27f	
11:44:59	Alert trunk-group 10 member 7 cid 0x27f	
11:44:59	G711MU ss:off ps:20	
	rgn:1 [10.80.100.37]:5004	

On Communication Manager Feature Server, use the CM SAT, **list trace station xxx**, where **xxx** is the extension number of the 9600 Series SIP telephone as shown below:

list trace station 6663000		Page 1
LIST TRACE		
time	data	
11:46:35	active station 6663000 cid 0x282	
11:46:44	dial 333301 route:AAR	
11:46:44	term trunk-group 10 cid 0x282	
11:46:44	dial 333301 route:AAR	
11:46:44	route-pattern 10 preference 1 cid 0x282	
11:46:44	seize trunk-group 10 member 8 cid 0x282	
11:46:44	Calling Number & Name NO-CPNumber NO-CPName	
11:46:44	Setup digits 333301	
11:46:44	Calling Number & Name 6663000 John Smith	
11:46:44	Proceed trunk-group 10 member 8 cid 0x282	
11:46:44	Alert trunk-group 10 member 8 cid 0x282	
11:46:44	G711MU ss:off ps:20	
	rgn:1 [10.80.100.37]:5004	
	rgn:1 [10.80.100.53]:2060	
11:46:44	xoip options: fax:Relay modem:off tty:US uid:0x50006	
	rgn:1 [10.80.100.37]:5004 cid 0x27f7fe	

Perform similar actions to verify the status of Communication Manager Access Element.

7.4. Verify Status of Avaya Modular Messaging

Log in with the proper credentials to the web page used to manage the MSS and select **Reports** → **Messaging Measurements** task from the navigation menu.

On the **Messaging Measurements** page, select the type of report to obtain traffic and other usage statistics for the system.

The screen below shows the results of running a **Feature** report for the sample configuration:

The screenshot displays the Avaya Messaging Measurements web interface. On the left is a navigation menu with categories like Messaging Administration, Server Administration, IMAP/SMTP Administration, Utilities, Logs, Reports, Diagnostics, Software Management, Security, Alarming, and Backup/Restore. The main content area is titled "Messaging Measurements" and includes filters for Type (Feature), Cycle (Daily), and Start Date (April 16, 2010, 00:00). Below these are buttons for "Get Report", "Help", "Previous Day", "Clear Report", and "Next Day". The report title "FEATURE DAILY TRAFFIC" is prominently displayed. The report data is organized into three main sections: REMOTE SUBSCRIBERS, VOICE MAIL, and CALL ANSWER, each with a table of metrics.

REMOTE SUBSCRIBERS		
Administered	Non Administered	
0	0	

VOICE MAIL		
	Number Sent	Current
Total Messages	8	0
Voice Components	0	0
FAX Components	0	0
Binary Attachments	8	0
Text Components	8	0
Broadcast Messages	0	0
Login Announcements	0	0
Urgent Messages	0	0
Private Messages	0	0
Minutes		
Average Storage Time	277	

CALL ANSWER		
	Number Received	Current
Total Messages	1	20
Voice Components	0	18
FAX Components	0	0
Minutes		
Average Storage Time	0	

7.5. Call Scenarios Verified

Verification scenarios for the configuration described in these Application Notes included the following call scenarios:

Note: All stations in the configuration were administered as subscribers on Modular Messaging and were configured to cover to Modular Messaging in the event of busy and no-answer scenarios.

Basic Voice Mail Features:

- Verified different types of stations on Communication Manager could leave a Voice Mail message for stations on Business Communication Manager for both busy and no-answer scenarios.
- Verified the Message Waiting Indication was enabled for new Voice Mail messages.
- Verified stations on Business Communication Manager could leave a Voice Mail message for different types of stations on Communication Manager for both busy and no-answer scenarios.
- Verified stations on Business Communication Manager could access Modular Messaging to retrieve new Voice Mail messages. Verified the Message Waiting Indication was disabled when all new Voice Mail messages are retrieved.

Advanced Modular Messaging Features:

- Verify different types of stations on Communication Manager could use advanced Modular Messaging features such as Auto-Attendant feature or Call Sender to place calls to stations on Business Communication Manager.
- Verified stations on Business Communication Manager could use advanced Modular Messaging features such as Auto-Attendant or Call Sender to place calls to different types of stations on Communication Manager.
- Verified stations on Business Communication Manager could activate Modular Messaging Find-Me feature.

Long Duration Messages :

- Verified different types of station on Communication Manager could leave long Voice Mail messages for stations on Business Communication Manager for both busy and no-answer scenarios.
- Verified stations on Business Communication Manager could leave a long Voice Mail message for different types of stations on Communication Manager for both busy and no-answer scenarios.
- Verified stations on Business Communication Manager could access Modular Messaging to retrieve long Voice Mail messages.

Fax Scenarios:

- Verified an analog fax machine on Communication Manager could send a fax document to the mailbox for a station on Business Communication Manager.
- Verified the Message Waiting Indication was enabled when a new fax document is received. Verified the user could retrieve the fax document.

- Verified an analog fax machine on Business Communication Manager can send a fax document to the mailbox for a station on Communication Manager.
- Verified an analog fax machine on Communication Manager Access Element could send a multi-page fax document to the mailbox for a station on Business Communication Manager.
- Verified an analog fax machine on Business Communication Manager could send a multi-page fax document to the mailbox for a station on Communication Manager.

