

Avaya Solution & Interoperability Test Lab

Configuring SIP Trunks Among Avaya Aura<sup>™</sup> Session Manager 6.0, Avaya Aura<sup>™</sup> Communication Manager Feature Server 6.0, Avaya one-X® Deskphone Edition for 9600 Series SIP IP Telephones, and Avaya Communication Server 1000E 6.0 – Issue 1.0

#### Abstract

These Application Notes present a sample configuration for a network that uses Avaya Aura<sup>TM</sup> Session Manager 6.0 to connect Avaya Aura<sup>TM</sup> Communication Manager Feature Server 6.0, Avaya 96xx SIP telephones and an Avaya (formerly Nortel) Communication Server 1000E 6.0 using SIP trunks.

- Avaya Aura<sup>TM</sup> Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura<sup>TM</sup> Communication Manager Feature Server operates as a feature server for the SIP endpoints which communicate with Avaya Aura<sup>TM</sup> Session Manager using the SIP protocol. Unlike the Avaya Aura<sup>TM</sup> Communication Manager Evolution Server, Avaya Aura<sup>TM</sup> Communication Manager Feature Server does not support traditional telephones such as DCP, analog and H.323 registered directly to it.

For the sample configuration, Avaya Aura<sup>TM</sup> Session Manager runs on an Avaya S8800 Server, Avaya Aura<sup>TM</sup> Communication Manage Feature Server runs on an Avaya S8300D Server with an Avaya G450 Media Gateway and the 96xx SIP telephones are registered to Avaya Aura<sup>TM</sup> Session Manager. The Avaya Communication Server 1000E runs on a co-res CP+PM server blade version 6.0. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura<sup>TM</sup> Communication Manager 6.0 Feature Server and Avaya Communication Server 1000E 6.0.

(This page intentionally left blank)

#### **Table of Contents**

1.	Intro	oduction	5
2.	Equ	ipment and Software Validated	7
3.		n-level List of Tasks:	
4.	Con	figuring Avaya Aura <sup>TM</sup> Communication Manager Feature Server	8
	4.1	Verify System Capabilities and Licensing	
	4.1.1		
	4.1.2		
	4.1.3	6	
	4.1.4		
	4.2	Add Node Name of Avaya Aura <sup>TM</sup> Session Manager	
	4.3	Configure IP Network Regions	
	4.3.3		
	4.3.2	5	
	4.3.3		
	4.4	Add SIP Signaling Group	
	4.5	Add SIP Trunk Group	
	4.6	Administer Private Numbering	
	4.7	Administer Call Routing	
	4.7.	6	
	4.7.2	•	
	4.7.3	1	
	4.7.4		
	4.7.4		
	4.0 4.9	Configure Stations Verify Off-Pbx Telephone Station-Mapping	
	4.9		
5		Save Translation	
э.		figure Avaya Aura <sup>TM</sup> Session Manager	
	5.1	Administer SIP Domains	
	5.2	Define Locations	
	5.3	Add SIP Entitites	
	5.3.		
	5.3.2		
	5.3.3		r
	5.3.4		
	5.3.5	5	
	5.4	Create Entity Links	
	5.5	Add Routing Policies	
	5.6	Add Dial Patterns	
	5.7	Define Avaya Aura <sup>TM</sup> Communication Manager Feature Server as an Admi	nistrable Entity
		34	
	5.7.		
	5.7.2		
	5.8	Define an Application Sequence for Avaya Aura <sup>TM</sup> Communication Manag 37	er Feature Server
	5.9	Add SIP Users	
		Reviewed: Solution & Interoperability Test Lab Application Notes	Page 3 of 58
	SPOC	©2010 Avaya Inc. All Rights Reserved.	CS1KSM6CM6FS

6. Co	nfigure 96xx SIP Deskphone	44
6.1	Configure IP Address, Subnet Mask & Default Gateway	
6.2	Configure SIP Global and Proxy Settings	
6.3	Login Phone to Avaya Aura <sup>TM</sup> Session Manager	
7. Co	nfigure the Communication Server 1000	50
8. Ve	rification Steps	51
8.1	Verify Avaya Aura <sup>TM</sup> Communication Manager 6.0	
8.2	Verify Avaya Aura <sup>TM</sup> Session Manager	
8.3	Verify 96xx SIP Phones are Registered	
8.4	Verify Avaya Communication Server 1000	
8.4	.1 Verify Status of the Signaling Server	
8.4	.2 Verify Status of an Active Call	55
8.5	Verification Scenarios	
9. Co	nclusion	56
10. Ad	ditional References	56

### 1. Introduction

These Application Notes present a sample configuration for a network that uses Avaya Aura<sup>TM</sup> Session Manager 6.0 to connect Avaya Aura<sup>TM</sup> Communication Manager Feature Server 6.0 SP1, Avaya 96xx SIP telephones and an Avaya Communication Server 1000E 6.0 using SIP trunks.

In addition to these Applicates Notes, it is recommed to download the Application Notes from **Reference** [12] Section 10 for additional detail on configuring the CS1000 and Avaya Aura<sup>TM</sup> Communication Manager Evolution Server.

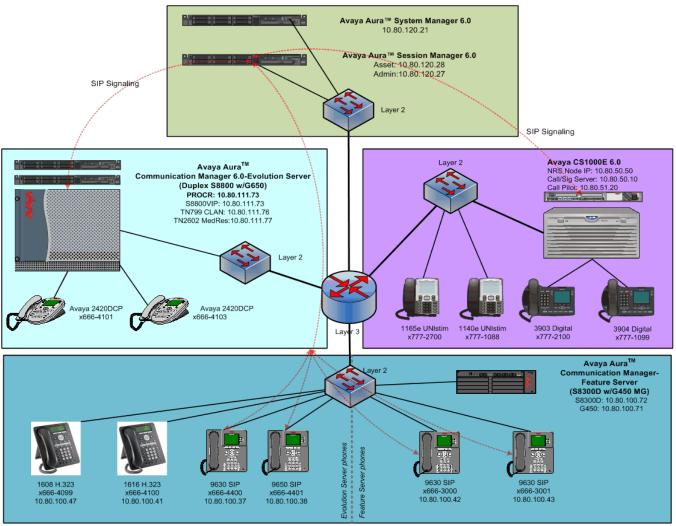
The Avaya Aura<sup>TM</sup> Communication Manager Feature Sever was a new concept for the 5.2.1 release and carries forward in 6.0. Unlike the Avaya Aura<sup>TM</sup> Communication Manager Evolution Server, the Avaya Aura<sup>TM</sup> Communication Manager Feature Server communicates with Avaya Aura<sup>TM</sup> Session Manager via an <u>IMS-enabled</u> SIP signaling group and associated SIP trunk group and supports only 96xx SIP telephones.

- Avaya Aura<sup>TM</sup> Session Manager provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and registrations for SIP endpoints.
- Avaya Aura<sup>TM</sup> Communication Manager Feature Server operates as a feature server for the SIP endpoints which communicate with Avaya Aura<sup>TM</sup> Session Manager using the SIP protocol. Unlike the Avaya Aura<sup>TM</sup> Communication Manager Evolution Server, Avaya Aura<sup>TM</sup> Communication Manager Feature Server does not support traditional telephones such as DCP, analog and H.323 registered directly to it.

For the sample configuration, Avaya Aura<sup>TM</sup> Session Manager runs on an Avaya S8800 Server, Avaya Aura<sup>TM</sup> Communication Manage Feature Server runs on an Avaya S8300D Server with an Avaya G450 Media Gateway and the 96xx SIP telephones are registered to Avaya Aura<sup>TM</sup> Session Manager. The Avaya (formerly Nortel) Communication Server 1000E runs on a co-res Communication Server 1000E version 6.0 and supports digital and UNIStim (IP) telephones. The results in these Application Notes should be applicable to other Avaya servers and media gateways that support Avaya Aura<sup>TM</sup> Communication Manager 6.0 Feature Server and Avaya Communication Server 1000E 6.0.

As shown in **Figure 1** below, the Avaya 96xx SIP telephones are registered to Avaya Aura<sup>TM</sup> Session Manager but supported by the Avaya Aura<sup>TM</sup> Communication Manager. Telephones in the 6664xxx utilize the Avaya Aura<sup>TM</sup> Communication Manager Evolution Server while telephones in the 666300x range utilize the Avaya Aura<sup>TM</sup> Communication Manager Feature Server.

The Avaya (formerly Nortel) 1140e/1165e UNIstim (IP) and 3903/3904 digital telephones are supported by the Avaya Communication Server 1000E (CS1000E) PBX. SIP trunks are used to connect these two systems to Avaya Aura<sup>TM</sup> Session Manager, using its SM-100 (Security Module) network interface. All inter-system calls are carried over these SIP trunks. Avaya Aura<sup>TM</sup> 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<sup>TM</sup> System Manager, which can manage multiple Avaya Aura<sup>TM</sup> Session Managers by communicating with their management network interfaces.



**Figure 1 – Sample Configuration** 

Avaya Aura<sup>™</sup> Communication Manager's Uniform Dial Plan (UDP) and AAR tables in conjunction with the Avaya Communication Server 1000E Coordinated Dial Plan (CDP) feature are used to implement extension-extension 7-digit dialing between systems. Unique extension ranges are associated with Avaya Aura<sup>™</sup> Communication Manager Feature Server telephones (6663xxx) and Avaya Communication Server 1000 phones (777xxx). Avaya Aura<sup>™</sup> Communication Manager Evolution Server endpoints (6664xxx) are included in **Figure 1** in order to show the complete solution however the actual administration is covered in a separate Application Note. See **Reference [12]** in **Section 10**.

These Application Notes focus on configuration of the SIP trunks, configuration of the 96xx SIP phones as 'users' on Avaya Aura<sup>TM</sup> Session Manager and call routing between the SIP Entitites. It's important to understand that the 96xx phones are registered directly to Avaya Aura<sup>TM</sup> Session Manager with Avaya Aura<sup>TM</sup> Communication Manager supplying 'call features' via Session Manager's **Sequenced Application** capability.

