



Avaya Solution & Interoperability Test Lab

Front-Ending Avaya Communication Server 1000 R4.5 with an Avaya G450 Media Gateway Controlled by Avaya Aura™ Communication Manager 5.2.1 to Support SIP Trunks to Avaya Aura™ Session Manager 5.2 and Avaya Modular Messaging 5.2 – Issue 1.0

Abstract

These Application Notes present a sample configuration that uses an Avaya G450 Media Gateway as a PRI-QSIG/SIP gateway to connect Avaya Communication Server 1000 R4.5 (formerly known as Nortel Communication Server 1000) with Avaya Aura™ Session Manager 5.2, which in turn provides call routing support to other Avaya SIP products such as Avaya Modular Messaging 5.2.

For the sample configuration, Session Manager runs on an Avaya S8510 Server, Communication Manager runs on Avaya S8720 servers, and Avaya Communication Server 1000 runs on Avaya Communication Server 1000S. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Communication Manager.

1 Introduction

Previous Avaya Application Notes [9] describe how Release 4.5 Avaya Communication Server 1000 (formerly known as Nortel Communication Server 1000 and hereafter referred to as the CS1000) can be directly integrated with Avaya Aura™ Session Manager using SIP trunks. While effective in terms of supporting basic and supplementary call features, this configuration does have some limitations in areas such as DTMF support and call coverage¹. There are also many installations of the CS1000 which are not SIP or IP capable. In these cases, an effective solution is to front-end the CS1000 with a PRI-QSIG/SIP gateway, which then signals on SIP trunks to Session Manager. This configuration supports basic and supplementary call features as well as RFC 2833 DTMF and message-waiting signaling for applications such as voice messaging. See [10] for one example of this technique using an AudioCodes Mediant 1000 Modular Media Gateway.

The sample configuration shown in **Figure 1** illustrates another example of front-ending using an Avaya G450 Media Gateway as the PRI-QSIG/SIP gateway. The G450 Media Gateway is controlled by Avaya Aura™ Communication Manager, which supports SIP trunks to the SM-100 (Security Module) network interface of Session Manager, which in turn performs call routing to Avaya Modular Messaging. Session Manager can support flexible inter-system call routing based on dialed number, calling number and system location, and can also provide protocol adaptation to allow multi-vendor systems to interoperate. It is managed by a separate Avaya Aura™ System Manager, which can manage multiple Session Managers by communicating with their management network interfaces. Modular Messaging expands the capabilities and features of messaging services. Centralized messaging enables the local Modular Messaging system to provide voicemail service to subscribers at both sites in a multi-site configuration.

For the sample configuration, Session Manager runs on an Avaya S8510 Server, Communication Manager runs on Avaya S8720 servers, and the CS1000 runs on Avaya Communication Server 1000S. These Application Notes should apply to other Avaya servers and Media Gateways running Communication Manager.

As shown in **Figure 1**, Communication Manager controls the G450 Media Gateway, Avaya 9630 IP Telephone (H.323), and 6408D+ Digital Telephone. The CS1000 controls the Avaya i2004 IP Telephone and 3904 Digital Telephone (formerly sold under the Nortel label). A five digit Uniform Dial Plan (UDP) is used for dialing between systems. Unique extension ranges are associated with Communication Manager (3xxxx) and Avaya Communication Server 1000 (53xxx). Session Manager routes calls based on this five digit plan, using an adaptation module to convert to the normalized eleven digit plan used in Modular Messaging.

These Application Notes will focus on configuration of the QSIG trunks, SIP trunks, dial plan support, call routing, and call coverage for voice messaging. Detailed administration of the endpoint telephones will not be described (see the appropriate documentation listed in **Section 9**).

¹ These limitations are resolved in later releases of Avaya Communication Server 1000.

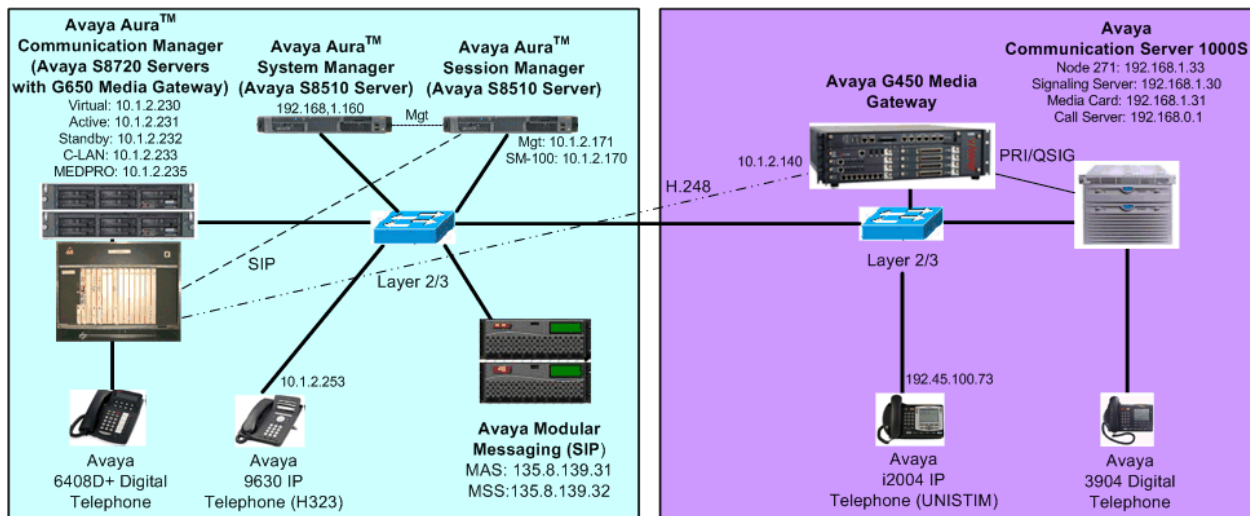


Figure 1 – Sample Configuration

2 Equipment and Software Validated

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

Hardware Component	Software Version
Avaya S8720 Servers with G450 and G650 Media Gateways	Avaya Aura™ Communication Manager 5.2.1, Load 16.4, Update 17774
Avaya S8510 Server	Avaya Aura™ Session Manager 5.2 SP 0, Load 5.2.0.1.520017
	Avaya Aura™ System Manager 5.2 Load 5.2.0.7.11 VSP patch 1.1.0.4.8
Avaya 9630 IP Telephone (H.323)	3.1
Avaya 6408D+ Digital Telephone	-
Avaya Modular Messaging Storage Server	5.2, Build 5.2-11.0
Avaya Modular Messaging Application Server	5.2, Build 5.2.150.13 (Patch 520008)
Avaya Communication Server 1000S <ul style="list-style-type: none"> Call Server Signaling Server NTRB21 DTI/PRI TMDI Card 	Avaya Communication Server 1000 Release 450w, Version 2121 sse-4.50.88 NA
Avaya (formerly Nortel) 3904 Digital Telephone	NA
Avaya (formerly Nortel) I2004 IP Telephone (UNISTIM)	C502B41

3 Configure Avaya Aura™ Communication Manager

This section describes configuring Communication Manager in the following areas. Some administration screens have been abbreviated for clarity.

- Avaya Communication Manager license
- System parameters features
- IP node names
- IP interface
- IP codec set and network region
- G450 Media Gateway
- DS1 Interface
- PRI QSIG signaling group and trunk group
- SIP signaling group and trunk group
- Route pattern
- Location and public/private numbering
- Uniform dial plan and AAR analysis
- Voice messaging hunt group
- Voice messaging coverage path
- Sample station form specifying voice messaging coverage path

3.1 Verify Avaya Aura™ Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

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

display system-parameters customer-options		Page	2 of	10
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		800	200	
Maximum Concurrently Registered IP Stations:		18000	2	
Maximum Administered Remote Office Trunks:		0	0	
Maximum Concurrently Registered Remote Office Stations:		0	0	
Maximum Concurrently Registered IP eCons:		0	0	
Max Concur Registered Unauthenticated H.323 Stations:		0	0	
Maximum Video Capable H.323 Stations:		0	0	
Maximum Video Capable IP Softphones:		0	0	
Maximum Administered SIP Trunks:		800	47	

3.2 Configure System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers. Submit the change.

This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented using Class Of Restriction or Class Of Service levels. Refer to the appropriate documentation in **Section 9** for more details.

change system-parameters features	Page 1 of 18
FEATURE-RELATED SYSTEM PARAMETERS	
Self Station Display Enabled? y	
Trunk-to-Trunk Transfer: all	
Automatic Callback with Called Party Queuing? n	
Automatic Callback - No Answer Timeout Interval (rings): 3	
Call Park Timeout Interval (minutes): 10	
Off-Premises Tone Detect Timeout Interval (seconds): 20	
DID/Tie/ISDN/SIP Intercept Treatment: attd	
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred	

3.3 Configure IP Node Names

Use the “change node-names ip” command to add entries for the C-LAN that will be used for signaling, its default gateway, and Session Manager. In this case, “clan1” and “10.1.2.233” are entered as **Name** and **IP Address** for the C-LAN, “sm1” and “10.1.2.170” are entered for the Session Manager Security Module (SM-100) interface, and “Gateway001” and “10.1.2.1” are entered for the default gateway. Note that “Gateway001” will be used to configure the IP interface for the C-LAN (see **Section 3.4**). The actual node names and IP addresses may vary. Submit these changes.

change node-names ip	Page 1 of 2
IP NODE NAMES	
Name	IP Address
clan1	10.1.2.233
Gateway001	10.1.2.1
sm1	10.1.2.170

3.4 Configure IP Interface for C-LAN

Add the C-LAN to the system configuration using the “add ip-interface 1a02” command. The actual slot number may vary. In this case, “1a02” is used as the slot number. Enter the C-LAN node name assigned from **Section 3.3** into the **Node Name** field.

Enter proper values for the **Subnet Mask** and **Gateway Node Name** fields. In this case, “24” and “Gateway001” are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** and **Allow H.323 Endpoints** fields to “y”. Default values may be used in the remaining fields. Submit these changes.

add ip-interface 1a02		Page 1 of 3
IP INTERFACES		
Type: C-LAN	Target socket load and Warning level: 400	
Slot: 01A02	Receive Buffer TCP Window Size: 8320	
Code/Suffix: TN799 D		
Enable Interface? y	Allow H.323 Endpoints? y	
VLAN: n	Allow H.248 Gateways? y	
Network Region: 1	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: clan1		
Subnet Mask: /24		
Gateway Node Name: Gateway001		
Ethernet Link: 2		
Network uses 1's for Broadcast Addresses? y		

3.5 Configure IP Codec Set and Network Region

Configure the IP codec set to use for calls to the Avaya Communication Server 1000 via Session Manager. Use the “change ip-codec-set n” command, where “n” is an existing codec set number to be used for interoperability. Enter the desired audio codec type in the **Audio Codec** field. Retain the default values for the remaining fields and submit these changes.

