



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2 to support Magnetic North's SIP Trunk Service - Issue 1.0**

## **Abstract**

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Magnetic North's SIP Trunk Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya Aura® Communication Manager as an Evolution Server. Magnetic North is a member of the DevConnect Service Provider program.

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

# 1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Magnetic North's SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP-enabled enterprise solution with Magnetic North SIP Trunk are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Communication Manager, Session Manager and Avaya SBCE. The enterprise site was configured to use the SIP Trunking service provided by Magnetic North.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the SIP Trunk provided by Magnetic North, calls made to analogue, digital, SIP and H.323 telephones at the enterprise
- Outgoing calls from the enterprise site completed via Magnetic North's SIP Trunk to PSTN destinations, calls made from analogue, digital, SIP and H.323 telephones
- Calls using the G.711A, G.729 and G.711MU codecs
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator and Avaya Flare® Experience for Windows Softphone clients running on a laptop PC as well as Avaya Flare® Experience running on an Avaya A175 Desktop Video Device
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Caller ID Presentation and Caller ID Restriction
- Direct IP-to-IP media (also known as "shuffling") with SIP and H.323 telephones
- Call coverage and call forwarding for endpoints at the enterprise site
- Transmission and response of SIP OPTIONS messages sent by Magnetic North's SIP Trunk requiring Avaya response and sent by Avaya requiring Magnetic North response

## 2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Magnetic North's SIP Trunk Service with the following observations:

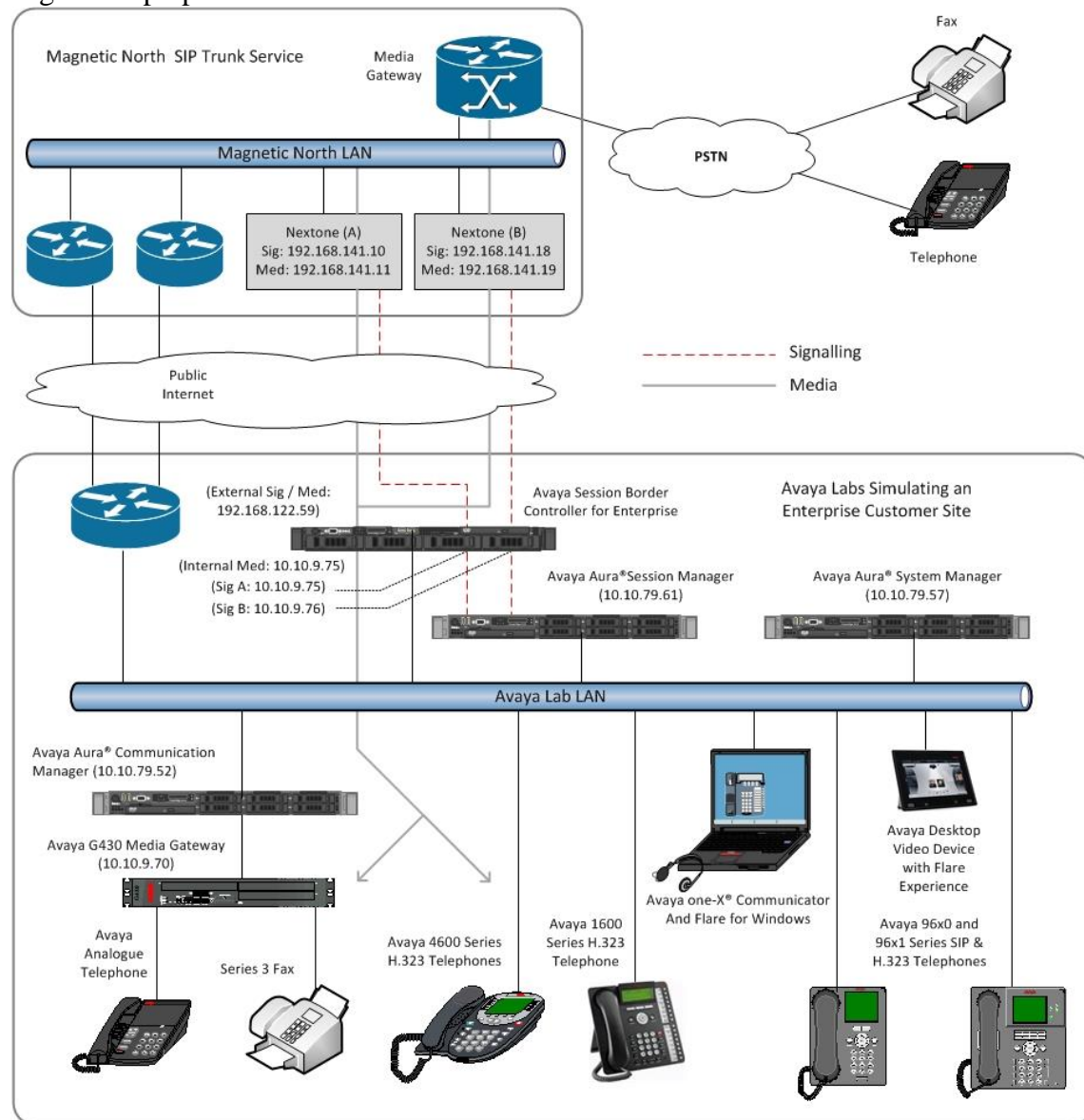
- The response from the network to an outgoing test call with an SDP with no matching codec from Communication Manager was "406 Not Acceptable". The more commonly observed response is "488 Not Acceptable Here".
- Inbound Toll-Free calls were not tested as no Toll-Free access was available for test.
- Emergency Services access was not tested as no test call was booked with the emergency Services Operator.
- When the signalling link was unavailable and the network received "500 Server Link Monitor Status Down", it re-attempted the call several times resulting in a 20 second delay before a tone was played to the caller. This failure could be more graceful.