# 2. Equipment and Software Validated

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

Hardware Component	Software/Firmware Version
Avova 58800 Samor	Avaya Aura <sup>TM</sup> Session Manager R6.0
Avaya S8800 Server	Avaya Aura <sup>TM</sup> System Manager R6.0
Avaya S8300D Server	Avaya Aura <sup>TM</sup> Communication Manager
Avaya 58500D Server	6.0-345 + SP1*
Avaya G450 Media Gateway	FW 32.10.12
Avaya 9630/9650 one-X® Deskphone (SIP)	2.6
Avaya Communication Server 1000E CP+PM	Release 6.0.18
Avaya Network Routing Server (NRS)	6.0
Avaya 3903/3904 Digital Telephones	NA
Avaya 1140e UNIstim Telephone	0625C7J
Avaya 1165e UNIstim Telephone	0626C7J

# 3. High-level List of Tasks:

The following is a high-level list of tasks that will be covered in this document:

- 1) Configure Communication Manager Feature Server to communicate with Session Manager using the SIP protocol.
- 2) Configure Communication Manager and the CS1000E as SIP nodes in Session Manager via System Manager.
- 3) Configure SIP routing in Session Manager.
- 4) Configure Communication Manager in System Manager as an administrable element.
- 5) Add SIP users/endpoints to Session Manager using System Manager.
- 6) Configure 96xx SIP phones to register to Session Manager.
- 7) Configure the CS1000E Network Routing Server (NRS) to communicate with the CS1000E Signaling Server and Call Server.
- 8) Configure the CS1000E Call Server to route calls to 666xxxx to the NRS.
- 9) Configure the NRS to route 666xxxx calls to Session Manager

# 4. Configuring Avaya Aura<sup>™</sup> Communication Manager Feature Server

This section describes the administration of Communication Manager using a System Access Terminal (SAT). Alternatively, some of the station administration could be performed using the Communication System Management application on System Manager. These instructions assume the G450 Media Gateway is already configured on Communication Manager. Some administration screens have been abbreviated for clarity.

- Verify System Capabilities and Communication Manager Licensing
- Administer network regions
- Administer IP node names
- Administer IP interface
- Administer SIP trunk group and signaling group
- Administer route patterns
- Administer numbering plan

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

#### 4.1 Verify System Capabilities and Licensing

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

#### 4.1.1 SIP Trunk Capacity Check

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

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

#### 4.1.2 AAR/ARS Routing Check

Verify that the **ARS** and **ARS/AAR Dialing without FAC** options are enabled (on page 3 of systemparameters customer options).

```
display system-parameters customer-options
OPTIONAL FEATURES
A/D Grp/Sys List Dialing Start at 01? n
Answer Supervision by Call Classifier? n
ARS? y
ARS/AAR Partitioning? y
ARS/AAR Dialing without FAC? y
ASAI Link Core Capabilities? y
DCS Call Coverage?
```

#### 4.1.3 Enable Private Networking and Uniform Dialing Plan

Use the **display system-parameters customer-options** command to verify that **Private Networking** and **Uniform Dialing Plan** are enabled as shown below:

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

#### 4.1.4 Configure Trunk-to-Trunk Transfers

Use the **change system-parameters features** command to enable trunk-to-trunk transfers. 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:** This feature can pose a significant security risk by increasing the chances of toll fraud, and must be used with caution. To minimize the risk, a COS can be defined to allow trunk-to-trunk transfers for a specific trunk group(s). For more information regarding how to configure a Communication Manager to minimize toll fraud, see **Reference [9]** in **Section 10**.

```
change system-parameters featuresPage1 of18FEATURE-RELATED SYSTEM PARAMETERS<br/>Self Station Display Enabled?nTrunk-to-Trunk Transfer: allAutomatic Callback with Called Party Queuing?nAutomatic Callback - No Answer Timeout Interval (rings):3
```

# 4.2 Add Node Name of Avaya Aura<sup>™</sup> Session Manager

Using the **change node-names ip** command, add the node-name and IP address for the Session Manager SM-100 interface, if not previously added during the initial install of the solution. This same screen shows the node-name for the C-LAN interface which will be used in administering a SIP signaling-group in **Section 4.4**.

change node-names	ip			Page	1 of	2
		IP 1	NODE NAMES			
Name	IP Address					
ASM1-SM100	10.80.120.28					
ASM2-SM100	10.80.120.30					
default	0.0.0.0					
gateway1	10.80.100.1					
procr	10.80.100.73					

### 4.3 Configure IP Network Regions

In the sample configuration shown in **Figure 1**, calls to/from Session Manager will be viewed by Communication Manager as calls to/from ip-network-region 2. Communication Manager and its endpoints are in ip-network-region 1. To enable communication between the two network regions requires additional administration of the **ip-network-region** and **signaling-group** forms as shown in the next few sections.

#### 4.3.1 Configure IP Network Region 1

Using the **change ip-network-region 1** command, set the **Authoritative Domain** to the correct SIP domain for the configuration. Verify the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields are set to **yes**.

```
      change ip-network-region 1
      Page 1 of 19

      IP NETWORK REGION

      Region: 1
      Authoritative Domain: avaya.com

      Name:
      Intra-region IP-IP Direct Audio: yes

      Codec Set: 1
      Inter-region IP-IP Direct Audio: yes

      UDP Port Min: 2048
      IP Audio Hairpinning? n

      UDP Port Max: 16585
      Image 1 of 19
```

Navigate to page 4 and connect ip-network-region 1 to ip-network-region 2 by typing a **y** under the **direct WAN** column for **dst rgn 2**. Select an **ip-codec-set** to be used for negotiating audio between the two regions as well. In this case ip-codec-set 2 was used. See **Section 4.3.3** for additional information on the **ip-codec-set** form.

chang	ge ip-1	networ	k-region 1	Page	4	of	20
Sour	cce Reg	gion:	1 Inter Network Region Connection Managemer	ıt	I	_	M
					G.	A	t
dst	codec	direc	<b>t</b> WAN-BW-limits Video Intervening	Dyn	А	G	C
rgn	set	WAN	Units Total Norm Prio Shr Regions	CAC	R	L	е
1	1				a	11	
2	2	У	NoLimit		n		t

#### 4.3.2 Configure IP Network Region 2

Using the **change ip-network-region 2** command, set the **Authoritative Domain** to the correct SIP domain for the configuration. Verify the **Intra-region IP-IP Direct Audio**, and **Inter-region IP-IP Direct Audio** fields are set to **yes**.

```
change ip-network-region 2Page 1 of 19IP NETWORK REGIONRegion: 2Location: 1Authoritative Domain: avaya.comName:Intra-region IP-IP Direct Audio: yesMEDIA PARAMETERSIntra-region IP-IP Direct Audio: yesCodec Set: 1Inter-region IP-IP Direct Audio: yesUDP Port Min: 2048IP Audio Hairpinning? nUDP Port Max: 16585IP Audio Hairpinning? n
```

Navigate to Page 4 and verify that ip-network-region 1 and 2 are directly connected and use ip-codec-set **2** as shown below.

change ip-r	networ	k-region 2	Page	4	of	20
Source Reg	gion:	2 Inter Network Region Connection Managemen	t	I G	Δ	M t
dst codec	direc	t WAN-BW-limits Video Intervening	Dyn	-		C
rgn set	WAN	Units Total Norm Prio Shr Regions	CAC	R I	L	е
1 <b>2</b>	У	NoLimit		n		t
2 2				a	11	

#### 4.3.3 Administer IP Codec Set

In Section 4.3.1 ip-codec-set 2 was chosen as the inter-region codec to be used for call between ipnetwork-region's 1 and 2. In the sample configuration G.711MuLaw was the preferred codec to be used for RTP audio between Communication Manager and the CS1000E, therefore ip-codec-set 2 will be configured to prefer this codec as well. Use the command **change ip-codec-set 2** to administer this codec-set.

• Audio Codec 'G.711MU' is entered as the first choice. Optionally enter in a secondary Codec like 'G.729A' to help ensure there will be two-way audio in most cases.

Leave all other fields at their defaults.

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

Solution & Interoperability Test Lab Application Notes ©2010 Avaya Inc. All Rights Reserved. Page 12 of 58 CS1KSM6CM6FS

#### 4.4 Add SIP Signaling Group

Issue the **add signaling-group n** command, where "n" is an available signaling group number, for one of the SIP trunks to the Session Manager, and fill in the indicated fields. In the sample configuration, trunk group "10" and signaling group "10" were used to connect to Avaya Aura<sup>™</sup> Session Manager. Default values can be used for the remaining fields.

• Group Type:	sip
Transport Method:	tcp <sup>(1)</sup>
• IMS Enabled?:	y Feature Server must have this set to y
• Peer Detection Enabled?	у
• Near-end Node Name:	procr node-name from Section 4.2
• Far-end Node Name:	Session Manager SM-100 node name from Section 4.2
• Near-end Listen Port:	5060
• Far-end Listen Port:	5060
• Far-end Network Region:	2
• Far-end Domain:	Authoritative Domain from Section 4.3.1
• Enable Layer 3 Test:	у
Session Estab. Timer:	<b>3</b> <sup>(2)</sup>

display signaling-group 10

SIGNALING GROUP

Group Number: 10 <b>IMS Enabled? y</b> Q-SIP? n IP Video? n <b>Peer Detection Enable</b>	Group Type: Transport Method: ed? y Peer Server:	tcp SIP Enabled LSP? Enforce SIPS URI for SRTP?	
Near-end Node Name: Near-end Listen Port:	5060	Far-end Node Name: <b>ASM1-SM100</b> Far-end Listen Port: <b>5060</b> ar-end Network Region: <b>2</b>	
Far-end Domain: avaya.c	om		
		Bypass If IP Threshold Exceeded?	n
Incoming Dialog Loopbac	ks: eliminate	RFC 3389 Comfort Noise?	n
DTMF over IP:	rtp-payload	Direct IP-IP Audio Connections?	У
Session Establishment 7	limer(min): 3	IP Audio Hairpinning?	n
Enable Layer 3	Test? y	Initial IP-IP Direct Media?	n
H.323 Station Outgoing	Direct Media? n	Alternate Route Timer(sec):	6

 <sup>(1)</sup> TCP was used for the sample configuration. However, TLS would typically be used in production environments.
 (2) If any call originating from the SIP phone is not expected to be answered within 3 minutes such would happen if the call is made to a VDN and agents are not available within 3 minutes, this value may need to be increased.

#### 4.5 Add SIP Trunk Group

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- Group Type: sip
- **Group Name:** A descriptive name.
- TAC: An available trunk access code
- **Direction two-way** for both incoming and outgoing calls
- Service Type: tie
- **Signaling Group:** The number of the signaling group added in **Section 4.4**
- Number of Members: The number of SIP trunks to be allocated to calls routed to Session Manager (must be within the limits of the total number of trunks configured in Section 4.1.1)

		Page 1	of 21
TRUNK GROUP			
Group Type:	sip	CDR Repor	ts: y
COR:	1	TN: 1 T	AC: <b>#10</b>
Outgoing Display?	У		
	Night	Service:	
Auth Code?	n		
	S	Signaling Group	: 10
	Num	nber of Members	: 25
	Group Type: COR: Outgoing Display?	Group Type: <b>sip</b> COR: 1 Outgoing Display? y Night Auth Code? n	TRUNK GROUP Group Type: <b>sip</b> CDR Repor COR: 1 TN: 1 T Outgoing Display? y Night Service:

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

#### On Page 2, set the Preferred Minimum Session Refresh Interval to 1200.

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

add trunk-group 10			Gro	oup Type	: sip	Page	2	of	21	
TRUNK PARAMETERS										
Unicode Name:	aut	to								
				Red	irect On (	OPTIM Fail	ure	: 50	00	
SCCAN?	n	Preferred 1	Minimum	Session	5	al Loss Gr Interval(s	-		00	

On Page 3, set Numbering Format to be private. Use default values for all other fields.

add trunk-group 10 TRUNK FEATURES	Page 3 of 21
ACA Assignment? n	Measured: none Maintenance Tests? y
Numbering Format:	<b>private</b> UUI Treatment: service-provider
	Replace Restricted Numbers? n Replace Unavailable Numbers? n

#### 4.6 Administer Private Numbering

SIP Users registered to Session Manager need to be added to either the private or public numbering table on the Communication Manager Feature Server. For the sample configuration, **private** numbering was used and all extension numbers were unique within the private network. However, in many customer networks, it may not be possible to define unique extension numbers for all users within the private network. For these types of networks, additional administration may be required as described in **References** [5] and [6].