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:			
3:			

In the test configuration, network region “1” was used for calls to Session Manager. Use the “change ip-network-region 1” command to configure this network region. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise network (See **Section 4.1**). This value is used to populate the SIP domain in the From header of SIP INVITE messages for outbound calls. It also must match the SIP domain in the request URI of incoming INVITEs from other systems. Enter a descriptive **Name**. For the **Codec Set** field, enter the corresponding audio codec set configured above in this section. Enable the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio**. These settings will enable direct media between Avaya IP telephones. Retain the default values for the remaining fields, and submit these changes.

```
change ip-network-region 1                                     Page 1 of 19
                                IP NETWORK REGION
Region: 1
Location:      Authoritative Domain: avaya.com
Name: ASM
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: 10001
DIFFSERV/TOS PARAMETERS                                RTCP Reporting Enabled? y
Call Control PHB Value: 46                        RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46                                Use Default Server Parameters? y
Video PHB Value: 26
```

3.6 Add G450 Media Gateway

The Avaya G450 Media Gateway is used to support the PRI QSIG trunk connection to the CS1000. Install and configure the G450 Media Gateway as described [6], noting its serial number, and specifying the IP address of the C-LAN configured in **Section 3.3** in its controller list. The following screen shows the G450 Media Gateway Command Line Interface commands to obtain the serial number (**show system**), and to set and verify the controller list (**set mgc list**, **show mgc list**):

```
G450-FE-???(super)# show system
System Name      :
System Location  :
System Contact    :
Uptime (d,h:m:s) : 46,21:32:25
MV Time          : 09:51:53 11 MAR 2010
Serial No       : 08IS38199678
Model           : G450
.
.
.
G450-FE-???(super)# set mgc list 10.1.2.233
Done!
G450-FE-???(super)# show mgc list

CONFIGURED MGC HOST
-----
10.1.2.233
-- Not Available --
-- Not Available --
-- Not Available --
```

On Communication Manager, use the “add media-gateway n” command, where “n” is an unused media gateway number. Enter the following values for the specified fields, and retain the default values for all remaining fields. Submit these changes.

- **Type:** “g450”
- **Name:** A descriptive name.
- **Serial No:** Serial number obtained from the G450 media gateway above

```
add media-gateway 1                                     Page 1 of 1

                                MEDIA GATEWAY
      Number: 1                                Registered? n
      Type: g450                                FW Version/HW Vintage:
      Name: Avaya CS1000                        MGP IP Address:
      Serial No: 08IS38199678                  Controller IP Address:
      Encrypt Link? y                          MAC Address:
      Network Region: 1      Location: 1
      Recovery Rule: none

      Site Data:

Slot  Module Type      Name      DSP Type  FW/HW version
V1:
V2:
V3:
```

Make sure that the DS1 interface card (MM710) is installed in the desired slot in the gateway. When the media gateway is registered with Communication Manager, the DS1 interface should be displayed in that slot, as shown below for the sample configuration.

```
display media-gateway 1

                                MEDIA GATEWAY
      Number: 1                                Registered? y
      Type: g450                                FW Version/HW Vintage: 30 .10 .4 /1
      Name: Avaya CS1000                        MGP IP Address: 10 .1 .2 .140
      Serial No: 08IS38199678                  Controller IP Address: 10 .1 .2 .233
      Encrypt Link? y                          MAC Address: 00:1b:4f:03:52:18
      Network Region: 1      Location: 1
      Recovery Rule: none

      Site Data:

Slot  Module Type      Name      DSP Type  FW/HW version
V1:   MM710           DS1 MM      MP80      29 3
V2:
V3:
```


3.7 Add DS1 Interface

The DS1 circuit pack is used for connectivity to the CS1000. Use the “add ds1 1v1” command. Note that the actual slot number may vary. In this case “1v1” is used as the slot number (see **Section 3.6**). Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Name:** A descriptive name.
- **Line Coding:** “b8zs”
- **Framing Mode:** “esf”
- **Signaling Mode:** “isdn-pri”
- **Connect:** “pbx”
- **Interface:** “peer-slave”
- **Peer Protocol:** “Q-SIG”

The **Interface** field must be complementary on both switches. For the sample configuration, Communication Manager is administered as the *peer-slave*, and the CS1000 is administered as the *peer-master* (note that **Reference** [11] shows the opposite relationship).

add ds1 01v1		Page 1 of 2
DS1 CIRCUIT PACK		
Location: 001V1	Name: Avaya CS1000	
Bit Rate: 1.544	Line Coding: b8zs	
Line Compensation: 1	Framing Mode: esf	
Signaling Mode: isdn-pri	Interface: peer-slave	
Connect: pbx	Peer Protocol: Q-SIG	
TN-C7 Long Timers? n	Side: b	
Interworking Message: PROgress	CRC? n	
Interface Companding: mulaw		
Idle Code: 11111111		
DCP/Analog Bearer Capability: 3.1kHz		

3.8 Add PRI QSIG Signaling Group and Trunk Group

Configure an ISDN trunk group to interface with the CS1000. Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “isdn”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Direction:** “two-way”
- **Carrier Medium:** “PRI/BRI”
- **Service Type:** “tie”

add trunk-group 100		Page 1 of 21
TRUNK GROUP		
Group Number: 100	Group Type: isdn	CDR Reports: y
Group Name: Avaya CS1000	COR: 1	TN: 1 TAC: 100
Direction: two-way	Outgoing Display? n	Carrier Medium: PRI/BRI
Dial Access? n	Busy Threshold: 255	Night Service:
Queue Length: 0		
Service Type: tie	Auth Code? n	TestCall ITC: rest
	Far End Test Line No:	

Navigate to **Page 2**. For the **Supplementary Service Protocol** field, enter “b” for QSIG. Retain the default values for the remaining fields.

add trunk-group 100		Page 2 of 21
Group Type: isdn		
TRUNK PARAMETERS		
Codeset to Send Display: 6	Codeset to Send National IEs: 6	
Max Message Size to Send: 260	Charge Advice: none	
Supplementary Service Protocol: b	Digit Handling (in/out): enbloc/enbloc	
Trunk Hunt: cyclical		
		Digital Loss Group: 13
Incoming Calling Number - Delete:	Insert:	Format:
Bit Rate: 1200	Synchronization: async	Duplex: full
Disconnect Supervision - In? y Out? y		
Answer Supervision Timeout: 0		
Administer Timers? n	CONNECT Reliable When Call Leaves ISDN? n	

Navigate to **Page 3**. Enable the **Send Name**, **Send Calling Number**, and **Send Connected Number** fields. For the **Format** field, enter “unk-pvt” to construct the calling and connected numbers using the “private numbering” table, but encode the numbering plan format as “unknown” in the ISDN messages toward the CS1000. Setting the **Internal Alert** field to “y” allows calls arriving from CS1000 users to be treated as internal calls. For example, if a CS1000 telephone dials a Communication Manager telephone, the Communication Manager telephone will ring with the ring pattern for an internal station-station call, internal coverage criteria will apply, and the CS1000 caller will hear tones such as coverage tone, similar to a call between Communication Manager telephones.

add trunk-group 100		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Wideband Support? n
	Internal Alert? y	Maintenance Tests? y
	Data Restriction? n	NCA-TSC Trunk Member:
	Send Name: y	Send Calling Number: y
Used for DCS? n	Hop Dgt? n	Send EMU Visitor CPN? n
Suppress # Outpulsing? n	Format: unk-pvt	
Outgoing Channel ID Encoding: preferred	UII IE Treatment: service-provider	
	Replace Restricted Numbers? y	
	Replace Unavailable Numbers? n	
	Send Connected Number: y	
	Hold/Unhold Notifications? y	
	Modify Tandem Calling Number? n	
Send UII IE? y		
Send UCID? n		
Send Codeset 6/7 LAI IE? y	Dsl Echo Cancellation? n	
Apply Local Ringback? n		
Show ANSWERED BY on Display? y		
	Network (Japan) Needs Connect Before Disconnect? n	

3.8.1 Signaling Group

Configure an ISDN signaling group for the new trunk group. Use the “add signaling-group n” command, where “n” is an available signaling group number. For the **Primary D-Channel** field, enter the slot number for the DS1 module from **Section 3.7** and port “24”.

For the **Trunk Group for NCA TSC** and **Trunk Group for Channel Selection** fields, enter the ISDN trunk group number from **Section 3.8**. For the **Supplementary Service Protocol** field, enter “b” for QSIG. Maintain the default values for the remaining fields, and submit these changes.

add signaling-group 100		Page 1 of 1
SIGNALING GROUP		
Group Number: 100	Group Type: isdn-pri	
Associated Signaling? y	Max number of NCA TSC: 10	
Primary D-Channel: 001V124	Max number of CA TSC: 0	
	Trunk Group for NCA TSC: 100	
Trunk Group for Channel Selection: 100		
TSC Supplementary Service Protocol: b	Network Call Transfer? n	

3.8.2 Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number added in **Section 3.8**. Navigate to **Page 4**. Shown below are default values that were used during testing. If the Communication Manager Auto Callback feature will be used with CS1000 users, then the **TSC Method for Auto Callback** field must be set to “always-retain”, as shown in bold below.

change trunk-group 100	Page 4 of 21
QSIG TRUNK GROUP OPTIONS	
TSC Method for Auto Callback: always-retain	
Diversions by Reroute? y	
Path Replacement? y	
Path Replacement with Retention? n	
Path Replacement Method: better-route	
SBS? n	
Display Forwarding Party Name? y	
Character Set for QSIG Name: eurofont	
QSIG Value-Added? n	

Navigate to **Pages 5 and 6**. Enter all 23 ports of the DS1 module into the **Port** fields, and the corresponding **Code** and **Sfx** fields will be populated automatically. Enter the ISDN signaling group number from **Section 3.8.1** into the **Sig Grp** fields as shown below. Submit these changes.