## 2.3. Support

For technical support on Magnetic North products please visit the website at [www.magneticnorth.co.uk](http://www.magneticnorth.co.uk) or contact an authorized Magnetic North representative.

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to Magnetic North SIP Trunk. Located at the Enterprise site is an Avaya Session Border Controller for Enterprise, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya A175 Desktop Video Device running Avaya Flare® Experience (audio only), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Flare® Experience for Windows running on a laptop PC.



**Figure 1: Test Setup Magnetic North SIP Trunk to Avaya Enterprise**

**Note:** The diagram uses “Sig” for signalling and “Med” for media for brevity. The two Nextone (Genband S3) SBCs in Magnetic North’s network are referred to as “A” and “B” for clarity in the configuration described in this document. This is used in this document only and in no way reflects the naming convention used by Magnetic North.

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
<b>Avaya</b>	
Dell PowerEdge R620 running Avaya Aura® Session Manager on VM Version 8	SM-6.3.2.0.632023-e50-00
Dell PowerEdge R620 running Avaya Aura® System Manager on VM Version 8	SMGR-6.3.0.8.5682-e50-64 (Build 5682)
Dell PowerEdge R620 running Avaya Aura® Communication Manager on VM Version 8	R016x.03.0.124.0
Avaya G430 Media Gateway	FW 33.13.0
Avaya Session Border Controller Advanced for Enterprise Server	6.2.0.Q48
Avaya 1616 Phone (H.323)	1.302
Avaya 4621 Phone (H.323)	2.902
Avaya 9670 Phone (H.323)	3.200
Avaya A175 Desktop Video Device (SIP)	Avaya Flare® Experience Release 1.1.2
Avaya 9630 Phone (SIP)	R2.6 SP9
Avaya 9608 Phone (SIP)	R6.2 SP1
Avaya one-X® Communicator (H.323) on Lenovo T510 Laptop PC	6.1.8.06-SP8-40314
Avaya Flare® Experience for Windows (SIP) on Lenovo T510 Laptop PC	1.1.3.14
Analogue Handset	NA
Analogue Fax	NA
<b>Magnetic North</b>	
Nextone (Genband S3) SBC	5.2

## 5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP signalling associated with the Magnetic North SIP Trunk. For incoming calls, the Session Manager receives SIP messages from the Avaya SBC for Enterprise (Avaya SBCE) and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed

within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE at the enterprise site that then sends the SIP messages to the Magnetic North network. Communication Manager Configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Servers and Avaya G430 Media Gateway is presumed to have been previously completed and is not discussed here.