To enable SIP endpoints to send their caller ID number when dialing over a trunk you must define their extension pattern on either the **private** or **public-numbering** table. In **Section 4.5** trunk-group 10 was configured as 'private'. Use the command **change private-numbering 7** to define the caller ID number which will be sent out with the call. For the sample configuration, extension numbers in the range of 666xxxx are used on the Feature Server.

- **Ext Len:** Enter the extension length allowed by the dial plan
- **Ext Code:** Enter leading digit (s) from extension number
- **Trunk Grp:** Enter the SIP Trunk Group number for the SIP trunk between the Feature Server and Session Manager
- **Private Prefix:** Leave blank unless an enterprise canonical numbering scheme is defined in Session Manager. If so, enter the appropriate prefix

char	nge private-num	bering 7			Page 1 c	f 2
			NUMBERING - PRIVATE FORMAT		AT	
Fvt	Ext	Trk	Private	Total		
-						
Len	Code	Grp(s)	Prefix	Len		
7	6	10		7	Total Administered:	1
					Maximum Entries: 540	

#### 4.7 Administer Call Routing

There are several administration screens one must edit in order to enable 7-digit dialing from Communication Manager to Session Manager (and ultimately to the CS1000 or other PBX's) without the need to dial a Feature Access Code (FAC) like **9** or **\*9**. These steps are shown in the next few sections.

#### 4.7.1 Administer DialPlan Analysis

In the screenshot below, the following entries we added using the **change dialplan analysis** command:

- **Dialed String** 666 was added for extensions local to Communication Manager
  - 777 was added for extensions on the CS1000E
- Total Length 7
- Call Type Ext

change dial	plan an	alysis	DIAL PLA				Page	1 of	12
			ЦС	cation:	all	Pe	ercent F	ull: 2	
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call	
String	Lengt	h Type	String	Length	Туре	String	Length	Type	
0	1	attd							
1	2	dac							
2	2	fac							
666	7	ext							
777	7	ext							
8	1	fac							
9	1	fac							
*	3	dac							
#	3	dac							

#### 4.7.2 Administer Uniform Dialplan

Using the command **change uniform-dialplan 7** make the following changes:

- Matching Pattern 777 for the CS1000 & 6664 for Evolution Server endpoints
- Len 7 Length of digit string
- **Del 0** Number of digits to delete
- Net aar

change unifor	m-dialplan 7	Page	1 of 2		
	UNI				
				Percent	Full: 0
Matching		Insert	Nod	e	
Pattern	Len Del	Digits	Net Conv Num		
777	70		<b>aar</b> n		
6664	70		aar n		

#### 4.7.3 Administer AAR table

In the sample configuration the AAR table is used for two purposes: To route calls to 777xxxx (calls to the CS1000E) from Communication Manager to Session Manager as well as to route calls to 96xx SIP telephones which are registered to Session Manager and are in the 666xxxx extension range. Using the command **change aar analysis 6**, make the following changes which instruct Communication Manager to use the appropriate route-patern for a given digit string.

- Dialed String 777 & 666
- Total Min 7 Minimum number of dialed digits
- Total Max 7 Maximum number of dialed digits
- **Route Pattern** 10 (route-pattern admin shown in next section)
- Call type unku Unknown numbering plan

change aa	r analysis 6					Page 1 of 2	
		A	 GIT ANALYS Location:		ΓE	Percent Full: 1	
777 666	Dialed String	Tot Min <b>7</b> 6	 Route Pattern <b>10</b> <b>10</b>	Call Type <b>unku</b> unku	Node Num	ANI Reqd n n	

#### 4.7.4 Administer Route Pattern

The final step for enabling 7-digit dialing to Session Manager is to add the trunk group created in **Section 4.5** to a route pattern. Use the command change route-pattern 10 to add trunk-group 10 to the route pattern.

- **Pattern Name** Use a descriptive name for the route pattern
- Group No 10 Trunk-group number created in Section 4.5
- **FRL** 0 Restriction Level with 0 being the least restrictive

chai	nge 1	route	e-pat	terr	n 10									Page	1 of	3
					Patt	tern 1	Numbe	r: 10	Pat	tern 1	Name: .	ASM1-6	5.0			
							SCCAI	N? n	S	Secure	SIP?	n				
	Grp	FRL	NPA	Pfx	Нор	Toll	No.	Inse	rted						DCS	/ IXC
	No			Mrk	Lmt	List	Del	Digit	ts						QSIC	5
							Dgts								Intv	v
1:	10	0													n	user
2:															n	user
3:															n	user
4:															n	user
5:															n	user
6:															n	user
				TSC	CA-	ГSC	ITC	BCIE	Serv	/ice/F	eature	PARM	No.	Numbe	ering	LAR
	0 1	2 M	4 W		Requ	lest							0	Forma	at	
												Suk	baddr	ess		
1:	УУ	УУ	y n	n			res	t								none

#### 4.8 Configure Stations

For each SIP user to be defined in Session Manager, add a corresponding station on the Communication Manager Feature Server.

**Note:** Instead of manually defining each station using the Communication Manager SAT interface, an alternative option is to automatically generate the SIP station when adding a new SIP user in System Manager. See **Section 5.9** for more information on adding SIP users.

The phone number defined for the station will be the number the SIP user enters to register to Session Manager. Use the "**add station x**" command where x is a valid extension number defined in the system. On **Page 1** of the change station form:

- **Phone Type:** Set to "9630SIP"
- Name: Display name for user
- Security Code: Numeric password used when user logs into station. Note: this code should match the Shared Communication Profile Password field defined when adding this user in Session Manager. See Section 4.9

add statior	n 6664400		Page	1 of 6
			STATION	
Extension:	666-4400		Lock Messages? n	BCC: 0
Type:	9630SIP		Security Code: 123456	TN: 1
Port:	S00006		Coverage Path 1: 1	COR: 1
Name:	John Smith		Coverage Path 2:	COS: 1
			Hunt-to Station:	
STATION OPT	FIONS			
			Time of Day Lock Table:	
	Loss Group:	19		
			Message Lamp Ext:	666-4400
Dis	splay Language:	english	Button Modules:	0
S	Survivable COR:	internal		
Survival	ole Trunk Dest?	У	IP SoftPhone?	n
			IP Video?	n

On **Page 6**, note the following:

• -SIP Trunk : AAR which corresponds to the 666 entry from Section 4.7.3

change station 6664400	Page	6 of	6
STATION			
SIRIION			
SIP FEATURE OPTIONS			
Type of 3PCC Enabled: None			
SIP Trunk: AAR			

#### 4.9 Verify Off-Pbx Telephone Station-Mapping

Use the **display off-pbx-telephone station-mapping** command for each extension associated with SIP users defined in Session Manager to verify settings:

display off-pbx-telephone station-mapping 6664400 Page 1 of 3										
	STATIONS W	ІТН ОҒҒ-РВХ	TELEPHONE INTE	GRATION						
Station Extension	Application	Dial CC Prefix	Phone Number	Trunk Selection	Config Set	Dual Mode				
666-4400	OPS	-	6664400	AAR	1					
		-								

On Page 2, verify the following values:

- Mapping Mode: both
- Calls Allowed: all

change off-pb	x-teleph	one stati	on-mapping 666	4400	Page	2 of 3
	STATI	ONS WITH	OFF-PBX TELEPH	ONE INTEGRA	TION	
Station Extension 666-4400	Appl Name <b>OPS</b>	Call Limit <b>3</b>	Mapping Mode <b>both</b>	Calls Allowed <b>all</b>	Bridged Calls <b>none</b>	Location

#### 4.10 Save Translation

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

**Note:** After a change on Communication which alters the dial plan, synchronization between Communication Manager and Session Manager needs to be completed and SIP phones must be reregistered. To request an on demand synchronization, log into the System Manager console, navigate to **Elements**  $\rightarrow$  **Inventory**  $\rightarrow$  **Synchronization**  $\rightarrow$  **Communication System** and initiate an incremental syncronization of Communication Manager as shown below:

AVAYA	Avay	/a Aura™ :	System Mar	nager 2	Welcome, <b>admin</b> Last Logged on at May 21, 2010 6:30 PM Help   About   Change Password   <b>Log off</b>					
Home / Elements / Inventory / Synch		/ Communication S	ystem							
▼ Elements	Syne	chronize CM	1 Data and C	onfigure Oj	otions					
▶ Conferencing										
Presence	Synck	Synchronize CM Data/Launch Element Cut Through   Configuration Options								
Application Management		nd All   Collapse All	andri Elemenc dac mi	ough ( comigarade	in options (					
▶ Endpoints										
SIP AS 8.1	Syn	Synchronize CM Data/Launch Element Cut Through 💌								
▶ Feature Management	O Ito	ms   Refresh	Pofrach							
Tinventory	5 Ite									
Manage Elements		Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type				
Discovered Inventory		<u>CM-FS</u>	10.80.100.73	May 24, 2010 2:00:53 AM - 06:00	10:00 pm SUN MAY 23, 2010	Incremental				
<ul> <li>Discovery Management</li> <li>Synchronization</li> </ul>		<u>S8300D-ES</u>	135.8.19.121	May 3, 2010 2:00:57 AM - 06:00	10:00 pm SUN MAY 23, 2010	Incremental				
Communication System Messaging System		<u>S8800-CM6-</u> <u>West-</u> Evolution	10.80.111.73	May 24, 2010 2:01:00 AM - 06:00	10:00 pm SUN MAY 23, 2010	Incremental				
> Templates	<	Evolution								
Session Manager										
Events     Initialize data for selected devices       Groups & Roles     Incremental Sync data for selected devices       Licenses     Save Translations for selected devices										

# 5. Configure Avaya Aura<sup>™</sup> Session Manager

This section provides the procedures for configuring Session Manager and includes the following items:

- Administer SIP domain
- Define Logical/physical Locations that can be occupied by SIP Entitites
- Add Session Manager to System Manager
- For each SIP Entitity in the sample configuration:
  - Define SIP Entitity
  - Define Entity Links, which define the SIP trunk parameters used by Avaya Aura <sup>™</sup> Session Manager when routing calls to/from SIP Entitites
  - o Define Routing Policies, which control call routing between the SIP Entitites
  - o Define Dial Patterns, which govern to which SIP Entitity a call is routed

**NOTE:** You do not define a dial pattern or routing policy for the 96xx SIP telephones that are registered to the Feature Server.