change trunk-group 100	Page 5 of 21
TRUNK GROUP	
Administered Members (min/max): 1/23	
Total Administered Members: 23	
GROUP MEMBER ASSIGNMENTS	
Port	Code Sfx Name Night Sig Grp
1: 001V101	MM710 100
2: 001V102	MM710 100
3: 001V103	MM710 100
4: 001V104	MM710 100
5: 001V105	MM710 100
6: 001V106	MM710 100
7: 001V107	MM710 100
8: 001V108	MM710 100
9: 001V109	MM710 100
10: 001V110	MM710 100
11: 001V111	MM710 100
12: 001V112	MM710 100
13: 001V113	MM710 100
14: 001V114	MM710 100
15: 001V115	MM710 100

change trunk-group 100				Page 6 of 21	
TRUNK GROUP				Administered Members (min/max): 1/23	
GROUP MEMBER ASSIGNMENTS				Total Administered Members: 23	
	Port	Code Sfx	Name	Night	Sig Grp
16:	001V116	MM710			100
17:	001V117	MM710			100
18:	001V118	MM710			100
19:	001V119	MM710			100
20:	001V120	MM710			100
21:	001V121	MM710			100
22:	001V122	MM710			100
23:	001V123	MM710			100

3.9 Configure SIP Signaling Group and Trunk Group

3.9.1 SIP Signaling Group

In the test configuration, trunk group “32” and signaling group “32” were used to reach Session Manager. Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields, and retain the default values for all remaining fields. Submit these changes.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** C-LAN node name from **Section 3.3**.
- **Far-end Node Name:** Session Manager node name from **Section 3.3**.
- **Near-end Listen Port:** “5061”
- **Far-end Listen Port:** “5061”
- **Far-end Network Region:** Network region number “1” from **Section 3.5**.
- **Far-end Domain:** SIP domain name from **Section 4.1**.
- **DTMF over IP:** “rtp-payload”

add signaling-group 32		Page 1 of 1	
SIGNALING GROUP			
Group Number: 32	Group Type: sip		
	Transport Method: tls		
IMS Enabled? n			
Near-end Node Name: clan1		Far-end Node Name: sml	
Near-end Listen Port: 5061		Far-end Listen Port: 5061	
		Far-end Network Region: 1	
Far-end Domain: avaya.com			
Bypass If IP Threshold Exceeded? n			
DTMF over IP: rtp-payload		Direct IP-IP Audio Connections? y	
		IP Audio Hairpinning? n	
Enable Layer 3 Test? n		Direct IP-IP Early Media? n	
Session Establishment Timer(min): 3		Alternate Route Timer(sec): 6	

3.9.2 SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”
- **Number of Members:** The number of SIP trunks allocated for calls routed to Session Manager (must be within the limits of the total trunks configured in **Section 3.1**).

add trunk-group 32		Page 1 of 21	
TRUNK GROUP			
Group Number: 32	Group Type: sip	CDR Reports: y	
Group Name: To SM1	COR: 1	TN: 1	TAC: 132
Direction: two-way	Outgoing Display? y		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	Auth Code? n		
Signaling Group: 32			
Number of Members: 4			

Navigate to **Page 3**, and enter “public” for the **Numbering Format** field as shown below. Use default values for all other fields. Submit these changes.

add trunk-group 32		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			

3.10 Configure Route Patterns

Create a route pattern to use for routing calls to the CS1000 using the PRI QSIG trunk. Use the “change route-pattern n” command, where “n” is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The trunk group number from **Section 3.8**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **TSC:** “y” (NCA-TSCs will be used)
- **CA-TSC Request:** “none” (since CA-TSC are used for DCS but not for QSIG)
- **Numbering Format:** “unk-unk” (The numbering format and type of number for the Called Party Number will be encoded as “unknown” toward the CS1000).

change route-pattern 100													Page 1 of 3	
Pattern Number: 100 Pattern Name: Avaya CS1000														
SCCAN? n Secure SIP? n														
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC						
No			Mrk	Lmt	List	Del	Digits	QSIG						
								Dgts	Intw					
1:	100	0											n	user
2:											n	user		
3:											n	user		
4:											n	user		
5:											n	user		
6:											n	user		
BCC VALUE		TSC	CA-TSC	ITC BCIE Service/Feature PARM				No.	Numbering	LAR				
0	1	2	M	4	W	Request		Dgts		Format				
											Subaddress			
1:	y	y	y	y	y	n	y	none	rest		unk-unk	none		
2:	y	y	y	y	y	n	n		rest			none		

Configure a route pattern for routing calls to Session Manager using the SIP trunk group. Use the “change route-pattern n” command, where “n” is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 3.9.2**.
- **FRL:** Enter a level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 32													Page 1 of 3				
Pattern Number: 32 Pattern Name: To ASM																	
SCCAN? n Secure SIP? n																	
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC			
No			Mrk	Lmt	List	Del	Digits						QSIG				
							Dgts						Intw				
1:	32	0											n	user			
2:												n	user				
3:												n	user				
4:												n	user				
5:												n	user				
6:												n	user				
		BCC	VALUE	TSC	CA-TSC			ITC	BCIE	Service/Feature			PARM	No.	Numbering	LAR	
		0	1	2	M	4	W	Request								Dgts	Format
															Subaddress		
1:	y	y	y	y	y	n	n	rest								none	

3.11 Configure Location and Public/Private Numbering

Use the “change locations” command to specify the SIP route pattern to be used as a “default SIP route” for the location corresponding to the Main site. In this way, calls to non-numeric users or unknown domains will still be routed to Session Manager. Add an entry for the Main site if one does not exist already, enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Name:** A descriptive name to denote the Main site.
- **Timezone:** An appropriate timezone offset.
- **Rule:** An appropriate daylight savings rule.
- **Proxy Sel. Rte. Pat.:** The SIP route pattern number from the previous section

change locations															Page 1 of 1	
LOCATIONS																
ARS Prefix 1 Required For 10-Digit NANP Calls? y																
Loc	Name				Timezone	Rule	NPA								Proxy Sel	
No					Offset										Rte Pat	
1:	Main				+ 00:00	0									32	

Use the “change public-unknown-numbering 0” command, to define the calling party number to be sent to Session Manager. Add an entry for the trunk group defined in **Section 3.9.2**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed to trunk group 32 will result in a 5-digit calling number. The calling party number will be in the SIP “From” header. Submit these changes.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	3	32		5	Total Administered: 3
					Maximum Entries: 9999

Use the “change private-numbering” command to define the calling party number to be sent to the CS1000. Add an entry for the trunk group defined in **Section 3.8**. As shown below, all calls originating from a 5-digit extension beginning with 3 and routed to trunk group 100 will result in the 5-digit calling number to be sent. Submit these changes.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
5	3	100		5	Total Administered: 2
					Maximum Entries: 540

3.12 Configure Dial Plan and AAR Analysis

Configure dial plan and Automatic Alternate Routing (AAR) used for routing calls with dialed digits 53xxx to the CS1000 via the G450 Media Gateway and for calls covering to Modular Messaging via hunt group extension 33000. Use the “change uniform-dialplan 0” command, and add an entry to specify use of AAR for routing of digits 53xxx. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Matching Pattern:** Dialed prefix digits to match on, in this case “53”.
- **Len:** Length of the full dialed number.
- **Del:** Number of digits to delete.
- **Net:** “aar”

Add an entry to cover calls that will cover to the voice messaging hunt group extension (33000). Session Manager will route these calls to Modular Messaging. Submit these changes.

change uniform-dialplan 0					Page 1 of 2
UNIFORM DIAL PLAN TABLE					
					Percent Full: 0
Matching			Insert	Node	
Pattern	Len	Del	Digits	Conv	Num
53	5	0	aar	n	
3	5	0	aar	n	

Use the “change aar analysis 0” command, and add corresponding entries to specify use of the SIP trunk for non-extension numbers beginning with 3 (e.g. voice messaging hunt group 33000) and the PRI QSIG trunk for the calls to the CS1000 (53xxx). Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case “53” and “3”.
- **Total Min:** Minimum number of digits.
- **Total Max:** Maximum number of digits.
- **Route Pattern:** The route pattern number from **Section 3.10**.
- **Call Type:** “aar” for voice messaging, “lev0” for private numbering (PRI/QSIG)

change aar analysis 0							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all					Percent Full:		1	
Dialed		Total		Route	Call	Node	ANI	
String		Min	Max	Pattern	Type	Num	Reqd	
3		5	5	32	aar		n	
53		5	5	100	lev0		n	

Use the “change dialplan analysis” command to define “8” as a feature access code. This will be used for AAR dialing in **Section 3.13**. Note also that the 3xxxx and 5xxxx extension ranges are defined in this form as well.

change dialplan analysis							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 1		
	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1		3	dac						
2		5	ext						
3		5	ext						
5		5	ext						
6		5	ext						
7		5	ext						
8		1	fac						
9		1	fac						

Use the “change feature-access-codes” command to assign the feature access code “8” to AAR.

change feature-access-codes		Page 1 of 8
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code: *01		
Abbreviated Dialing List2 Access Code: *02		
Abbreviated Dialing List3 Access Code: *03		
Abbreviated Dial - Prgm Group List Access Code: *04		
Announcement Access Code: *05		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

3.13 Configure Voice Messaging Hunt Group

Use the “add hunt group n” command to add a hunt group to be used by the voice messaging coverage path to be defined in the next section. “n” is an unused hunt group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Number:** An unassigned hunt group number.
- **Group Name:** A meaningful name (Modular Messaging).
- **Group Extension:** An unassigned extension number.
- **Group Type:** “ucd-mia”
- **ISDN/SIP Caller Display:** “mbr-name”

add hunt-group 32		Page 1 of 60
HUNT GROUP		
Group Number: 32	ACD? n	
Group Name: MM	Queue? n	
Group Extension: 33000	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: mbr-name		

On page 2, assign the following field values:

- **Message Center:** “sip-adjunct”
- **Voice Mail Number:** The **Group Extension** from Page 1.
- **Voice Mail Handle:** The **Group Extension** from Page 1.
- **Routing Digits:** The AAR feature access code from the previous section.

Submit these changes.

add hunt-group 32		Page 2 of 60
HUNT GROUP		
Message Center: sip-adjunct		
Voice Mail Number	Voice Mail Handle	Routing Digits
		(e.g., AAR/ARS Access Code)
33000	33000	8

3.14 Configure Voice Messaging Coverage Path

Use the “add coverage path n” command to specify a coverage path to be used for telephone users. This will specify use of the voice messaging hunt group. “n” is an unused coverage path number. Enter the hunt group number defined in the previous section in **Point 1**. Default values can be used for the remaining fields. It may be desirable to adjust the **Number of Rings** before a no-answer call goes to coverage.

add coverage path 32		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 32			
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: h32	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

3.15 Configure Coverage Path for Telephone Users

The following sample station form illustrates how to configure voice mail coverage for a given station user. Set **Coverage Path 1** to the value of the coverage path defined in the previous section.

change station 30001		Page 1 of 5	
STATION			
Extension: 30001	Lock Messages? n	BCC: 0	
Type: 9630	Security Code: 123456	TN: 1	
Port: S00504	Coverage Path 1: 32	COR: 1	
Name: AvayaH323	Coverage Path 2:	COS: 1	
	Hunt-to Station:		

3.16 Save Translations

Configuration of Communication Manager is complete. Use the “save translations” command to save these changes.