## 5.1. Confirm System Features

The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the Magnetic North SIP Trunk network, and any other SIP trunks used.

<b>display system-parameters customer-options</b>		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	18000	3
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	0
Maximum Video Capable IP Softphones:	18000	0
<b>Maximum Administered SIP Trunks:</b>	<b>24000</b>	<b>10</b>
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0
Maximum TN2501 VAL Boards:	128	0
Maximum Media Gateway VAL Sources:	250	1
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0

On **Page 4**, verify that **IP Trunks** field is set to **y**.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y		IP Stations? y
Enable 'dadmin' Login? y		
Enhanced Conferencing? y		ISDN Feature Plus? n
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n		ISDN-BRI Trunks? y
Enterprise Wide Licensing? n		ISDN-PRI? y
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		

## 5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SMVM1** and **10.10.79.61** are the **Name** and **IP Address** for the Session Manager SIP interface. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signalling interface to Session Manager.

display node-names ip		IP NODE NAMES
Name	IP Address	
SMVM1	10.10.79.61	
default	0.0.0.0	
procr	10.10.79.52	
procr6	::	

### 5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled (**yes**) to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled, the media stream is established directly between the enterprise end-point and the internal media interface of the Avaya SBCE.
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** is used.
- The rest of the fields can be left at default values.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1
    Location: 1          Authoritative Domain: avaya.com
        Name: default      Stub Network Region: n
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: 3329
DIFFSERV/TOS PARAMETERS
    Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
        Keep-Alive Count: 5
```



## 5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the IP Network Region form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec supported by Magnetic North was configured, namely **G.711A**.

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

Magnetic North's SIP Trunk supports T.38 for transmission of fax. Navigate to **Page 2** and define T.38 fax as follows:

- Set the **FAX - Mode** to **t.38-standard**
- Leave **ECM** at default value of **y**

change ip-codec-set 1				Page 2 of 2
IP Codec Set				
Allow Direct-IP Multimedia? n				
FAX	Mode	Redundancy	ECM: y	
Modem	t.38-standard	0		
TDD/TTY	off	0		
Clear-channel	US	3		
	n	0		

**Note:** **Redundancy** can be used to send multiple copies of T.38 packets which can help the successful transmission of fax over networks where packets are being dropped. This was not experienced in the test environment and **Redundancy** was left at the default value of **0**.

## 5.5. Administer SIP Signaling Groups

This signalling group (and trunk group) will be used for inbound and outbound PSTN calls to the Magnetic North SIP Trunk network. During test, this was configured to use TCP and port 5060 to facilitate tracing and fault analysis. It is recommended however, to use TLS (Transport Layer Security) and the default TLS port of 5061 for security. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**
- Set **Transport Method** to **tcp**
- Set **Peer Detection Enabled** to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set **Near-end Node Name** to the processor interface (node name **procr** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Far-end Node Name** to the Session Manager (node name **SMVM1** as defined in the **IP Node Names** form shown in **Section 5.2**)
- Set **Near-end Listen Port** and **Far-end Listen Port** to **5060** (Commonly used TCP port value)
- Set **Far-end Network Region** to the IP Network Region configured in **Section 5.3**. (logically establishes the far-end for calls using this signalling group as network region 1)
- Leave **Far-end Domain** blank (allows the CM to accept calls from any SIP domain on the associated trunk )
- Set **Direct IP-IP Audio Connections** to **y**
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from the Communication Manager)

The default values for the other fields may be used.

add signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Near-end Node Name: procr	Far-end Node Name: SMVM1	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group x** command, where **x** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-ntwrk**
- Specify the signalling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

add trunk-group 1		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: OUTSIDE CALL	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 1		
	Number of Members: 10		

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

add trunk-group 1		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 10000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in formats other than E.164 with leading “+”. In test, CLI was sent as the unaltered extension number and was modified using an adaptation on the Session Manager.