- Administer Feature Server as a 'Sequenced Application'.
- Define the Communication Manager Feature Server as an administrable entity
- Adding SIP Endpoints/SIP users in System Manager

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "http://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and accept the Copyright Notice. Expand the **Routing** link on the left side of Navigation Menu. Select a specific item such as **SIP Entitites**. When the specific item is selected, the color of the item will change to blue as shown below:



#### 5.1 Administer SIP Domains

Expand Routing as described above and select Domains.

- Click New
- In the **General** Section, under *Name* add a domain name. Under **Notes** add a brief description.
- Click **Commit** to save.

The screen below shows the domain **avaya.com** for the sample configuration.

AVAYA	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at May 11, 2010 10:13 AM Help     Change Password   <b>Log off</b>							
Home / Routing / Domains									
<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> </ul>	Edit New Duplicate Delete More Actions								
Licenses Routing	2 Items   Refresh	Filter: Enable							
Domains	Name Type Defau	lt Notes							
Locations	🗌 <u>avaya.com</u> sip 🔲								
Adaptations	avocs.contoso.com sip								
SIP Elements	Select : All, None								
Element Links									

#### 5.2 Define Locations

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

- Name Add a descriptive name for the location
- Notes Add a brief description
- **IP Address Pattern** Enter pattern used to logically identify the location Under **Notes** add a brief description

The screen below shows the information for all locations administered on Session Manager. Notice the location created for the CS1000E.

AVAYA	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at May 11, 201 10:13 AM Help     Change Password   <b>Log of</b>		
Home / Routing / Locations				
▶ Elements	Location			
▶ Events	Edit New Duplicate Delete More Actions			
Groups & Roles	Edit New Duplicate Delete More Actions •	Commit		
Licenses				
▼ Routing	6 Items   Refresh	Filter: Enable		
Domains	Name	Notes		
Locations	Location 1 Subnet 10.80.100.x			
Adaptations	Location 1 Subnet 10.80.111.x	Location 1 Subnet 10.80.111.x		
SIP Elements	Location 1 Subnet 10.80.120.X			
Element Links	Location 1 Subnet 10.80.50.X	CS1000E		
Time Ranges	Location 1 Subnet 135.8.19.X			
Policies	Location for BCM			
Dial Patterns	Select : All, None			
Regular Expressions	Select : All, None			
Dofaulte				

The following screen shows the location information as entered for the Feature Server:

AVAYA	Avaya Aura™ System Manager 6 0	Welcome, <b>admin</b> Last Logged on at May 21, 2010 1:05 PM Help     Change Password   <b>Log off</b>
Home / Routing / Locations / Locat	on Details	
▶ Elements	Location Details	Commit Cancel
<ul><li>Events</li><li>Groups &amp; Roles</li></ul>	General	
Licenses  Routing  Domains  Locations  Adaptations  SIP Elements  Element Links  Time Ranges  Policies	Name: Location 1 Subnet 10.80     Notes:     Managed Bandwidth:     Average Bandwidth per Call:     80 Kbit/sec Location Pattern Add Remove	
Dial Patterns Regular Expressions Defaults		Filter: Enable
<ul> <li>Security</li> <li>System Manager Data</li> <li>Users</li> </ul>	* 10.80.100.*  Select : All, None	

#### 5.3 Add SIP Entitites

#### 5.3.1 Define Avaya Aura<sup>™</sup> Session Manager as a SIP Entitity

One of the first steps in properly setting up Session Manager and System Manager is to add Session Manager as SIP Entitity. Generally this is done during the initial installation of Session Manager and System manager. To do this, log in to System Manager and from the left-side navigation pane, expand the **Routing** link by selecting it, and then select **SIP Entitites**. Fill in the fields as described and shown below. Click **Commit** to complete:

- Name A descriptive name
- FQDN or IP Addr Hostname or IP address of the SM-100 interface in Session Mgr.
- Type Session Manager
- Notes Free-form text
- Location Appropriate location created in Section 5.2
- **Oubound Proxy** Leave blank
- **Time Zone** Time zone value appropriate for the physical location
- Sip Link Mon Usually set to Use Session Mgr Config though it can be
- customized on a per-element basis

AVAYA	Avaya Aura™ Systen	Welcome, <b>admin</b> Last Logged on at June 3, 2010 9:00 AM				
	60	<b>J</b>	Help   About   C	hange Password   L	.og off	
Home / Routing / SIP Entities / SIP	Entity Details					
▶ Elements	SIP Entity Details			Commit	ancel	
▶ Events	General					
Groups & Roles Licenses	* Name:	SM1				
▼ Routing	* FQDN or IP Address:	10.80.120.28				
Domains	Туре:	Session Manager 🛛 👻				
Locations	Notes:					
Adaptations						
SIP Entities	Location:	Location 1 Subnet 10.80.	120 X 🗸			
Entity Links						
Time Ranges	Outbound Proxy:		*			
Routing Policies	Time Zone:	America/Denver	*			
Dial Patterns	Credential name:					
Regular Expressions						
Defaults	SIP Link Monitoring					
▶ Security	SIP Link Monitoring:	Use Session Manager Co	nfiguration 💌			
▶ System Manager Data						

#### 5.3.2 Define Ports for Use by Avaya Aura™ Session Manager

Session Manager has the ability to translate communication between two SIP entities that 'talk' using different ports and protocols. However to do so, it's necessary to define the ports and protocols that Session Manager will need to communicate with. The screen shot shown below is the lower half of the same screen used to add/edit Session Manager as a SIP Entitity and discussed in the previous section. As shown below, two ports (**5060** & **5070**) and 2 protocols (**TCP** & **UDP**) are defined for one instance of Session Manager. TLS can also be configured:

Add	Remove				
3 Iter	ns   Refresh				Filter: Enable
	Port	Protocol	Default Domain	Notes	
	5060	ТСР 🔽	avaya.com 🕑		
	5060	UDP 💌	avaya.com 💌		
	5070	TCP 🔽	avocs.contoso.com 💌		
Selec	t : All, None				

\* Input Required

Commit Cancel

#### 5.3.3 Add Avaya Aura<sup>™</sup> Session Manager to Avaya Aura<sup>™</sup> System Manager

To complete the linkage between System Manager and Session Manager it's necessary to identify the SIP Entitity created in the previous section as an instance of Session Manager to System Manager. Generally this is done during the initial installation of System Manager and Session Manager.

As shown below, expand the **Elements** menu on the left pane then select **Session Manager** then **Session Manager Administration**. Then click **New** (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 Session Manager
- **Description**: Descriptive comment (optional)
- Management Access Point Host Name/IP Enter the IP address of the Session Manager <u>management</u> interface (not the SM-100 interface address).

Under Security Module:

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

Use default values for the remaining fields. Click **Commit** to add this Session Manager. The screen below shows the resulting Session Manager definition.

AVAYA	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at May 11, 2010 1:18 PM Help   About   Change Password   <b>Log off</b>
Home / Elements / Session Manage	r / Session Manager Administration / Edit Session Manager	
Elements  Conferencing  Presence  Application Management	Edit Session Manager General   Security Module   NIC Bonding   Monitoring   CDR   Pers	Commit Cancel
Endpoints SIP AS 8.1	General 🕏	
Feature Management  Inventory  Templates  Session Manager  Dashboard  Session Manager	SIP Entity Name  SM1 Description Session Manag *Management Access Point Host Name/IP 10.80.120.27 *Direct Routing to Endpoints Enable •	er 6.0 #1
Administration Communication Profile Editor Network Configuration Device and Location Configuration Application Configuration System Status System Tools Events Groups & Roles Licenses	Security Module S SIP Entity IP Address 10.80.120.28 *Network Mask 255.255.0 *Default Gateway 10.80.120.1 *Call Control PHB 46 *QOS Priority 6 *Speed & Duplex Auto VLAN ID	

# 5.3.4 Define a SIP Entitity for Avaya Aura<sup>™</sup> Communication Manager Feature Server

The following screen shows the addition of Communication Manager Feature Server as a SIP Entitity.

- Name A descriptive name
- FQDN or IP Addr near-end node IP used on the signaling-group form from Section 4.2
- Type
- Notes Free-form text
- Location Appropriate location created in Section 5.2
- **Oubound Proxy** Leave blank
- **Time Zone** Time zone value appropriate for the physical location
- Sip Link Mon Usually set to Use Session Mgr Config though it can be
- customized on a per-element basis

CM



Avaya Aura™ System Manager

Welcome, **admin** Last Logged on at June 3, 2010 9:00 AM

	6.0		About   Change Password   Log off
Home / Routing / SIP Entities / SIP	Entity Details		
▶ Elements	SIP Entity Details		Commit Cancel
▶ Events	General		
Groups & Roles		8300D-FeatServ	7
Licenses <b>T</b> Routing	* FQDN or IP Address: 10	0.80.100.73	7
Domains	Туре: С	CM 💌	
Locations	Notes: CI	M6.0 Feature Server	7
Adaptations			
SIP Entities	Adaptation:	*	
Entity Links			1
Time Ranges	Location:	<b>*</b>	]
Routing Policies	Time Zone: 🔺	merica/Denver	<b>~</b>
Dial Patterns	Override Port & Transport with DNS SRV:	]	
Regular Expressions	* SIP Timer B/F (in seconds): 4		
Defaults	* SIP TIMER BYF (III seconds): 4		
▶ Security	Credential name:		
🕨 System Manager Data	Call Detail Recording: n	ione 💌	
▶ Users			

#### 5.3.5 Define a SIP Entitity for the Avaya Communication Server1000E

The following screen shows the addition of the CS1000E as a SIP Entitity.

- Name A descriptive name
- FQDN or IP Addr IP address is that of the Signaling Server
- Type Other
- Notes Free-form text
- Location Appropriate location created in Section 5.2
- **Oubound Proxy** Leave blank
- **Time Zone** Time zone value appropriate for the physical location
- Sip Link Mon Usually set to Use Session Mgr Config though it can be

customized on a per-element basis

AVAYA	Avaya Aura™ System Manage	Welcome, <b>admin</b> Last Logged on at June 3, 2010 9:00 AM
	6 0	Help   About   Change Password   Log off
Home / Routing / SIP Entities / SI	P Entity Details	
▶ Elements	SIP Entity Details	Commit Cancel
▶ Events	General	
Groups & Roles Licenses	* Name: CS1000E-West	
▼ Routing	* FQDN or IP Address: 10.80.50.10	
Domains	Type: Other	~
Locations	Notes: CS1000E-6.0	
Adaptations		
SIP Entities	Adaptation:	~
Entity Links		~
Time Ranges	Location:	
Routing Policies	Time Zone: America/Denver	▼
Dial Patterns	Override Port & Transport with DNS SRV:	
Regular Expressions		
Defaults	* SIP Timer B/F (in seconds): 4	
▶ Security	Credential name:	
▶ System Manager Data	Call Detail Recording: 🛛 none 🔍	
▶ Users		

#### 5.4 Create Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Element Link. To add an Element Link, expand **Routing** from the left-pane then select **Entity Links**. Click on the **New** button on the right-pane to create a new entry.