7.6. Issues Found and Known Limitations

All test calls of Modular Message Features for stations on Business Communication Manager were successful. The following issues were observed during testing:

- There were some issues with displays when calls were forwarded to Modular Messaging.
Note: The display issues on the Business Communication Manager stations have been identified as known limitations since the proprietary MCDN networking features are not yet supported on standard SIP trunks.
- Calls to stations on Business Communication Manager with the Modular Messaging Find-Me feature enabled were successful if the Find-Me number was an external number.
Note: this issue is under investigation.
- There were some issues when Avaya IP H.323 stations on Communication Manager Access Element used advanced Modular Messaging features to place calls to stations on Business Communication Manager.
Note: these issues are under investigation. However, if IP-Shuffling is disabled on the Communication Manager Access Element, all test calls were successful.
- It was not possible to use an analog fax machine connected to Business Communication Manager to send fax documents to a Modular Messaging mailbox. A second issue was found when sending fax documents containing 4 or more pages to the Modular Messaging mailbox for a station on Business Communication Manager.
 - **Note:** these issues are under investigation.

8. Conclusions

These Application Notes describe how to configure a network that uses SIP trunks between Avaya Business Communication Manager Release 5.0, Avaya AuraTM Session Manager Release 5.2, Avaya Modular Messaging Release 5.2, Avaya AuraTM Communication Manager Access Element Release 5.2.1 and a second Avaya AuraTM Communication Manager operating as a Feature Server. Interoperability testing included verification of calls from several different types of endpoints including analog fax machines forwarded to Modular Messaging.

9. Acronyms

AAR	Automatic Alternative Routing (Routing on Communication Manager)
ARS	Automatic Route Selection
CLAN	Control LAN (Control Card in Communication Manager)
DCP	Digital Communications Protocol
DNIS	Dialed Number Identification Service
DHCP	Dynamic Host Configuration Protocol
DTMF	Dual Tone Multi Frequency
FQDN	Fully Qualified Domain Name (hostname for Domain Naming Resolution)
GUI	Graphical User Interface
IMS	IP Multimedia Subsystem
IE	Internet Explorer
IP	Internet Protocol
IPSI	IP-services interface (Control Card in Communication Manager)
LAN	Local Area Network
MCDN	Meridian Customer Defined Network MCDN is a heritage Nortel proprietary ISDN-PRI signaling protocol and provides networking features such as Calling Party Name Display, Network Messaging Services and Message Waiting Indication
OAM	Operation, Administration and Maintenance
PSTN	Public Switched Telephone Network
RTP	Real Time Protocol
SAT	System Access Terminal (Communication Administration Interface)
SIL	Solution Interoperability Lab
SIP	Session Initiation Protocol
SM	Avaya Aura TM Session Manager
SMGR	System Manager (used to configure Session Manager)
SNMP	Simple Network Management Protocol
SRE	SIP Routing Element
SSH	Secure Shell
SSL	Secure Socket Layer
TAC	Trunk Access Code (Communication Manager Trunk Access)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URE	User Relation Element
URL	Uniform Resource Locator
WAN	Wide Area Network
XML	eXtensible Markup Language

10. Additional References

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

Session Manager

- 1) Avaya Aura™ Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>.
- 2) Installing and Administering Avaya Aura™ Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>.
- 3) Avaya Aura™ Session Manager Case Studies, dated January 2, 2010, available at <http://support.avaya.com>
- 4) Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

Communication Manager

- 5) Hardware Description and Reference for Avaya Aura™ Communication Manager (COMCODE 555-245-207)
http://support.avaya.com/elmodocs2/comm_mgr/r4_0/avayadoc/03_300151_6/245207_6/245207_6.pdf
- 6) SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers, Doc ID 555-245-206, May 2009, available at <http://support.avaya.com>.
- 7) Administering Avaya Aura™ Communication Manager, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.
- 8) Avaya Toll Fraud Security Guide, Doc ID 555-025-600, February 2010, available at <http://support.avaya.com>
- 9) Administering Avaya Aura™ Communication Manager as a Feature Server, Doc ID 03-603479, November 2009, available at <http://support.avaya.com>

Business Communication Manager

- 10) BCM50 Administration Guide, Doc ID NN40020-600_02, available at <http://support.nortel.com>
- 11) BCM50 Networking Configuration Guide, Doc ID NN40020-603, available at <http://support.nortel.com>
- 12) BCM50 Device Configuration Guide, Doc ID NN400200-300, available at <http://support.nortel.com>
- 13) IP Phone 1200 Series Installation, Doc ID NN40050-302, available at <http://support.nortel.com>
- 14) Business Communications Manager 5.0 Administration and Security Guide, Doc ID NN40170-603, Rev 02.06, available at <http://support.nortel.com>
- 15) Business Communications Manager 5.0 Installation Checklist and Quick Start Guide, Doc ID NN40170-302, Rev 02.01, available at <http://support.nortel.com>
- 16) Business Communications Manager 5.0 – Configuration – System, Doc ID NN40170-501, Rev 02.04, available at <http://support.nortel.com>

Avaya Modular Messaging

- 17) Avaya Modular Messaging for the Message Storage Server Configuration, Release 5.2, Installation and Upgrades Guide, November 2009, available at <http://support.avaya.com>
- 18) Avaya Modular Messaging Release 5.2 with Avaya MSS, Messaging Application Server Administration Guide, November 2009, available at <http://support.avaya.com>

Avaya Application Notes

- 19) Configuring 9600 Series SIP Phones on Avaya Aura™ Session Manager Release 5.2, available at <http://www.avaya.com>
- 20) Configuring multiple Avaya Aura™ Session Managers to address different Network Failure Scenarios, available at <http://support.avaya.com>
- 21) Configuring SIP Trunks among Business Communication Manager 50, Avaya Aura™ Session Manager 5.2 and Avaya Aura™ Communication Manager, available at <http://www.avaya.com>
- 22) Configuring SIP Trunks among Avaya Aura™ Session Manager 5.2, Avaya IP Office, and Communication Server 1000E6.0, available at <http://www.avaya.com>

©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