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UUI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n

On **Page 4** of this form:

- Set **Support Request History** to **n** as the required information for forwarded and transferred calls will be sent in the **Diversion Header** and **Transferring Party Information**
- Set **Send Transferring Party Information** to **y**
- Set **Send Diversion Header** to **y**
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by Magnetic North (this Payload Type is not applied to calls from SIP end-points)
- Set the **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on the Communication Manager extension

add trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
	Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
	<b>Send Transferring Party Information? y</b>
	Network Call Redirection? n
	<b>Send Diversion Header? y</b>
	<b>Support Request History? n</b>
	<b>Telephone Event Payload Type: 101</b>
	Convert 180 to 183 for Early Media? n
	Always Use re-INVITE for Display Updates? n
	<b>Identity for Calling Party Display: From</b>
	Block Sending Calling Party Location in INVITE? n
	Accept Redirect to Blank User Destination? n
	Enable Q-SIP? n

## 5.7. Administer Calling Party Number Information

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number in the format required. In test, calling party number was sent as the unaltered extension number and was modified using an adaptation on the Session Manager. This calling party number is sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

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

**Note:** The above configuration accepts all 4 digit numbers starting with 2, which includes all SIP and H.323 extension numbers, and passes them on with no prefix.

## 5.8. Administer Route Selection for Outbound Calls

In the test environment, the Automatic Route Selection (ARS) feature was used to route outbound calls via the SIP trunk to Magnetic North's SIP Trunk. The single digit 9 was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line.

Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

<b>change feature-access-codes</b>		Page 1 of 10
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code: *69		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 7		
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>		Access Code 2:

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit 9. A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to numbers beginning 0. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 1**.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
	0	11	14	1	pubu		n
	00	13	15	1	pubu		n
	0035391	13	13	1	pubu		n
	030	10	10	1	pubu		n
	0800	8	10	1	pubu		n
	0900	8	8	1	pubu		n
	118	3	6	1	pubu		n

Use the **change route-pattern x** command, where **x** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **1**. **Numbering Format** is applied to CLI and is used to set TDM signalling parameters such as type of number and numbering plan indicator. This doesn't have the same significance in SIP calls and during testing it was set to **unk-unk**.

change route-pattern 1													Page	1 of	3				
Pattern Number: 1													Pattern Name:						
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: 1	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	<b>unk-unk</b>	none								
2:	y	y	y	y	y	n	n		rest		none								
3:	y	y	y	y	y	n	n		rest		none								
4:	y	y	y	y	y	n	n		rest		none								
5:	y	y	y	y	y	n	n		rest		none								
6:	v	v	v	v	v	n	n		rest		none								

## 5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DDI calls to the Communication Manager extensions. The incoming digits sent in the INVITE message from Magnetic North can be manipulated as necessary to route calls to the desired extension. During test, the incoming DDI numbers were changed in the Session Manager to the Communication Manager Extension number using an adaptation. When done this way, there is no requirement for any incoming digit translation in the Communication Manager. If incoming digit translation is required, use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in Section 5.6.

change inc-call-handling-trmt trunk-group 1					Page 1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/	Number	Number	Del	Insert	
Feature	Len	Digits			

**Note:** One reason for configuring the enterprise in this way is that it was found when using national number format for CLI delivery, the message waiting indicator was not successfully sent to SIP extensions when a voice mail message was available and unread.

## 5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 2396. Use the command **change off-pbx-telephone station-mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate with station extension
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** enter the phone that will also be called (e.g. **0035386781nnnn**)
- Set the **Trunk Selection** to **1** so that Trunk Group 1 will be used for routing
- Set the **Config Set** to **1**