AVAYA	Avaya Aura™ System Manager 6.0 9:00 /m Help   About   Change Password   Log off								
Home / Routing / Entity Links									
▶ Elements	Entity	Links							
<ul><li>▶ Events</li><li>▶ Groups &amp; Roles</li></ul>	Edit	New Duplicate Del	ete	More Action	is 🔹	Commit			
Licenses Trouting	13 Items   Refresh Filter: Enable								
Domains Locations		Name	SIP Entity	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
Adaptations		<u>ASM1 CM1-</u> 135.8.19.121 5060 TCP	1 SM1	тср	5060	Avaya-CM	5060	2 2	
SIP Entities Entity Links		ASM1-CS1000E	SM1	тср	5060	CS1000E- West	5060	V	
Time Ranges Routing Policies		<u>ASM1 OCS1-</u> <u>135.8.19.139 5070 TCP</u>	SM1	тср	5070	Microsoft- OCS- Mediation- Server	5070	V	
Dial Patterns		ASM1 to BCM-450	SM1	UDP	5060	BCM-450	5060	$\checkmark$	
Regular Expressions		BSM1 to CM-Evolution	BSM1	TCP	5060	S8800-CM 6.0 ES	5060	$\checkmark$	
Defaults		58800-CM 6 0	SM1	тср	5060	S8800-CM	5060		

Fill in the following fields in the new row that is displayed:

• Name: A descriptive name. • SIP Entitity 1 Select the Session Manager. • Protocol Select TCP, TLS or UDP from the dropdown Port number to which the other system sends SIP requests • Port • SIP Entitity 2 Select the name of the other system. Port number on which the other system receives SIP requests • Port • Trusted Check this box. Note: If this box is not checked, calls from the associated SIP Entitity specified in Section 5.3 will be denied.

Click **Commit** to save each Element Link definition. The following screens illustrate the Entity Links for Communication Manager Feature Server and the CS1000, both of which use port 5060 and TCP to communicate with Session Manager.

▶ Elements	Entity Links					Commit	Cancel
▶ Events							
▶ Groups & Roles							
Licenses							
▼ Routing	1 Item   Refresh					Filter:	Enable
Domains	Name	SIP Entity	Protocol	Port	SIP Entity 2	Port	Trusted
Locations	Name	1	Protocol	FUR	SIF Endly 2	FULL	
Adaptations	* SM-to-CM_FS	* SM1 🔽	ТСР 🔽	* 5060	* S8300D-FeatServ 👻	* 5060	<ul><li>✓</li></ul>
SIP Entities	<						>
Entity Links							

▶ Elements	Entity Links						Commit	Cancel
➤ Events								
► Groups & Roles								
Licenses								
▼ Routing	1 Item   Refresh						Filter	: Enable
Domains	Name	SIP Entity	Protocol	Port	SIP Entity 2		Port	Trusted
Locations	Name	1	Protocol	PUR	SIP Enuty 2		PUFL	
Adaptations	* ASM1-CS1000E	* SM1 🔽	ТСР 🔽	* 5060	* CS1000E-West	*	* 5060	<b>~</b>
SIP Entities	<							>
Entity Links								

#### 5.5 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5.3**. Only a routing policy for the CS1000 will be added. For 96xx SIP telephones registered to Session Manager, the necessary SIP communication between Session Manager and Feature Server happens as a result of administering a 'Sequenced Application' shown in **Section 5.7**.

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:

- **General** Enter a descriptive name in **Name**.
- SIP Entitity as Destination Click Select, and then select the appropriate SIP Entitity to which this routing policy applies.
   Time of Day Click Add, and select the default 24/7 time range.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for the Communication Server 1000:

AVAYA	Avaya Aura™ System Manager 6.0					Welcor	Welcome, <b>admin</b> Last Logged on at May 11, 2010 2:18 PM Help     Change Password   Log of				
Home / Routing / Policies / Policy D	etails										
<ul> <li>Elements</li> <li>Events</li> <li>Groups &amp; Roles</li> </ul>	Routing Policy Details									(	Commit Cancel
Licenses		* Nan	e to (	CS1000E				1			
▼ Routing											
Domains		Disable	:d:								
Locations		Note	25:								
Adaptations											
SIP Elements	SIP Element as Destinatio	n									
Element Links	Select										
Time Ranges			-	-							
Policies	Name	FQDN o		iress				Type Notes			
Dial Patterns	CS1000E-West	10.80.50	.10					C	ther	CS1000E-6.0	)
Regular Expressions	Time of Day										
Defaults											
▶ Security	Add Remove View G	Gaps/Overla	ps								
<ul> <li>▶ System Manager Data</li> <li>▶ Users</li> </ul>	1 Item   Refresh										Filter: Enable
7 0505	□ Ranking 1 ▲ Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
Help	0 24/7	Image: A start and a start	Image: A start of the start		×	Image: A start of the start	Image: A start of the start		00:00	23:59	Time Range 24/7
Help for Routing Policy Details fields	Select : All, None										
Help for SIP Entity List											
Help for Time Range List	Dial Patterns										
Help for Pattern List	Add Remove										

NHK; Reviewed: SPOC 8/18/2010

Solution & Interoperability Test Lab Application Notes ©2010 Avaya Inc. All Rights Reserved. Page 32 of 58 CS1KSM6CM6FS

#### 5.6 Add Dial Patterns

Define dial patterns to direct calls to the appropriate SIP Entitity. Calls to 7-digit extensions beginning with **777** should be routed to the Communication Server 1000. 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 (or **ALL**) and routing policy from the list. Default values can be used for the remaining fields. Click **Commit** to save the dial pattern. The following screenshot shows the dial pattern for routing calls to the Communication Server 1000.

AVAYA	Avaya Aura™ System M		st Logged on at May 1 elp     Change Pass				
Home / Routing / Dial Patterns /	Dial Pattern Details						
▶ Elements	Dial Pattern Details					Com	nmit Cancel
▶ Events							
▶ Groups & Roles	General						
Licenses	* Pat	ttern: 777					
▼ Routing							
Domains		Min: 7					
Locations	*	Max: 7					
Adaptations	Emergency	Call:					
SIP Elements	SIP Do	main: -ALL-	*				
Element Links	N	lotes:					
Time Ranges		lotes.					
Policies							
Dial Patterns	Originating Locations and Routing	g Policies					
Regular Expressions	Add Remove						
Defaults	1 Item   Refresh						Filter: Enable
▶ Security			Routing		Routing		Routing
▶ System Manager Data	Originating Location Name 1 🔺	Originating Location Notes	Policy Name	Rank 2 🔺	Policy Disabled	Routing Policy Destination	Policy Notes
▶ Users	-ALL-	Any Locations	to CS1000E	0		CS1000E-West	
Help	Select : All, None						

# 5.7 Define Avaya Aura<sup>™</sup> Communication Manager Feature Server as an Administrable Entity

Before adding SIP users, the Communication Manager Feature Server must be added to System Manager as an administrable entity. This action allows System Manager to access Communication Manager over its administration interface similar to how other administration tools such as Avaya Site Administration access Communication Manager. Using this administration interface, System Manager will notify the Communication Manager Feature Server when new SIP users are added.

#### 5.7.1 Add Avaya Aura<sup>™</sup> Communication Manager as an Administerable Element

To define the Communication Manager Feature Server as an administrable entity go to **Elements**  $\rightarrow$  **Inventory**  $\rightarrow$  **Manage Elements** and select **New** (not shown). In the section titled **Application** enter in the following information:

- **Type** Select **CM** from the drop-down
- Name Enter an identifier for the Communication Manager Feature Server.
- Node Enter the IP address of the administration interface for the Feature Server

AVAYA	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at May 21, 2010 6:30 PM
	·····g-····g-·····g-·····	Help   About   Change Password   Log off
Home / Elements / Application Man	agement / Applications / Applications Details	
▼Elements ▶ Conferencing	Edit CM: CM-FS	Commit
Presence     Application Management	Application   Port   Access Point   SNMP Attributes   Attributes   Expand All   Collapse All	
Other Applications Session Manager 6.0	Application 💌	
System Manager	* Name CM-FS	
► Endpoints	* Туре СМ	
SIP AS 8.1	S8300D G450 CM6.0	
Feature Management	Description	
▶ Inventory	Description	
Templates		
▶ Session Manager	* Node 10.80.100.73	

Scroll down to the section titled **Attributes** and enter the following login information for Communication Manager:

- Login Enter a login ID that System Manager will use to login to a SAT session on Communication Manager. NOTE: This login ID should be dedicated for System Manager's use only.
- Password/Confirm Password for the login used in the above field
- Is SSH Connection Check this box if SSH access has been enbabled for SAT access to Communication Manager. SSH is enabled by default on Communication Manager.
- **Port** 5022 if SSH is enabled (default). 5023 if Telnet is enabled.

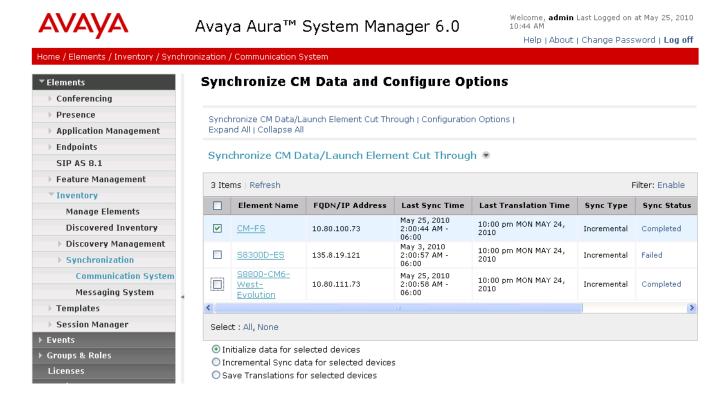
* Login	asm1	
Password	•••••	
Confirm Password	•••••	
Is SSH Connection		
* Port	5022	
Alternate IP Address		
RSA SSH Fingerprint (Primary IP)		
RSA SSH Fingerprint (Alternate IP)		
Is ASG Enabled		
ASG Key		
Confirm ASG Key		
Location		

\*Required

Commit Cancel

#### 5.7.2 Synchronize Avaya Aura<sup>™</sup> Communication Manager Data

Select Elements  $\rightarrow$  Inventory  $\rightarrow$  Manage Elements  $\rightarrow$  Synchronization  $\rightarrow$  Communication System on the left. Check the appropriate Element Name, click Initialize data for selected devices and click Now. This may take some time to complete while System Manager examines the entire configuration on Communication Manager.