4 Configure Avaya Aura™ Session Manager

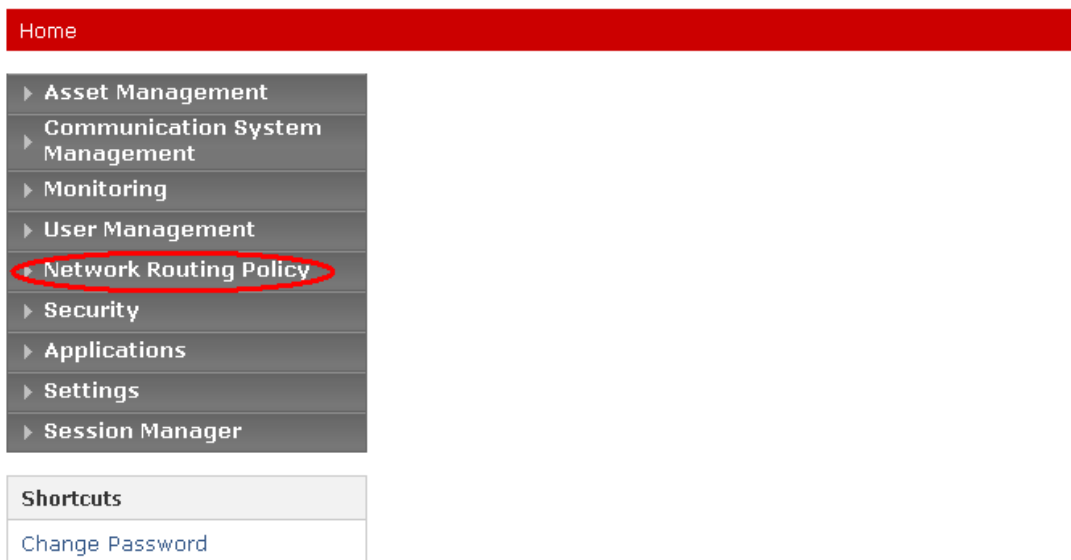
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation for Modular Messaging
- SIP Entities corresponding to Communication Manager, CS 1000, Modular Messaging, and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.
- Local host name resolution entries corresponding to fully qualified domain names (FQDN's) referenced in the previous steps.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **OK** in the subsequent confirmation screen. The menu shown below is then displayed. Expand the **Network Routing Policy** Link on the left side as shown. The sub-menus displayed in the left column below will be used to configure all but the last two of the above items (**Sections 4.1** through **4.9**).



Avaya Aura™ System Manager 5.2



4.1 Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **SIP Domains** on the left and click the **New** button (not shown) on the right. Fill in the following:

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

Click **Commit**.

The screenshot shows 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 Jan. 11, 2011'. A red breadcrumb trail reads 'Home / Network Routing Policy / SIP Domains'. On the left, a sidebar menu lists various management categories, with 'SIP Domains' under 'Network Routing Policy' circled in red. The main content area is titled 'Domain Management' and features a 'Commit' button. Below this is a table with one item, 'avaya.com', which has a red asterisk indicating a required field. The table columns are Name, Type, Default, and Notes. At the bottom of the main area, a red asterisk and the text '* Input Required' are displayed, along with another 'Commit' button.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 11, 2011 [Help](#)

Home / Network Routing Policy / SIP Domains

Domain Management [Commit](#)

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

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

* Input Required [Commit](#)

4.2 Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Under *General*, enter:

- **Name:** A descriptive name.
- **Notes:** Descriptive text (optional).

Under *Location Pattern*:

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Descriptive text (optional).

The screen below shows addition of the Basking Ridge location, which includes Communication Manager, Session Manager, and Modular Messaging, and the CS1000 in the 10.1.2 subnet. Click **Commit** to save the Location definition.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 11, 2011 Help

Home / Network Routing Policy / Locations / Location Details

Location Details Commit

General

* Name:

Notes:

Managed Bandwidth:

* Average Bandwidth per Call: Kbit/sec

* Time to Live (secs):

Location Pattern

Add Remove

1 Item Refresh Filter

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.1.2.*	<input type="text"/>

Select : All, None (0 of 1 Selected)

The fields under *General* can be filled in to specify bandwidth management parameters between Avaya Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that although not implemented in the sample configuration, routing policies can be defined based on location.

4.3 Add Adaptation Module

Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products. In the sample configuration, multi-site Modular Messaging represents its subscribers using 11 digit telephone numbers. The 5 digit extensions used by Communication Manager and the CS1000 are preceded by the 6 digits “120122”. **DigitConversionAdapter** is used in Session Manager to convert between the 5 and 11 digit formats when routing between Modular Messaging and those systems.

To add the generic adaptation module, select **Adaptations** on the left and click on the **New** button (not shown) on the right. Under *General*, fill in:

- **Name:** A descriptive name.
- **Adaptation Module:** Adaptation Module name and parameters (case sensitive)

The remaining fields can be left blank. Under *Digit Conversion for Incoming Calls to SM* and *Digit Conversion for Outgoing Calls from SM*, click **Add**, and then edit the fields in the resulting new row as shown below:

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

Click **Commit** to save the Adaptation Module definition. The screen below specifies **DigitConversionAdapter** and the SIP domain parameter “avaya.com” to be used when modifying the SIP messages. Incoming calls (SIP INVITE messages) from Modular Messaging that use 11 digit numbers will be converted to the 5 digit form by deleting the first 6 digits. Session Manager will route the call based on the resulting 5 digit extension. Calls routed to Modular Messaging will have their Request-URI, P-Asserted-Identity, and History-Info headers converted to 11 digit format by insertion of “120122” before being routed to Modular Messaging.



- ▶ Asset Management
- ▶ Communication System Management
- ▶ Monitoring
- ▶ User Management
- ▼ 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 Adaptation Details fields](#)
[Help for Committing configuration changes](#)

Adaptation Details[Commit](#)**General**

* **Adaptation name:** MM Normalized
Module name:
Module parameter: avaya.com
Egress URI Parameters:
Notes:

Digit Conversion for Incoming Calls to SM[Add](#) [Remove](#)

1 Item [Refresh](#) Filter

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

Select : All, None (0 of 1 Selected)

Digit Conversion for Outgoing Calls from SM[Add](#) [Remove](#)

2 Items [Refresh](#) Filter:

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 30	* 5	* 5	* 0	120122	both ▼	Avaya Call Center
<input type="checkbox"/>	* 53	* 5	* 5	* 0	120122	both ▼	Nortel CS1000

Select : All, None (0 of 2 Selected)

* Input Required

[Commit](#)

4.4 Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system supported by it using SIP trunks: the C-LAN board in the Avaya G650 Media Gateway and Modular Messaging. Select **SIP Entities** on the left and click on the **New** button (not shown) on the right.

Under *General*, fill in:


- **Name:** A descriptive name.
- **FQDN or IP Address:** FQDN or IP address of the Session Manager or the signaling interface on the telephony system.
- **Type:** “Session Manager” for Session Manager or “CM” for Communication Manager.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Time zone for this location.

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

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

Defaults can be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The following screen shows addition of Session Manager. The IP address of the SM-100 Security Module is entered for **FQDN or IP Address**. Two *Port* entries are added. TCP port 5060 is used for communicating with Modular Messaging and TLS port 5061 is used for communication with other Session Managers and Communication Manager.



Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 11, 2010
[Help](#)

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

Asset Management

Communication System Management

Monitoring

User Management

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 SIP Entity Details fields](#)
[Help for Committing configuration changes](#)

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type: Session Manager

Notes:

Location: BaskingRidge

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

Entity Links

Entity Links can be modified after SIP Entity is committed.

Port

2 Items | [Refresh](#) Filter

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

Select : All, None (0 of 2 Selected)


* Input Required

FS; Reviewed:
SPOC 3/31/2010

Solution & Interoperability Test Lab Application Notes
©2010 Avaya Inc. All Rights Reserved.

27 of 54
NrtlG450ASMMM

The following screen shows addition of Communication Manager. In this case, **FQDN or IP Address** is the Fully Qualified Domain Name (FQDN) of the C-LAN board in the Avaya G650 Media Gateway. Note that although not shown in the sample configuration, definition of multiple IP addresses (e.g., C-LANs) for the same FQDN (see **Section 4.9**) will cause Session Manager to load balance call traffic among those addresses.



Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 11, 2011
[Help](#)

[Home](#) / [Network Routing Policy](#) / [SIP Entities](#) / [SIP Entity Details](#)

- ▶ Asset Management
- ▶ Communication System Management
- ▶ Monitoring
- ▶ User Management
- ▼ Network Routing Policy
 - Adaptations
 - Dial Patterns
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities**
 - Time Ranges
 - Personal Settings
- ▶ Security
- ▶ Applications
- ▶ Settings
- ▶ Session Manager

SIP Entity Details
General

Commit

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

SIP Link Monitoring:

The following screen shows addition of the Modular Messaging Application Server (MAS) to which calls will be forwarded for busy/no-answer coverage of telephone users. **FQDN or IP Address** is the IP address of its network interface (see **Figure 1**). For **Adaptation**, select the adaptation module previously defined for dial plan digit manipulation in **Section 4.3**.

AVAYAAvaya Aura™ System Manager 5.2Welcome, **admin** Last Logged on at Jan. 11, 2011Help

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

▶ Asset Management

▶ Communication System Management

▶ Monitoring

▶ User Management

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

SIP Entities

Time Ranges

Personal Settings

▶ Security

▶ Applications

▶ Settings

▶ Session Manager

SIP Entity Details

Commit

General

* Name:alpinemas1

* FQDN or IP Address:135.8.139.31

Type:Modular Messaging

Notes:

Adaptation:MM Normalized

Location:BaskingRidge

Time Zone:America/New_York

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


SIP Link Monitoring

4.5 Add Entity Links

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

- **Name:** A descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Port:** Port number to which the other system sends SIP requests
- **SIP Entity 2:** Select the name of the other system.
- **Port:** Port number on which the other system receives SIP requests
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 4.4** will be denied.*

Click **Commit** to save each Entity Link definition. The following screens illustrate adding the Entity Links for Communication Manager and Modular Messaging. TLS (well-known port 5061) is used for Avaya Communication Manager. TCP (well-known port 5060) was used for Modular Messaging.

 Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Feb. 17, 2010 12:13 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy / Entity Links

▶ Asset Management

▶ Communication System Management

▶ Monitoring

▶ User Management

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

Entity Links

Commit

Cancel


1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* Call Center	* SM1	TLS	* 5061	* CallCenter	* 5061	<input checked="" type="checkbox"/>	CLAN 10.1.2.233

* Input Required

Commit

Cancel

 Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 11, 2010 4:52 PM
[Help](#) | [Log off](#)

Home / Network Routing Policy / Entity Links

▶ Asset Management

▶ Communication System Management

▶ Monitoring

▶ User Management

▼ Network Routing Policy

Adaptations

Dial Patterns

Entity Links

Locations

Regular Expressions

Routing Policies

SIP Domains

Entity Links

Commit

Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* MAS-Alpine	* SM1	TCP	* 5060	* alpinemas1	* 5060	<input checked="" type="checkbox"/>	Between SM1 and M

* Input Required

Commit

Cancel

4.6 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 4.4**. Two routing policies must be added for Communication Manager and Modular Messaging. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

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

Under *Time of Day*:

Select the default time range shown.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screens show the Routing Policies for Communication Manager and Modular Messaging.

AVAYA

Avaya Aura™ System Manager 5.2

Welcome, **admin** Last Logged on at Jan. 11, 2010 4:52 PM
[Help](#) | [Log off](#)

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

▶ Asset Management

▶ Communication System Management

▶ Monitoring

▶ User Management

▼ 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

Routing Policy Details

Commit

Cancel

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CallCenter	callcenter.avaya.com	CM	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item

Refresh

Filter: Enable

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

Select : All, None (0 of 1 Selected)

[Home](#) / [Network Routing Policy](#) / [Routing Policies](#) / [Routing Policy Details](#)

- ▶ Asset Management
- ▶ Communication System Management
- ▶ Monitoring
- ▶ User Management
- ▼ 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

Routing Policy Details

[Commit](#) [Cancel](#)

General

* Name: Disabled: ☐Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
alpinemas1	135.8.139.31	Modular Messaging	For use by Tony Matos's group

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	<input type="text" value="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)

4.7 Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entity. Calls to 5-digit extensions beginning with “3” or “53” should be routed to Communication Manager. The common access number for voice messaging for both systems is 33000, and calls to that number should be routed to Modular Messaging. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** SIP domain specified in **Section 4.1**
- **Notes:** Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save each dial pattern. The following screens show the resulting three dial pattern definitions. Note that similar to Communication Manager, the dial pattern selected will correspond to the longest match of a **Pattern** with the dialed number.

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 11, 2010 4:52 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	Call Center	0	<input type="checkbox"/>	CallCenter	

Select : All, None (0 of 1 Selected)

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

- Asset Management
- Communication System Management
- Monitoring
- User Management
- Network Routing Policy**
 - Adaptations
 - Dial Patterns**
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities
 - Time Ranges
 - Personal Settings
- Security
- Applications
- Settings
- Session Manager

Dial Pattern Details

[Commit](#) [Cancel](#)

General

* Pattern: * 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"/>	BaskingRidge	Fred's ACM & ASM's	Call Center	0	<input type="checkbox"/>	CallCenter	
Select : All, None (0 of 1 Selected)							

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

- Asset Management
- Communication System Management
- Monitoring
- User Management
- Network Routing Policy**
 - Adaptations
 - Dial Patterns**
 - Entity Links
 - Locations
 - Regular Expressions
 - Routing Policies
 - SIP Domains
 - SIP Entities
 - Time Ranges
 - Personal Settings
- Security
- Applications
- Settings
- Session Manager

Dial Pattern Details

[Commit](#) [Cancel](#)

General

* Pattern: * 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	ToAlpinemas1	0	<input type="checkbox"/>	alpinemas1	For calls to Tony's MM
Select : All, None (0 of 1 Selected)							

4.8 Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *General*:

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

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the resulting Session Manager definition.

 Avaya Aura™ System Manager 5.2 Welcome, **admin** Last l

Home / Session Manager / Session Manager Administration / **View Session Manager**

▶ Asset Management

▶ Communication System Management

▶ Monitoring

▶ User Management

▶ Network Routing Policy

▶ Security

▶ Applications

▶ Settings

▼ **Session Manager**

▶ Network Configuration

▶ Device and Location Configuration

▶ Application Configuration

▶ System Status

▶ System Tools

Shortcuts

Change Password

Help for Session Manager Administration

View Session Manager

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

General ▼

SIP Entity Name

Description

Management Access Point Host Name/IP

Direct Routing to Endpoints

SM1

Session Mgr 1

10.1.2.171

Enable

Security Module ▼

SIP Entity IP Address

Network Mask

Default Gateway

Call Control PHB

QOS Priority

Speed & Duplex

VLAN ID

10.1.2.170

255.255.255.0

10.1.2.1

46

6

Auto

4.9 Define Local Host Names

The host names (FQDN's) referenced in the definitions of the previous sections must be defined. To do so, Select **Session Manager -> Network Configuration -> Local Host Name Resolution** under the menu on the left. For each host name, click **New** and enter the following:

- **Host Name:** The FQDN used for the host
- **IP Address:** IP address of the host's network interface
- **Port:** Port number to which SIP requests are sent
- **Transport:** Transport to be used for SIP requests

Defaults can be used for the remaining fields. The **Priority** and **Weight** fields are used when multiple IP addresses are defined for the same host. The circled entry in the following screen shows the host name used in the sample configuration (see Entity Link configuration for Communication Manager in **Section 4.4**).

AVAYA Avaya Aura™ System Manager 5.2 Welcome, admin Last Logged on at Jan. 11, 2010 4:52 PM Help Log off

Home / Session Manager / Network Configuration / Local Host Name Resolution

Local Host Name Resolution

This page allows you to add, edit, or remove local host name entries. Host name entries on this page will override information provided by DNS.

Local Host Name Entries

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

5 Items | [Refresh](#) Filter: Enable

<input type="checkbox"/>	Host Name	IP Address	Port	Priority	Weight	Transport
<input type="checkbox"/>	allanc-s8300-g350	10.32.2.80	5060	100	100	TCP
<input type="checkbox"/>	alpinemas1	135.8.139.31	5060	100	100	TCP
<input checked="" type="checkbox"/>	callcenter.avaya.com	10.1.2.233	5060	100	100	TCP
<input type="checkbox"/>	m1000.avaya.com	10.1.2.100	5060	100	100	TCP
<input type="checkbox"/>	MikeH-S8300-G450	10.32.2.20	5060	100	100	TCP

Select : All, None (0 of 5 Selected)

5 Configure Avaya Modular Messaging

In sample configuration, the Communication Manager and the CS1000 telephone systems were added as sites to an existing multi-site Modular Messaging system that was modified to support their subscribers and communication with Session Manager. The associated MAS server was named *alpinemas1*. As shown in the previous sections, Session Manager was configured to route incoming calls to *alpinemas1* (135.8.139.31). *alpinemas1* was also configured to send message waiting notifications (SIP NOTIFY messages) to Session Manager. This section focuses on the following configuration steps:

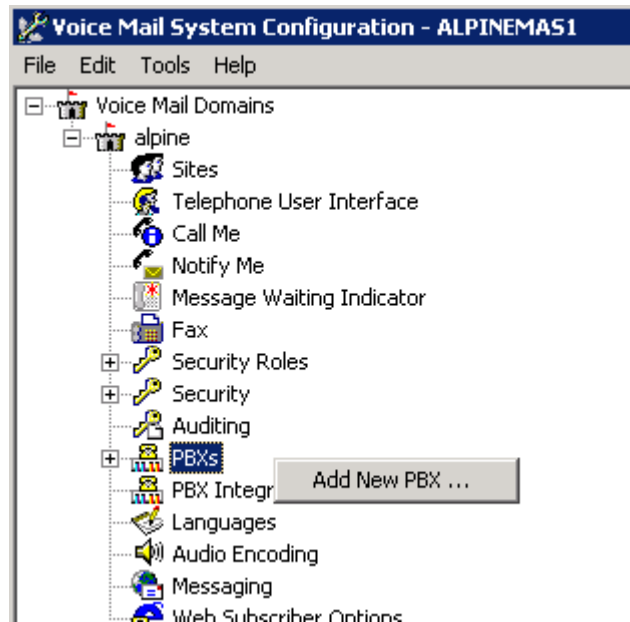
- Adding a PBX
- Configuring communication with Session Manager
- Defining dial plan translation rules

- Including the Communication Manager and CS1000 systems as sites
- Subscriber definition

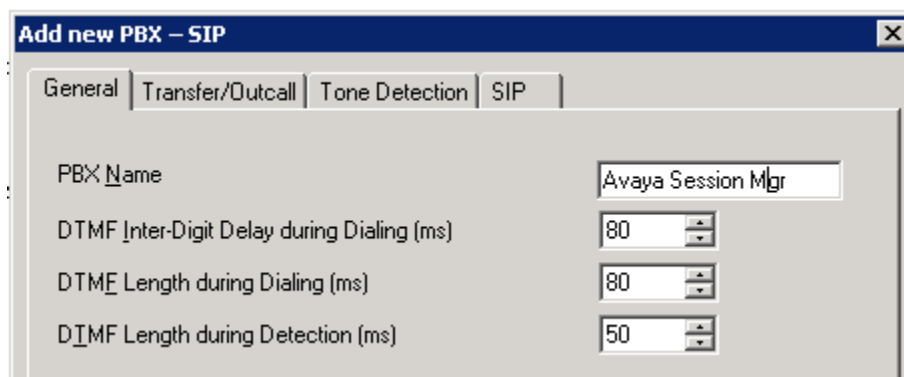
See references [7-8] in **Section 9** for standard installation and configuration information. General knowledge of the configuration tools and interfaces is assumed.

5.1 Add PBX

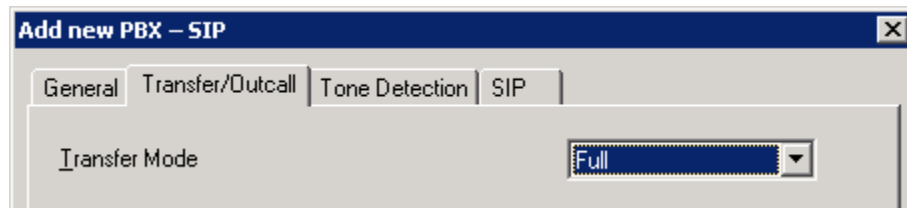
The aggregate Session Manager, Communication Manager, and CS1000 systems are defined to Modular Messaging as a “PBX.” Bring up the *Voice Mail System Configuration* tool, select **PBXs**, and use button two on the mouse to select **Add New PBX**, as shown below.