# 5.8 Define an Application Sequence for Avaya Aura<sup>™</sup> Communication Manager Feature Server

In order for 96xx SIP telephones registered to Session Manager to get call features from a Communication Manager instance, it's necessary to define the Communication Manager Feature Server as a Sequenced Application. To administer this, from the menu on the left select:

**Elements**  $\rightarrow$  **Session Manager**  $\rightarrow$  **Application Configuration**  $\rightarrow$  **Applications.** Select **NEW** (not shown) to define an application for Communication Manager Feature Server. Fill in the following information as shown below:

- Name A Descriptive name for the Application
  - **SIP Entity** Select the appropriate SIP Entity (Element) from the drop-down
- CM System for SIP Entity Select CM System added in Section 5.7
- **Description** Any additional information about the Application

AVAYA	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at May 21, 2010 6:30 PM Help   About   Change Password   <b>Log off</b>
Home / Elements / Session Manage	er / Application Configuration / Application Editor	
▼ Elements	Application Editor	Commit
<ul> <li>Presence</li> <li>Application Management</li> </ul>	Application Editor	
<ul> <li>Endpoints</li> <li>SIP AS 8.1</li> <li>Feature Management</li> <li>Inventory</li> <li>Templates</li> <li>Session Manager</li> <li>Dashboard</li> <li>Session Manager</li> <li>Administration</li> </ul>	Name       CM-FS-Seq-App         *SIP Entity       SB300D-FeatServ       v         *CM System for SIP Entity       CM-FS       v       Refresh       View CM Syst         Description       Feature Server       Application Attributes (optional)	¥/Add æms
Administration Communication Profile	Name         Value           Application Handle	
Editor  Network Configuration  Device and Location	URI Parameters	
Configuration	4	

•

Next select **Application Sequences** and define an application sequence for the Communication Manager Feature Server as shown below:

- Name
- Description
- Applications in this Sequence

A name for the Application Sequence

More descriptive info for the same Application Sequence

Select the + symbol next to the **Available Application** to be used in this sequence. This will add the Application to the **Applications in this Sequence** section as shown below

AVAVA	Avava Aur	a™ System Mana	ader 6.0 Welco	ome, <b>admin</b> Last Logged PM	on at May 21, 2010
	,	, , 5			assword   Log off
Home / Elements / Session Manager	/ Application Configur	ation / Application Sequence Ed	itor		
▼ Elements	Applicatio	on Sequence Edito	-		Commit
▶ Conferencing	Applicatio	in Sequence Euro			
Presence					
Application Management	Sequence Na	ame			
Endpoints	Name	CM-FS-Seq-App			
SIP AS 8.1	Description	CM6.0 Feature Server			
Feature Management	_				
> Inventory	Applications	in this Sequence			
Templates					
Session Manager	Move First	Move Last Remove			
Dashboard	1 Item				
Session Manager	Sequenc				
Administration	🗌 🛛 Order (fi		SIP Entity	Mandatory	Description
Communication Profile	last)	CM ER Reg App	S8300D-FeatServ		Feature Serve
Editor		CM-FS-Seq-App	S6300D-reatServ		reature Serve
Network Configuration	Select : All, Non	e			
Device and Location					
Configuration 4	Available App	olications			
* Application Configuration					
Applications	3 Items   Refresh	ı			Filter: Er
Application Sequences	Name		SIP Entity	Description	
Implicit Users	+ CM-FS-Sec	n-Ann	S8300D-FeatServ	Feature Server	
System Status		M6-ES-APP	Avaya-CM		
> System Tools		6-Evolution App	S8800-CM 6.0 ES	Evolution app for !	96XX SIP
▶ Events		++-			
▶ Groups & Roles					
Licenses	*Required				Commit Ca

#### 5.9 Add SIP Users

Add SIP users corresponding to the 96xx SIP station defined in Section 4.7. Alternatively, use the option to automatically generate the SIP stations on Communication Manager Feature Server when adding a new SIP user. To begin entering user info, from the left pane navigate to, Users  $\rightarrow$  Manage Users and select New (not shown)

**<u>Step 1</u>**: Enter values for the following required attributes for a new SIP user in the **General** section of the new user form.

- Last Name: Enter last name of user
- **First Name:** Enter first name of user

Ανανα	Avaya Aura™ System Manager 6.0	Welcome, <b>admin</b> Last Logged on at May 24, 2010 7:14 PM
		Help   About   Change Password   Log off
Home / Users / Manage Users / Use	er Edit	
▶ Elements		
▶ Events	User Profile Edit: 6663000@avaya.com	Commit
▶ Groups & Roles		
Licenses	General   Identity   Communication Profile   Roles   Override Permissio 	ins   Group Membership   Default Contact List   Prival
▶ Routing	Expand All   Collapse All	
▶ Security	General 💌	
▶ System Manager Data	General .	
▼ Users	* Last Name: Skywalker	
Manage Users	* First Name: Luke	
Public Contact Lists	Middle Name:	
Shared Addresses		
System Presence ACLs	Description:	
Hele	Administrator	
Help	Communication Use	r
Help for Edit User	Agent	
Help for New Private Contact	User Type: Supervisor	
Help for Edit Private Contact	Resident Expert     Service Technician	
Help for Delete Private Contact	Lobby Phone	

**<u>Step 2:</u>** Enter values for the following required attributes in the **Identity** section.

<b><u>tep 2.</u></b> Effet values for the following fo	quired attributes in the <b>ruentity</b> section.
Login Name:	Enter extension xxx@sip domain defined in
	Section 5.1. This field is the primary handle of the user
• Authentication Type:	Select Basic
• SMGR Login Password:	Enter an alphanumeric password which will be used to log into the System Manager application
Confirm Password:	Repeat value entered above
Shared Comm. Profile Pass.:	Enter a numeric value which will be used by the SIP phone to login to Session Manager. <i>Note</i> : this field must match the <b>Security Code</b> field on the station form defined in <b>Section 4.7.</b>
Confirm Password:	Repeat numeric password

Identity 💌	
* Login Name:	6663000@avaya.com
* Authentication Type:	Basic 💌
Change Password	1
Shared Communication Profile Password:	••••••• Edit
Source:	local
Localized Display Name:	Skywalker, Luke
Endpoint Display Name:	Skywalker, Luke
Honorific:	
Language Preference:	English 💌
Time Zone:	Eastern Time (US & Canada)

**<u>Step 3:</u>** Scroll down to the **Communication Profile** section and expand the view by selecting the icon. There should already be one profile called **Primary** which is already defined as the default. Select **New** to define a **Communication Address** for the new SIP user. Enter values for the following required attributes:

- Type: Select SIP
- **SubType:** Select username
- Handle: Enter extension number
- **Domain:** Enter SIP domain defined in **Section 5.1**

Once the above information is entered select **Add** to create the new Communication Address. The screen below shows the completed information when adding a new SIP user to the sample configuration.

- Type: Select Avaya SIP
- Fully Qualified Address extension@domain

Communication Profile 💌					
New Delete Done Cancel					
Name					
Primary					
Select : None					
* Name: Prin	ary				
Default : 🗹					
Communication Address 💌					
New Edit Delete					
Туре	Handle	Domain			
Avaya SIP	6663000	avaya.com			
Select : All, None					
۲ Fully Qualified Add *	ype: Avaya SIP ♥ ress: 6663000 @	avaya.com 💌	Add Cancel		

**Step 4:** Scroll down to the **Session Manager Profile** section and expand the view by selecting the **P** icon. Assign the user to a **Primary Session Manager** instance and the **Application Sequence** defined in **Section 5.8** for Communication Manager Feature Server. The **Application Sequence** must be used for both the originating and terminating sequence. Select the appropriate Location value from the drop-down.

Session Manager Profile				
* Primary Session Manager	SM1 🗸	Primary	Secondary	Maximum
Primary Session Manager		25	0	25
Secondary Session Manager	(None) 🗸	Primary	Secondary	Maximum
Secondary Session Manager	(None)			
Origination Application Sequence	CM-FS-Seq-	-Арр	~	
Termination Application Sequence	CM-FS-Seq-	-Арр	~	
Survivability Server	(None)		*	
* Home Location	Location 1 S	Subnet 10.8	B0.100.x 🔽	

**<u>Step 5:</u>** Scroll down to the **Endpoint Profile** section and expand the view by selecting the **•** icon. Enter values for the following required attributes of the **Endpoint Profile** section:

and the following required	autioutes of the Enupoint Frome section.
• System:	From the drop-down select the managed instance of the
	Communication Manager defined in Section 5.8.
• Use Existing Endpoints:	Enter checkmark if station was already created per Section 4.x.
	Else, station will automatically be created
• Extension:	Enter extension number
• Template:	Select template for type of SIP phone.
• Security Code:	Enter numeric value which will be used to logon to SIP
	phone
	Note: this field must match the value entered for the
	Shared Communication Profile Password field.
• Port:	Select <b>IP</b> from the drop-down
Delete Endpoint on Unas	sign of Endpoint from User
	Enter checkmark to automatically delete station from
	Communication Manager when the User Profile is removed in
	System Manager

The screen below shows the information when adding a new SIP user to the sample configuration.

🗹 Endpoint Profile 💌			
* System	CM-FS	~	
Use Existing Endpoints			
* Extension	<b>Q</b> 6663000	Endpoint Editor	]
Template	Select/Reset	8	٢
Set Type	9620SIP		
Security Code	•••••		
* Port	<b>Q</b> \$00000		
Voice Mail Number			
Delete Endpoint on Unassign of Endpoint from User			

## 6. Configure 96xx SIP Deskphone

Before configuring the 96xx SIP Deskphone, please refer to **reference** [7] for a more complete explanation on setting up these telephones. Also it's important to realize that the 96xx phones support both H.323 and SIP firmware so it is necessary to ensure that SIP firmware has been loaded on the phone. At a minimum, the following parameters must be set.

- IP address, subnet mask, default gateway of the phone itself.
- SIP domain
- SIP Proxy Server Address (in this case: Session Manager)
- Username (usually the extension number like 666-4400)
- Password

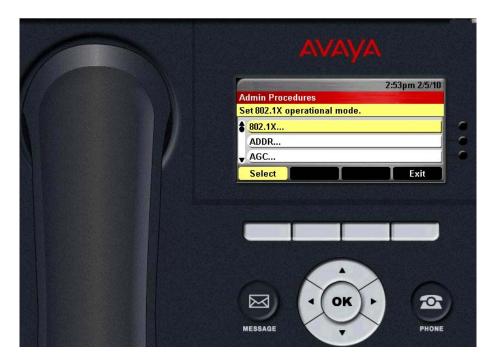
All but the last two values can configured with a combination of DHCP and the **46xxsettings.txt** file or by manually programming these values directly on the phone itself. The following sections illustrate how to set these values manually on the phone itself via the keypad.

#### 6.1 Configure IP Address, Subnet Mask & Default Gateway

To access the 96xx setup screens shown below press the following keys on the keypad: **Mute-c-r-a-f-t** # (mute-2-7-2-3-8-#).

The screen shown below will appear on the phone.

**Note:** These screenshots are from a 9650C telephone though all 96xx phones use the same basic settings.



Using the phone's down arrow, scroll down one row and select **ADDR...**. The following screen appears:



Using the up and down scroll buttons, select the appropriate fields for editing, pressing the **Change** button to edit each field. Scroll down further to see the fields for Mask (subnet mask), HTTPS & HTTP File Server, DNS Server, 802.1Q, VLAN ID, and VLAN Test.

The last row on this screen is **Host To Ping**. If needed, enter in an IP address and press the **PING** key to test network connectivity. Press the **Bksp** button when the test is complete to remove the IP address.

2:39pm 5/24/10
123
Ping
0.0.0.0
Auto 🚸
1

Shown below is a screenshot of a successful test to 10.80.120.28:

6663000	2:40pm 5/24/10
Address Procedures	
Successfully cont 10.80.111 Sent: 4 / Rece	.73

Once you have completed programming on the above screens be sure to press **Save** to get back to the main screen and save your configuration.

#### 6.2 Configure SIP Global and Proxy Settings

The next steps are to configure the SIP Domain and the SIP Proxy server address. From the main admin screen, scroll down and select **SIP...** 

And in the second se	3:28pm 2/5/10
Admin Procedures	
Configure SIP call settings.	
▲ SIG	
SIP	
SNTP	
Select	Exit

In the screen that appears select **SIP Global Settings**, The options as shown in the image below will appear. Verify the following are set:

Provied

- Sip Mode
- SIP Domain
- Avaya Environment
- **Registration Policy** alternate or simultaneous
- Failback Policy
- User ID field

I I O'MICU	
In this case	e set to avaya.com
Auto	
alternate	or simultaneous
auto	
no	

and the second division of the second division of the	3:36pm 2/5/10		3:34pm 2/5/10	A REAL PROPERTY AND A REAL	3:37pm 2/5/10
SIP Global Settings	•	SIP Global Settings	123	SIP Global Settings	123
Use <b>I</b> to change setting.		Enter IP address of Avaya config server. Enter IP address of device to Ping			
SIP Mode:	Proxied 🚸	A Reg. Policy	alternate 🚸	Avaya Config Server:	
SIP Domain:	avaya.com	Failback Policy	auto 🚸	User ID Field	No 🚸
🚽 Avaya Environment:	Auto 🚸	🚽 Avaya Config Server: [	]	Host to Ping: [	]
Save Change	Cancel	Save	Cancel More	Cance	el More

Select the Save button when complete. Next, select SIP Proxy Settings.

A design of the second se	3:42pm 2/5/10
SIP Settings	A CONTRACTOR OF
Press Select for choices.	
SIP Global Settings	
SIP Proxy Settings	
Select	Back

Select **NEW** and the following screen appears. Set fields according to your configuration. In this case:

- SIP Proxy Server Address of Session Manager SM-100 interface
- **Transport Type TCP** (can be TLS or UDP as well)
- **SIP Port 5060** for TCP & UDP, 5061 for TLS

10:57 am 5/12/10
•
10.80.120.28
ТСР 🚸
5060
Back
p SAC
XUA

Select **Save** when complete. Select **Back** two times to get back to the main menu. Select **Exit** to complete the configuration. The phone will reboot.

#### 6.3 Login Phone to Avaya Aura<sup>™</sup> Session Manager

Once the phone has rebooted, a login screen will be presented. Enter the following information:

- Username Extension number/User created in Section 5.9
- **Password** Password as it was programmed when creating a SIP user in Section 5.9

AVAYA	
And Personal Academic Street,	2:50pm 5/24/10
Login	123
Enter Password and press Enter.	
Username: 6663000	
Password: [******	
Enter Bksp 123	

Select Enter and the phone will login to Session Manager immediately. Shown below is a successfully logged in 9650C phone:



# 7. Configure the Communication Server 1000

Avaya Communication Server 1000 uses the Network Routing Server (NRS) to provide SIP and H.323 signaling interfaces to IP networks. The NRS communicates with the CS1000E Signaling Server over a private Ethernet interface. There can be one or more NRS supported CS1000E instance. The applications that can run on the CS1000e'S CP+PM processing module include the following:

Call Server	Provides the primary PBX functionality
NRS Server	Provides routing information for SIP call to/from the
	CS1000
• SIP Signaling Gateway (SSG)	Provides SIP signaling for IP networks.
• H.323 Gateway	Provides H323 Redirect & Registrar service
	components.
• NRS Manager	Provides web interface for NRS management.
• Element Manager	Provides web interface for system administrative
	tasks.

The Communication Server 1000 used in the interoperability test configuration contained one NRS and Call Server co-resident on the same CS1000E server blade. The Element Manager web interface was used to configure system resources such as SIP virtual routes and trunks, and the NRS Manager was used to configure the routing for SIP devices.

**NOTE:** The specific steps to configure the CS1000E with Avaya Aura Session Manager routing calls to Avaya Aura<sup>TM</sup> Communication Manager Feature Server or Access Element are essentially identical and are therefore not covered in this document.

See **Reference** [12] in Section 10 for the specific Applications Notes that describe the CS1000 configuration.

## 8. Verification Steps

This section provides the tests that can be performed on Communication Manager 6.0 and Session Manager to verify proper configuration of Communication Manager, Session Manager, and Communication Server 1000.

### 8.1 Verify Avaya Aura<sup>™</sup> Communication Manager 6.0

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

status t	runk 10		
		TRUNK G	ROUP STATUS
Member	Port	Service State	Mtce Connected Ports Busy
0010/001		in-service/idle	no
0010/002	T00227	in-service/idle	no
0010/003	T00228	in-service/idle	no
0010/004	Т00229	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 4.4**. Verify the signaling group is **in-service** as indicated in the **Group State** field shown below.

status signaling-group 10 STATUS SIGNALING GROUP

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

Make a call between Communication Manager and the CS1000E. Verify which trunks are in use by running the command **status trunk x** where **x** is the number of the SIP trunk group created in **Section 4.5**.

110.									
status tr	unk 10								
	TRUNK GROUP STATUS								
Member :	Port	Service State	Mtce Busy	e Connected Ports					
0010/018 * 0010/019 * 0010/020 * 0010/021 * 0010/022 *	T00019 T00020 T00021 T00022	<pre>in-service/idle in-service/idle in-service/idle in-service/idle in-service/idle</pre>	no no no no						
0010/023 ' 0010/024 ' 0010/025 '	Т00024	<pre>in-service/idle in-service/idle in-service/active</pre>	no no no	01A1201					

NHK; Reviewed: SPOC 8/18/2010

Solution & Interoperability Test Lab Application Notes ©2010 Avaya Inc. All Rights Reserved. Page 51 of 58 CS1KSM6CM6FS Verify the status of connected SIP trunks by using the **status trunk x/y**, where **x** is the number of the SIP trunk group from **Section 4.5** to reach Session Manager, and **y** is the member number of a connected trunk. As shown above trunk member 25 is in use.

Verify on Page 1 that the **Service State** is **in-service/active**. On Page 2, verify that the IP addresses of the C-LAN and Session Manager are shown in the **Signaling** section. In addition, the **Audio** section shows the G.711 codec and the IP addresses of the Communication Manager and CS1000E endpoints. The **Audio Connection Type** displays **ip-direct**, indicating direct (or 'shuffled') media between the two endpoints.

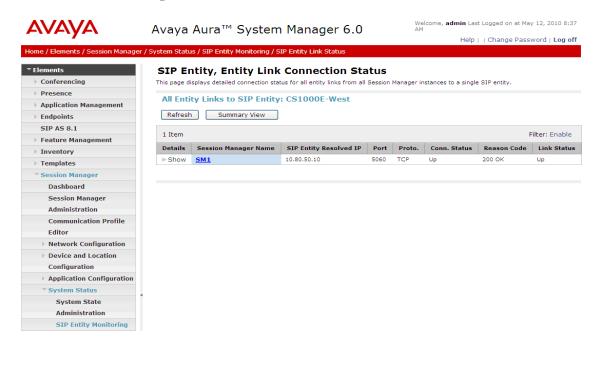
status trunk 10/25	Page 1 of 4
TR	UNK STATUS
Trunk Group/Member: 0010/025 Port: T00025 Signaling Group ID: 10	Service State: <b>in-service/active</b> Maintenance Busy? no
IGAR Connection? no	
Connected Ports: 01A1201	
status trunk 10/25	Page 2 of 4
	CALL CONTROL SIGNALING
Near-end Signaling Loc: 01A0417	
Signaling IP Address	Port
Near-end: 10.80.111.76	: 5060
Far-end: 10.80.120.28	: 5060
H.245 Near:	
H.245 Far:	
H.245 Signaling Loc:	H.245 Tunneled in Q.931? no
Audio Connection Type: ip-tdm	Authentication Type: None
Near-end Audio Loc: 01A0201	Codec Type: G.711
Audio IP Address	Port
Near-end: 10.80.111.77	: 25808
Far-end: 10.80.100.39	: 5004

#### 8.2 Verify Avaya Aura<sup>™</sup> Session Manager

Log in to System Manager. From the left-pane navigate to **Elements**  $\rightarrow$  **Session Manager**  $\rightarrow$  **System Status** \_\_> **SIP Entity Monitoring** to verify that none of the links to the defined SIP entities are down.

Αναγα	Avaya Aura™	<sup>™</sup> System Mai	nager 6.0	AM	gged on at May 12, 2010 8:37 Change Password   <b>Log off</b>
Home / Elements / Session Manager	/ System Status / SIP Enti	ity Monitoring			
	This page provides a sur	-	Status Summa SIP entity link monitoring Manager Instances	•	
SIP AS 8.1	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
Feature Management	SM2	1/1	0	0	0
Inventory     Templates	<u>SM1</u>	0/9	0	Ō	1
<ul> <li>Session Manager</li> <li>Dashboard</li> <li>Session Manager</li> </ul>	All Monitored SI Refresh	IP Entities			
Administration	8 Items		Filter: Enable		
Communication Profile Editor Network Configuration Device and Location Configuration Application Configuration System State Administration	SIP Entity Name Avaya-CM CS1000E-West IPO R6.0 Microsoft-OCS-Me ModMess5_2 S8300D-FeatServ S8800-CM 6.0 silconf-bridge				
SIP Entity Monitoring	_				

Under All Monitored SIP entities, select the appropriate SIP Entity Name and verify that the connection status is Up, as shown below for the Communication Server 1000.



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

#### 8.3 Verify 96xx SIP Phones are Registered

Log in to System Manager. Navigate to **Elements**  $\rightarrow$  **Session Manager**  $\rightarrow$  **System Status**  $\rightarrow$  **User Registrations** on the left-pane to verify which endpoints are registered with Session Manager.