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

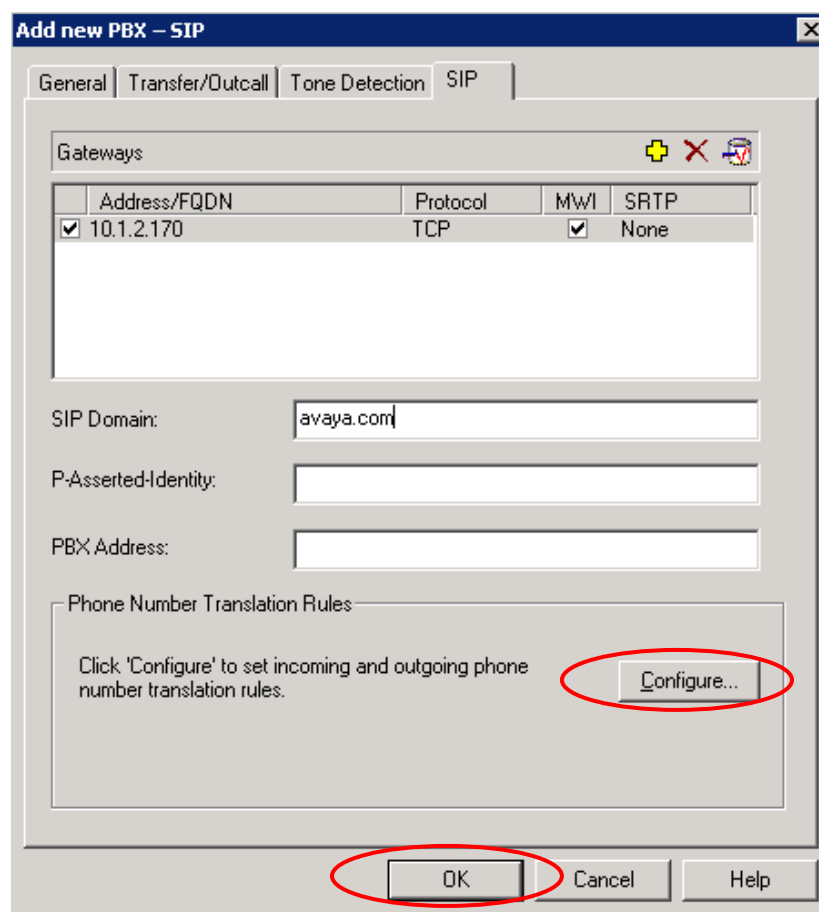


On the *Transfer/Outcall* tab, select “Full” for **Transfer Mode**.



Default values can be used for the *Tone Detection* tab. On the *SIP* tab under the *Gateways* section, click on the “+” icon and add Session Manager’s SM-100 IP address under **Address/FQDN**, “TCP” for **Protocol**, and check the **MWI** box so message waiting notifications will be sent. Fill in **SIP Domain** with the domain from **Section 4.1**.

Click on **Configure** to specify number translation rules for translating between the local dial plans of the Communication Manager and CS1000 telephone systems and the normalized 11 digit form used by Modular Messaging.



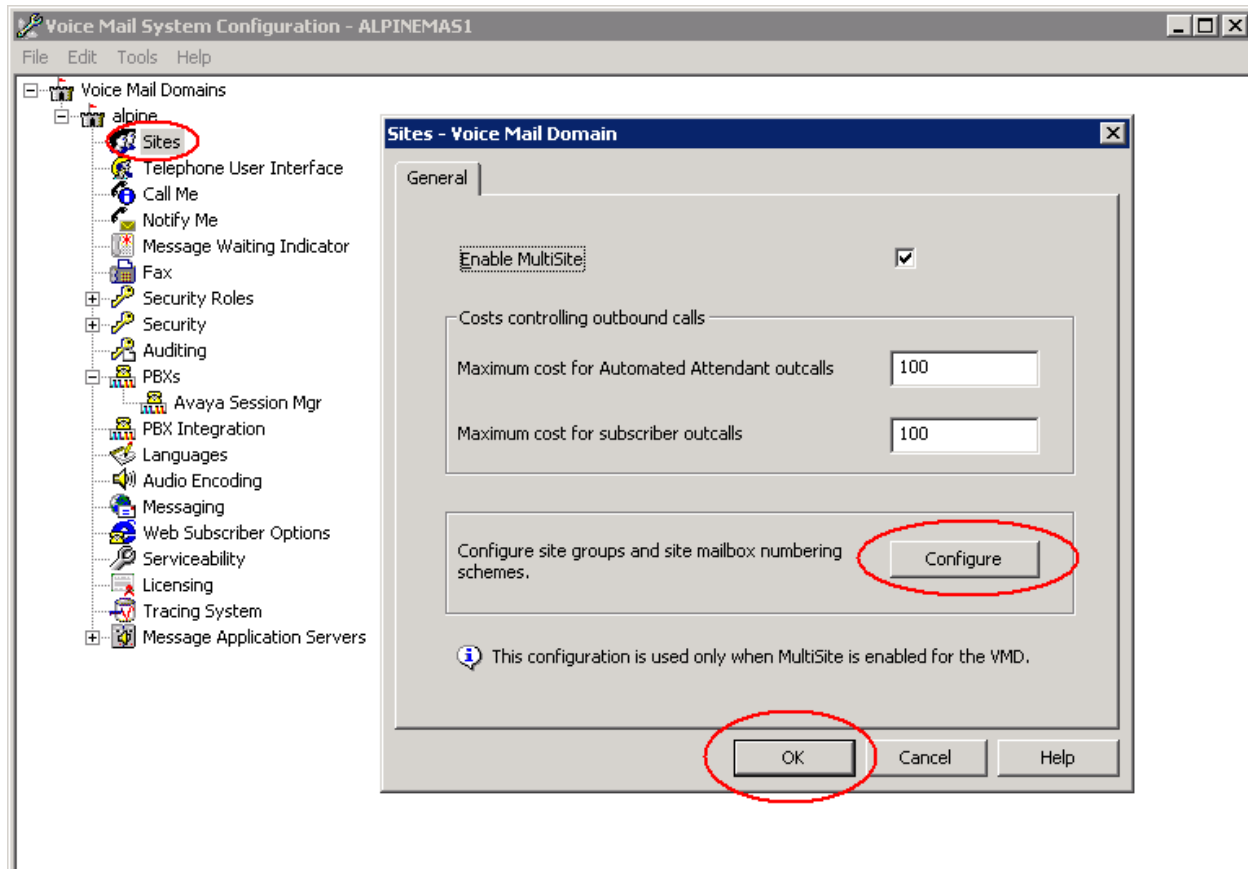
The following display appears. In the right pane, create the appropriate rules to translate between extension dialed and normalized 11 digit numbers. For the sample configuration, the last first rules were used, and were added by selecting **Add**. As described in **Section 4.3**, Session manager will translate between 11-digit numbers used by Modular Messaging and 5-digit numbering used by the telephone systems. The “Avaya-11-digit” and “Nortel-11-digit” **Incoming** and **Outgoing translation rules** specify that Modular Messaging will not change the numbering from its 11-digit format. The “Avaya-Ext” and “Nortel-Ext” rules support features such as extension dialing by subscribers while accessing Modular Messaging, and translate the 5-digit extension format into normalized 11-digit format. In the screen below, “Avaya” corresponds to Communication Manager subscribers, and “Nortel” corresponds to CS1000 subscribers. Proper operation of the rules can be verified by adding *Test inputs* in the left pane and viewing the resulting output in the corresponding rule in the right pane. Click on **OK** when finished, then again on **OK** in the original *Add new PBX* window (see previous screen).

Test inputs	Incoming translation rule				Outgoing translation rule			
	Description	Match	Output	Canonical Test	Match	Output	Switch Test	Cost
✓ 40006	ext 4xxxx	^(4\d{4})\$	+190875\$1	^+190875(\d{5})\$	\$1			0
✓ 42001	Avaya-Ext	^3\d{4}\$	+1201223\$1					0
✓ 30001	Avaya-11-digit	^(1201223\d{4})\$	+\$1	+12012230001	^+1201223\d{4}\$	1201223\$1	12012230001	0
✓ 12012230001	Nortel-Ext	^5\d{4}\$	1201225\$1					0
✓ 53500	Nortel-11-digit	^(1201225\d{4})\$	+\$1		^+1201225\d{4}\$	1201225\$1		0
✓ 12012253500	Juniper-Ext	^2\d{4}\$	1201222\$1					0
✓ 20503	Juniper-11-digit	^(1201222\d{4})\$	+\$1		^+1201222\d{4}\$	1201222\$1		0

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

5.2 Add Sites

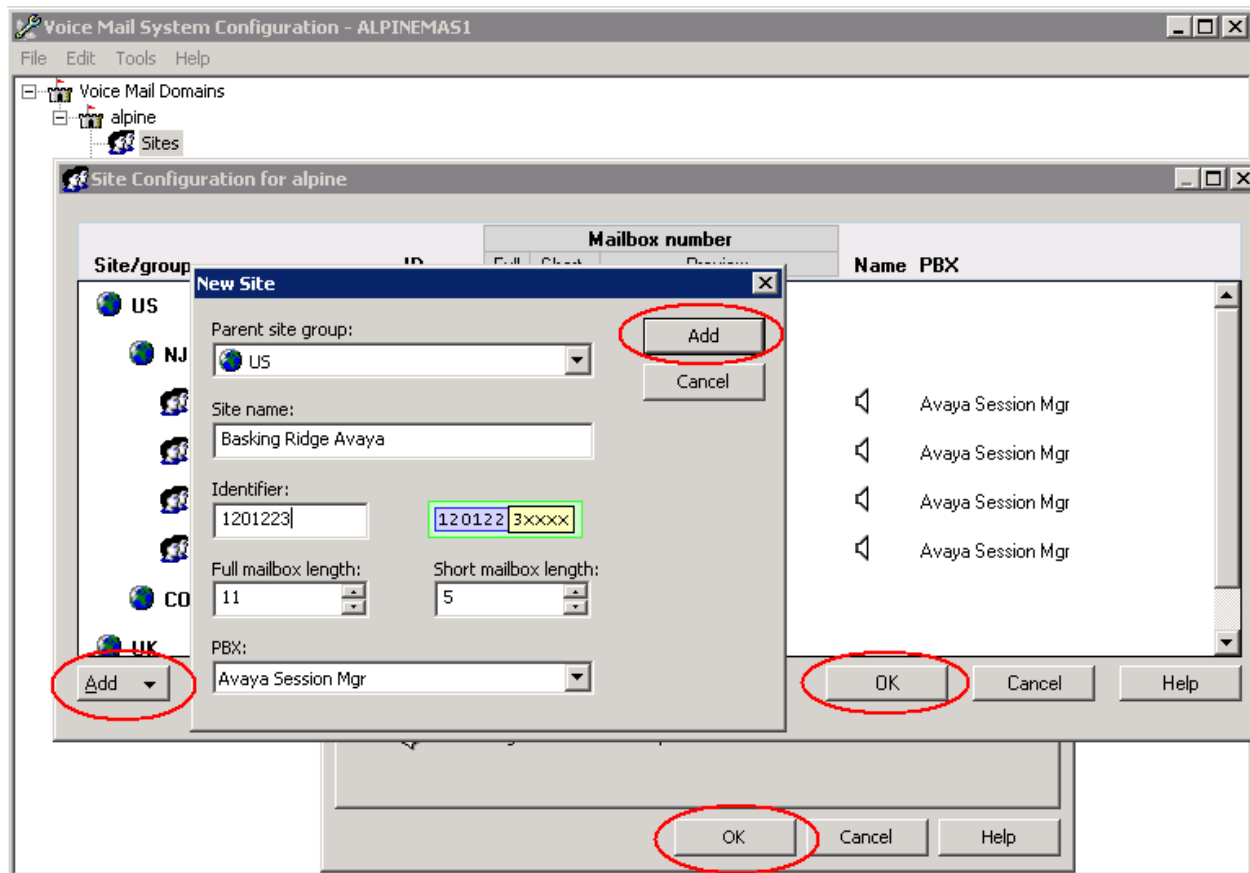
The telephone systems with different dial plans must be added as sites in Modular Messaging. This is done by double-clicking **Sites** in the *Voice Mail System Configuration* tool, as shown below. In the *Sites* window that is displayed, click on **Configure**.



The *Site Configuration* window is displayed. Click on **Add** to add the “Basking Ridge Avaya” site, and enter the following in the *New Site* window:

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

Click on **Add** when finished. Repeat for the site corresponding to the CS1000. The following screen shows the result of adding the Communication Manager at the Basking Ridge site. When all sites are added, click **OK** in the *Site Configuration* window, and then click on **OK** in the original *Sites* window (the first screen in this section).



5.3 Add Subscribers

Log in to the web interface of the Modular Messaging MSS to add subscribers for each voice messaging user on the telephone systems. Select **Subscriber Management** on the left. Then select **Manage** on the right for *Local Subscribers*.

The screenshot displays the Avaya Modular Messaging Administration web interface. The left sidebar contains a navigation menu with the following categories and items:

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

The main content area is titled "Manage Subscribers" and contains the following information:

- Local Subscriber Mailbox Number: Add or Edit
- Table with columns: Machine Name, Local Subscriber Mailboxes, Total Subscribers, Filtered Subscribers, and a Manage button.

	Machine Name	Local Subscriber Mailboxes	Total Subscribers	Filtered Subscribers	
Local Subscribers	alpinemss1	28	29	29	Manage
Remote Subscribers	internet		0	0	Manage

Page Status:

The *Manage Local Subscribers* screen is displayed. Click on **Add a New Subscriber**.

The screenshot shows the Avaya Modular Messaging Administration web interface. The left sidebar contains a navigation menu with categories like 'Messaging Administration', 'Server Administration', 'IMAP/SMTP Administration', 'Server Information', 'Utilities', and 'Logs'. The main content area is titled 'Manage Local Subscribers'. At the top of this area, it displays 'Local Subscriber Mailboxes: 28', 'Total Subscribers: 29', 'System Mailboxes: 1', and 'Filtered Subscribers: 29'. Below this is a table listing subscribers with columns for ASCII Name, Mailbox Number, Numeric Address, COS, CID, and Subscriber Name. The table contains 28 entries. Below the table are several buttons: 'Sort and Filter Subscribers', 'Launch Subscriber Options', 'Display Report of Subscribers', 'Delete the Selected Subscriber', 'Edit the Selected Subscriber', 'Add a New Subscriber' (which is circled in red), and 'Back'. At the bottom, there is a 'Page Status' section showing 'Form unchanged. Saved values are shown.' The browser window at the top shows the URL 'https://mss1/cgi-bin/do_login' and a 'Certificate Error' warning.

ASCII Name	Mailbox Number	Numeric Address	COS	CID	Subscriber Name
Nortel Four	12012230043	12012230043	507	1	Four, Nortel
OneX	12012230015	12012230015	507	1	H323, One-X
IP, Avaya	12012230001	12012230001	507	1	IP, Avaya
IP, Nortel	12012253505	12012253505	507	1	IP, Nortel
One, AC Branch2	19087542001	19087542001	507	1	One, AC Branch2
NortelOne	12012230040	12012230040	507	1	One, Nortel
One, User	19087540006	19087540006	507	1	One, User
SIP1, Avaya	12012230010	12012230010	507	1	SIP1, Avaya
SIP2, Avaya	12012230013	12012230013	507	1	SIP2, Avaya
Nortel Three	12012230042	12012230042	507	1	Three, Nortel
Two, AC Branch2	19087542002	19087542002	507	1	Two, AC Branch2
Nortel Two	12012230041	12012230041	507	1	Two, Nortel
Two, User	19087540007	19087540007	507	1	Two, User
postmaster	19087549999	19087549999	500	1	postmaster
testaudix	19087549998	19087549998	507	1	testaudix

Enter the following for the new subscriber:

- **Last Name:** Subscriber last name
- **First Name:** Subscriber first name
- **Password:** Subscriber access password
- **Mailbox number:** Full 11-digit mailbox number
- **PBX Extension:** 11-digit mailbox preceded by “+” and select **Canonical**
- **Class of Service:** Select one from those configured (controls access to voice messaging features)
- **Community ID:** Select one from those configured

All other fields can retain default values. Select **Save** when done (not shown). The screens below show a sample subscriber definition for each system.

The screenshot displays the Avaya Modular Messaging Administration web interface in a Windows Internet Explorer browser window. The browser address bar shows the URL https://mss1/cgi-bin/do_login. The page title is "Modular Messaging Administration" and it indicates "This server: 135.8.139.31".

The left sidebar contains a navigation menu with the following items:

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

The main content area is titled "Edit Local Subscriber" and contains the following sections:

BASIC INFORMATION * (Required Fields)

*Last Name	IP	First Name	Avaya
*Password		*Mailbox Number	12012230001
*Numeric Address	12012230001	PBX Extension	+12012230001
*Class Of Service	507 - audixtest		<input checked="" type="radio"/> Canonical <input type="radio"/> Switch Native
		*Community ID	1

SUBSCRIBER DIRECTORY

Email Handle	AvayaIP @alpinemss1.avaya.com	Telephone Number	12012230001
Common Name	Avaya IP	ASCII Version of Name	IP, Avaya

SUBSCRIBER SECURITY

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

MAILBOX FEATURES

Personal Operator Mailbox	30002	Personal Operator Schedule	Always Active
VoiceMail Enabled	yes	Intercom Paging	paging is off

135.8.139.31 - Remote Desktop

Messaging Administration

AVAYA Modular Messaging Administration This server:

Help Log Off

Messaging Administration

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

Edit Local Subscriber

BASIC INFORMATION
* (Required Fields)

*Last Name	IP	First Name	Nortel
*Password		*Mailbox Number	12012253505
*Numeric Address	12012253505	PBX Extension	+12012253505 <input checked="" type="radio"/> Canonical <input type="radio"/> Switch Native
*Class Of Service	507 - audixtest	*Community ID	1

SUBSCRIBER DIRECTORY

Email Handle	NortelIP @alpinemss1.avaya.com	Telephone Number	12012253505
Common Name	Nortel IP	ASCII Version of Name	IP, Nortel

SUBSCRIBER SECURITY

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

MAILBOX FEATURES

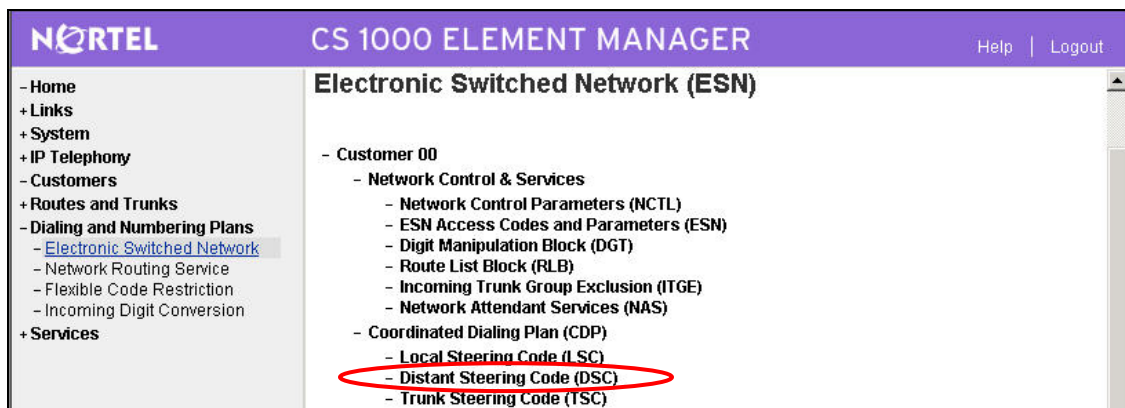
Personal Operator Mailbox	30001	Personal Operator Schedule	Always Active
VoiceMail Enabled	yes	Intercom Paging	paging is off

Start | Voice Mail System Config... | Control Panel | Messaging Administr... | 100%

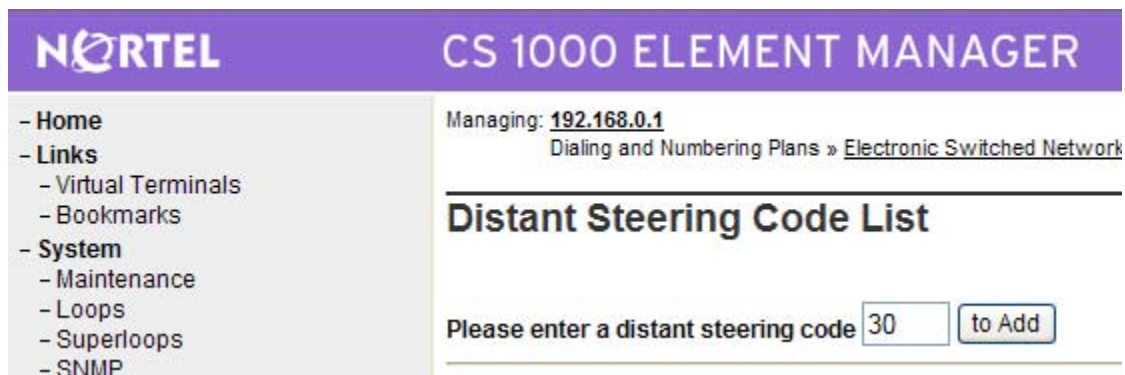
start | root@avay... | admin@ninte... | 10.1.2.160... | 10.1.2.160... | 10.3.3.50... | Nortel CS 1... | http://10.8... | 135.8.139... | ASM (Not R... | avaya_IP - ...