AVAYA	Avay	Avaya Aura™ System Manager 6.0								12, 2010 ssword	
Home / Elements / Session Manager	/ System S	tatus / User Registrations									
▼ Elements	Use	r Registrations									
> Conferencing	Select	to send notifications to AST devices.	Click on row to display registration o	detail.							
Presence											
Application Management	Ref	resh AST Device Reboot	: Reload 🔹 Failback						Adv	anced Se	earch 💌
► Endpoints											
SIP AS 8.1	15 It	ems   Refresh   Show ALL 💌								Filter: E	inable
Feature Management	_							Re	egistere	d	
> Inventory		Address	Login Name	First Name	Last Name	Location	IP Address	Prim	Prim Sec 9	Surv	AST
Templates			22011@avaya.com	Mrs	Kensington	Location 1 Subnet 10.80.100.x					
* Session Manager		22009@avaya.com	22009@avaya.com	Number	Two	Location 1 Subnet 10.80.100.x	10.80.100.95	✓ (AC)			$\checkmark$
Dashboard		22007@avaya.com	22007@avaya.com	Vanessa	Kensington	Location 1 Subnet 10.80.100.x	10.80.100.96	☑ (AC)			
Session Manager		22008@avaya.com	22008@avaya.com	Basil	Exposition	Location 1 Subnet 10.80.100.x	10.80.100.93	✓ (AC)			
Administration			22012@avaya.com	mr	mojo	Location 1 Subnet 10.80.100.x					
Communication Profile		21003@avocs.contoso.com	21003@avocs.contoso.com	Chuck (SIP)	Bertsch	Location 1 Subnet 135.8.19.X	135.8.19.149	(AC)			$\checkmark$
Editor		21001@avocs.contoso.com	21001@avocs.contoso.com	Skip (SIP)	Hubner	Location 1 Subnet 135.8.19.X	135.8.19.148	✓ (AC)			
Network Configuration		6663000@avaya.com	6663000@avaya.com	Luke	Skywalker	Location 1 Subnet 10.80.100.x	10.80.100.39	✓ (AC)			
Device and Location		22006@avaya.com	22006@avaya.com	bench	9630phone	Location 1 Subnet 10.80.100.x	10.80.100.82	(AC)			
Configuration			6664402@avaya.com	Darth	Vader	Location 1 Subnet 10.80.100.x					
Application Configuration     System Status		21002@avocs.contoso.com	21002@avocs.contoso.com	Joe	Arias	Location 1 Subnet 135.8.19.X	135.8.19.150	✓ (AC)			
System State		6663001@avava.com	6663001@avaya.com	Han	Solo	Location 1 Subnet 10.80.100.x	10.80.100.40	☑ (AC)			
Administration		6664401@avaya.com	6664401@avaya.com	Jarjar	Binks	Location 1 Subnet 10.80.100.x	10.80.100.46	☑ (AC)			
SIP Entity Monitoring		6664400@avaya.com	6664400@avaya.com	Jabba	The Hut	Location 1 Subnet 10.80.100.x	10.80.100.45	(AC)			
Managed Bandwidth		22010@avaya.com	22010@avaya.com	Scott	Evil	Location 1 Subnet 10.80.100.x	10.80.100.90	(AC)			
Usage		- ,	- ,					( · · · ·	-	1	
Security Module Status	Sele	ct : All, None									
Registration Summary											
User Registrations	Reg	istration Detail									

#### 8.4 Verify Avaya Communication Server 1000

#### 8.4.1 Verify Status of the Signaling Server

Select IP Network  $\rightarrow$  Nodes: Servers, Media Cards  $\rightarrow$  Maintenance and Reports on the left. Click Status for the Signaling Server node to verify that it is enabled and operational.

ØRTEL	CS 100	O ELEME	INT MA	ANAGER		
A Network Services	Managing: <u>10.80.51.10</u> Us System » IP Netw	sername: admin /ork » Node Maintei	nance and Re	ports		
rtual Terminals tem arms	Node Maintena	ance and l	Reports	5		
aintenance pre Equipment	- Node ID: 1			Node IP: 10.80.50.50		Total elements: 1
eripheral Equipment	Index	ELAN IP	Туре	TN		ELAN
Network Nodes: Servers, Media Cards <u>Maintenance and Reports</u> Media Gateways Zones Host and Route Tables Network Address Translation	interop.cs1000e	10.80.51.10	Signaling Server- Nortel CPPMv1	NO TN	GEN CMD SYSLOG OM RPT	Reset Virtual Terminal Statu
toS Thresholds ersonal Directories Inicode Name Directory	10.80.51.10 : Enab	leo				

#### 8.4.2 Verify Status of an Active Call

To verify the status of an active call on the CS1000, first login to the CPPM Linux shell via SSH. Next, make a phone call between the CS1000E and Communication Manager. From the Linux shell run the command **SIPGwShow tSSG all** (additional variations of this command can be found by running **SIPGwShow** without any additional qualifiers). The results as displayed below indicate, among other things, an active call on extension **7771088** that's using **G.711MuLaw** and is talking to another endpoint with the IP address of **10.80.48.200**. Chan **1** of the **VTRK** is in use.

[admin@interop-cs1000e ~]\$ SIPGwShow tSSG all	
<pre>=== VTRK === SIPNPM Status : Active Primary Proxy IP address : 10.80.50.10 Primary Proxy port : 5060 Primary Proxy Transport : TCP Secondary Proxy IP address : 0.0.0.0 Secondary Proxy port : 5060 Secondary Proxy Transport : TCP Active Proxy : Primary :Registered Time To Next Registration : 12 Seconds Channels Busy / Idle / Total : 1 / 5 / 6 Stack version : 4.0.0.30 TLS Security Policy : Security Disabled SIP Gw Registration Trace : OFF Output Type Used : RPT Channel tracing : -1</pre>	
There are 1 sessions.HandleChan TypeDirection CallState SIPState	RxState TxState
 Ox9677300 <b>1 VTRK</b> Terminate BUSY Ringing Sent Connected Codec AirTime FS MS Fax DestNum RemoteIP	
G_711_u_law_20MS_NOVAD 78 yes m no 7771088 10.80.48.200	SIP

## 8.5 Verification Scenarios

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

- Basic calls between various telephones on the Session Manager and Communication Server 1000 can be made in both directions using G.711MU, and G.729.
- 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 of the SIP trunk call to a local endpoint on the same site, and then repeating the scenario to transfer the SIP trunk call to a remote endpoint on the other site. The supplementary calling features verified are shown below. Note that calling/called/connected party name and number display may not be consistent in some cases.
  - Unattended transfer
  - o Attended transfer
  - o Hold/Unhold
  - Consultation hold
  - o Call forwarding
  - o Conference
  - Calling number block
- During testing an issue was discovered such that if a CS1000E endpoint is forwarded to Communication Manager Feature Server, a call from a SIP endpoint to the forwarded CS1000E endpoint will fail. A SIP trace reveals Communication Manager sends a "404 originating user not found" back to the CS1000E thus preventing the call from completing. This issue is currently being investivated.

## 9. Conclusion

As illustrated in these Application Notes, Avaya Aura<sup>TM</sup> Communication Manager can interoperate with the Avaya (formerly Nortel) Communication Server 1000 using SIP trunks via Avaya Aura™ Session Manager. The following is a list of interoperability items to note:

- Service Pack 1 (SP1) for Communication Manager 6.0 is required for proper interopability with the CS1000E.
- For G.729 interoperability, G.729 must be included in the codec set in Avaya Aura<sup>™</sup> Communication Manager.
- Audio shuffling between IP telephones, including SIP endpoints, on Avaya Aura<sup>™</sup> Communication Manager and the Avaya Communication Server 1000 telephones is supported.

Page 56 of 58

• Calling/called party name and number display may not be consistent for some supplementary calling features such as call transfers, call forwarding and call conferencing.

## 10. Additional References

This section references the product documentation relevant to these Application Notes. Avaya Aura<sup>TM</sup> Session Manager:

Avaya Aura<sup>™</sup> Session Manager Overview, Doc ID 03-603473, available at [1] http://support.avaya.com.

NHK; Reviewed:	Solution & Interoperability Test Lab Application Notes	Page 56 of 58
SPOC 8/18/2010	©2010 Avaya Inc. All Rights Reserved.	CS1KSM6CM6FS

- [2] *Installing and Upgrading Avaya Aura*<sup>TM</sup> *Session Manager 6.0*, Doc ID 03-603324, available at <u>http://support.avaya.com</u>.
- [3] *Maintaining and Troubleshooting Avaya Aura*<sup>TM</sup> Session Manager, Doc ID 03-603325, available at <u>http://support.avaya.com</u>.

Avaya Aura<sup>TM</sup> Communication Manager 5.2.1:

- [4] *Administering Avaya Aura*<sup>TM</sup> *Communication Manager as a Feature Server*, Doc # 03-603479, Issue 1.2, Release 5.2 January 2010, available at <u>http://support.avaya.com</u>
- [5] *SIP Support in Avaya Aura*<sup>™</sup> *Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May, 2009, available at <u>http://support.avaya.com</u>.
- [6] *Administering Avaya Aura<sup>TM</sup> Communication Manager*, Doc ID 03-300509, June 2010, available at <u>http://support.avaya.com</u>.
- [7] Avaya one-X<sup>TM</sup> Deskphone Edition for 9600 Series SIP IP Telephones: Administrator Guide, Release 2.6, Doc ID 16-601944 Issue 5. June 2010. <u>http://support.avaya.com</u>
- [8] *Avaya Toll Fraud Security Guide*, Doc ID 555-025-600, February 2010, available at <u>http://support.avaya.com</u>

Avaya Application Notes:

- [9] Front-Ending Nortel Communication Server 1000 with an AudioCodes Mediant 1000Modular Media Gateway to Support SIP Trunks to Avaya Aura<sup>™</sup> Session Manager with Avaya Aura<sup>™</sup> Communication Manager 5.2 as a Feature Server – Issue 1.0, available at <u>http://www.avaya.com</u>.
- [10] Configuring SIP Trunks among Avaya Aura<sup>™</sup> Session Manager, Avaya Aura<sup>™</sup> Communication Manager 5.2, and Nortel Communication Server 1000 – Issue 1.1, [ available at <u>http://www.avaya.com</u>.
- [11] Configuring 96xx SIP Phones with Avaya Aura<sup>™</sup> Session Manager, 5.2 Issue 1.0 available at <u>http://www.avaya.com</u>
- [12] Configuring SIP Trunks Among Avaya Aura<sup>™</sup> Session Manager 6.0, Avaya Aura<sup>™</sup> Communication Manager Evolution Server 6.0, Avaya one-X<sup>™</sup> Deskphone Edition for 9600 Series SIP IP Telephones, and Avaya (formerly Nortel) Communication Server 1000E 6.0 available at <u>http://www.avaya.com</u>

#### Nortel CS1000E Support Documents:

- [12] IP Peer Networking Installation and Commissioning, Nortel Communication Server 1000 Release 6, Document Number NN43001-313, Version 3.02, May, 2009, available on the Nortel Communication Server Electronic Reference Library CD. <u>http://support.nortel.com</u>
- [13] Network Routing Service Fundamentals, Nortel Communication Server 1000 Release 6, Document Number NN43001-130, Version 1.03, May, 2009, available on the Nortel Communication Server Electronic Reference Library CD. <u>http://support.nortel.com</u>

#### ©2010 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>®</sup> and <sup>TM</sup> 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 <u>interoplabnotes@list.avaya.com</u>