6 Configure Avaya Communication Server 1000

Configuration of the CS1000 for call routing and coverage to Modular Messaging (extension 33000) using a T1 PRI QSIG interface to the Avaya G450 Media Gateway is identical to that described in other Application Notes (see Reference [11]). In addition to those configuration steps, a route must be added for calls to Communication Manager, which has extension numbers of the form 30xxx. The CS1000 Element Manager is used to configure this routing. On the main web page, under *Dialing and Numbering Plans*, select **Electronic Switched Network**, and then click on **Distant Steering Code**.



The **Distant Steering Code List** screen is displayed. In the **Please enter a distant steering code** field, enter the dialed prefix digits to match on (in this case “30”). Click to **Add**.



The **Distant Steering Code** screen is displayed. For the **Route List to be accessed for trunk steering code (RLI)** field, select the route list index from the drop-down list that corresponds to that configured for the PRI QSIG trunk (as per Reference [11]). Retain the default values in all remaining fields, and scroll down to the bottom of the screen to click **Submit**. Repeat these two steps to add another Distant Steering Code for dialing the Modular Messaging pilot number (33000).

7 Verification Steps

7.1 Verify Avaya Aura™ Communication Manager

Verify the status of the ISDN trunk group to the CS1000 using the “status trunk” command. An example screen is shown below. Idle trunk members should show “in-service/idle”.

status trunk 100				Page 1
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0100/001	001V101	in-service/idle	no	
0100/002	001V102	in-service/idle	no	
0100/003	001V103	in-service/idle	no	
0100/004	001V104	in-service/idle	no	
0100/005	001V105	in-service/idle	no	
0100/006	001V106	in-service/idle	no	
0100/007	001V107	in-service/idle	no	
0100/008	001V108	in-service/idle	no	
0100/009	001V109	in-service/idle	no	
0100/010	001V110	in-service/idle	no	
0100/011	001V111	in-service/idle	no	
0100/012	001V112	in-service/idle	no	
0100/013	001V113	in-service/idle	no	
0100/014	001V114	in-service/idle	no	

If the trunk members are not in-service, check the signaling group status, as shown below, using the “status signaling-group” command. Verify the signaling group is “in-service” as indicated in the **Group State** and **Level 3 State** fields shown below.

```
status signaling-group 100
                        STATUS SIGNALING GROUP

      Group ID: 100                      Active NCA-TSC Count: 0
      Group Type: isdn-pri                Active CA-TSC Count: 0
      Signaling Type: facility associated signaling
      Group State: in-service

                        Primary D-Channel

      Port: 001V124      Level 3 State: in-service
```

If the signaling group **Level 3 State** is not in service, the health of the physical level can be checked by testing the DS1 board. Abridged output is shown below. While maintenance documentation is beyond the scope of these Application Notes, failure of the initial tests of the DS1 board likely indicate a problem with the physical layer connectivity to the CS1000 (e.g., improper cabling, framing, etc.). If test 144 fails, check that the G450 Media Gateway is deriving clock synchronization properly.

```
test board lv1
Page 1

                        TEST RESULTS

Port      Mtce Name    Alt. Name      Test No.  Result      Error Code
001V1     MG-DS1             138          PASS
001V1     MG-DS1             139          PASS
001V1     MG-DS1             140          PASS
001V1     MG-DS1             141          PASS
001V1     MG-DS1             142          PASS
001V1     MG-DS1             143          PASS
001V1     MG-DS1             144          PASS
001V1     MG-DS1             145          PASS
001V1     MG-DS1             146          PASS
```


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

```
status trunk 32
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0032/001	T00226	in-service/idle	no
0032/002	T00227	in-service/idle	no
0032/003	T00228	in-service/idle	no
0032/004	T00229	in-service/idle	no
0032/005	T00230	in-service/idle	no
0032/006	T00231	in-service/idle	no
0032/007	T00232	in-service/idle	no
0032/008	T00233	in-service/idle	no
0032/009	T00234	in-service/idle	no
0032/010	T00235	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 3.9**. Verify the signaling group is “in-service” as indicated in the **Group State** field shown below.

```
status signaling-group 32
```

STATUS SIGNALING GROUP	
Group ID: 32	Active NCA-TSC Count: 0
Group Type: sip	Active CA-TSC Count: 0
Signaling Type: facility associated signaling	
Group State: in-service	

Finally, make a call between the Avaya 9600 Series IP Telephone and the Avaya i2004 IP Telephone and verify two-way audio. Verify the status of connected trunks by using the “status trunk” command for the PRI QSIG trunk group (100) to the CS1000. More information can be obtained by using “status trunk 100/x” where x is the trunk member for the in-service/active trunk member for the call.

7.2 Verify Avaya Aura™ Session Manager

Expand the **Session Manager** menu on the left and click **SIP Monitoring**. Verify that none of the links to the defined SIP entities are down, indicating that they are all reachable for call routing. In the sample screen below, the SIP trunk to SM1 has been busied out on Communication Manager, so one of the links is shown as down.

▶ Asset Management

▶ User Management

▶ Monitoring

▶ Network Routing Policy

▶ Security

▶ Applications

▶ Settings

▼ Session Manager

Session Manager Administration

System State Administration

Security Module Status

Data Replication Status

Local Host Name Resolution

Maintenance Tests

SIP Firewall Configuration

SIP Monitoring

Tracer Configuration

Trace Viewer

Call Routing Test

Managed Bandwidth Usage

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
SM1	1/13	0	0	0

All Monitored SIP Entities

Refresh

15 Items | Filter: Enable

SIP Entity Name
AcmePacket
AS5400
AudioCodes M1000
Avaya MAS-BR1
Avaya-G430
Avaya-S8500
Avaya_MAS-Br2
Avaya_MAS-HQ
CallCenter

Select the corresponding Session Manager (**SM1** in this example) to view the Entity Link that is down and the Reason Code. The Reason Code reflects the result of Session Manager sending a SIP OPTIONS message to that SIP Entity.

▶ Asset Management

▶ User Management

▶ Monitoring

▶ Network Routing Policy

▶ Security

▶ Applications

▶ Settings

▼ Session Manager

Session Manager Administration

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager where at least one connection is currently down.

All Entity Links with Down Connections for Session Manager: SM1

Refresh | Summary View

11 Items | Filter: Enable

Details	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	CallCenter	10.1.2.233	5060	TCP	DOWN	408 Request Timeout	DOWN

7.3 Verify Nortel Communication Server 1000

Select **Services->Logs and Reports->IP Telephony Nodes** on the left. Click **Status** for the “SS_Node” to verify that the signaling server is enabled and operational.

The screenshot shows the Nortel CS 1000 Element Manager interface. The left sidebar contains a navigation tree with the following items: al Terminals, kmarks, m, itenance, os, erloops, IP, ware, aphony, es: Servers, Media Cards, as, work Address Translation, Thresholds, onal Directories, ware, mers, s and Trunks, tes and Trunks, hannels, tal Trunk Interface, g and Numbering Plans, tronic Switched Network, work Routing Service, ible Code Restriction, ming Digit Conversion, - Services, + Backup and Restore, - Date and Time, - Logs and Reports, - IP Telephony Nodes (selected), - Call Server Report Utility, - Equipped Feature Packages, - Peripheral Software Version Dat, - System License Parameters, + Security.

The main area displays the 'Node Maintenance and Reports' page. It shows a table of nodes with the following columns: Index, ELAN IP, Type, and TN. The table contains two rows: 'SS_Node' and 'Media-Card-14'. The 'SS_Node' row has a 'Status' button circled in red. Below the table, a status bar shows '192.168.0.3 : Enabled' circled in red.

See Reference [11] for verification of successful PRI QSIG trunk configuration.

7.4 Verification Scenarios

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

- Basic calls between various telephones on the Communication Manager 5.2 and Avaya Communication Server 1000 can be made in both directions using G.711MU. Proper display of the calling and called party name and number information was verified for all telephones with the basic call scenario.
- Supplementary calling features were verified. The feature scenarios involved additional endpoints on the respective systems, such as performing an unattended transfer to a local endpoint on the same system, and then repeating the scenario to transfer the call to a remote endpoint on the other system. The supplementary calling features verified are shown below. Note that calling/called party name and number display may not be consistent in certain scenarios for features shown in *italics*.
 - Unattended transfer
 - Attended transfer
 - *Hold/Unhold*
 - Consultation hold
 - Call forwarding
 - Conference

- Voice mail and voice mail calling features supported by Modular Messaging were verified, including message waiting indicator support for telephones on Communication Manager and Avaya Communication Server 1000. Voice mail calling features included the following. Note that calling/called party name and number display may not be consistent in certain scenarios for features shown in italics.
 - Busy/no answer greetings
 - Message Waiting Indicator (MWI)
 - Send all calls
 - Coverage on call forward
 - *Personal operator*
 - *Auto-attendant*
 - *Find me*
 - *Call me*
 - *Call sender*
 - *Transfer*

8 Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000 front-ended by an Avaya G450 Media Gateway can be integrated with Avaya SIP products, including Session Manager and Modular Messaging.

9 Additional References

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

Avaya Aura™ 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] Maintaining and Troubleshooting Avaya Aura™ Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.

Avaya Aura™ Communication Manager 5.2:

- [4] *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>.
- [5] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009, available at <http://support.avaya.com>.
- [6] *Upgrading, Migrating, and Converting Avaya Servers and Gateways, Release 5.0*, Doc ID 03-300412, January 2008, available at <http://support.avaya.com>.

Avaya Modular Messaging:

- [7] *Release 5.2 with Avaya MSS – Messaging Application Server (MAS) Administration Guide*, November, 2009, available at <http://support.avaya.com>.
- [8] *Avaya Modular Messaging for the Avaya Message Storage Server (MSS) Configuration – Release 5.2 Installation and Upgrades*, November, 2009, available at <http://support.avaya.com>.

Avaya Application Notes:

- [9] *Configuring SIP Trunks among Avaya Aura™ Session Manager, Avaya Aura™ Communication Manager 5.2, and Nortel Communication Server 1000 – Issue 1.1*, available at <http://www.avaya.com>.
- [10] *Front-Ending Nortel Communication Server 1000 with an AudioCodes Mediant 1000 Modular Media Gateway to Support SIP Trunks to Avaya Aura™ Session Manager with Avaya Aura™ Communication Manager 5.2 as an Access Element – Issue 1.1*, available at <http://www.avaya.com>.
- [11] *Configure an Avaya Centralized Messaging Solution with Avaya Communication Manager and Nortel Communication Server 1000 – Issue 1.0*, 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