change off-pbx-telephone station-mapping 2396						Page	1	of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual		
Extension		Prefix			Selection	Set	Mode		
2396	EC500	-		0035386781nnnn	1	1			
-									

**Note:** The phone number shown is for a mobile phone used for testing at Avaya Labs and is in international format with international dialling prefix 00. To use facilities for calls coming in from EC500 mobile phones, the number received in Communication Manager must exactly match the number specified in the above table.

Save Communication Manager changes by entering **save translation** to make them permanent.

## 6. Configuring Avaya Aura® Session Manager

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

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

### 6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.

**AVAYA** Avaya Aura® System Manager 6.3 Last Logged on at September 25, 2013 9:57 AM  
Help | About | Change Password | Log off admin

Users	Elements	Services
<b>Administrators</b> Manage Administrative Users	<b>Communication Manager</b> Manage Communication Manager 5.2 and higher elements	<b>Backup and Restore</b> Backup and restore System Manager database
<b>Directory Synchronization</b> Synchronize users with the enterprise directory	<b>Communication Server 1000</b> Manage Communication Server 1000 elements	<b>Bulk Import and Export</b> Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
<b>Groups &amp; Roles</b> Manage groups, roles and assign roles to users	<b>Conferencing</b> Manage Conferencing Multimedia Server objects	<b>Configurations</b> Manage system wide configurations
<b>User Management</b> Manage users, shared user resources and provision users	<b>IP Office</b> Manage IP Office elements	<b>Events</b> Manage alarms, view and harvest logs
	<b>Meeting Exchange</b> Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements	<b>Geographic Redundancy</b> Manage Geographic Redundancy
	<b>Messaging</b> Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging	<b>Inventory</b> Manage, discover, and navigate to elements
	<b>Presence</b> Presence	<b>Licenses</b> View and configure licenses
	<b>Routing</b> Session Manager Routing Administration	<b>Replication</b> Track data replication nodes, repair replication nodes
		<b>Scheduler</b> Schedule, track, cancel, update and



## 6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name agreed with Magnetic North; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on the Communication Manager. Refer to **Section 5.3** for details. In test, **avaya.com** was used. Optionally, a description for the domain can be entered in the Notes field (not shown). Click **Commit** to save changes.

The screenshot shows the Session Manager web interface. On the left is a navigation menu with 'Routing' expanded and 'Domains' selected. The main content area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Domain Management' section with buttons for 'New', 'Edit', 'Delete', 'Duplicate', and 'More Actions'. Below this is a table with one item, 'avaya.com', of type 'sip'. A 'Select' dropdown is set to 'All'.

Name	Type	Notes
avaya.com	sip	

## 6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu (not shown). Under **General**, in the **Name** field, enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, \* is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the enterprise.

Home / Elements / Routing / Locations

Location Details

CommitCancelHelp ?

General

\* Name:Galway

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):2000Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):2000Kbit/Sec

\* Minimum Multimedia Bandwidth:64Kbit/Sec

\* Default Audio Bandwidth:80Kbit/sec

Alarm Threshold

Overall Alarm Threshold:80%

Multimedia Alarm Threshold:80%

\* Latency before Overall Alarm Trigger:5Minutes

\* Latency before Multimedia Alarm Trigger:5Minutes

Location Pattern

AddRemove

2 Items RefreshFilter: Enable

IP Address Pattern	Notes
* 10.10.79.*	VMWare subnet
* 10.10.9.*	Lab subnet

## 6.4. Administer Adaptations

Calls from Magnetic North are received at the enterprise in national format with a leading “0” on the Request URI. An Adaptation specific to Magnetic North is used to convert the called number to an extension number as defined in the Communication Manager before forwarding to the Communication Manager SIP Entity.

The adaptation is also used to convert the calling party number from an extension number to national format with leading “0”.

On the **Routing** tab select **Adaptations** from the left-hand menu. Click on **New** (not shown).

- In the **Adaptation Name** field, enter a descriptive title for the adaptation.
- In the **Module Name** enter **DigitConversionAdapter**. This is used for simple digit conversion adaptations.
- In the **Module Parameter** field, enter **fromto=true**. This will apply the adaptation to the From and To headers as well as the Request URI.

Home / Elements / Routing / Adaptations

**Adaptation Details** Commit Cancel

**General**

\* **Adaptation name:**

**Module name:**

**Module parameter:**

**Egress URI Parameters:**

**Notes:**

Scroll down and in the section **Digit Conversion for Incoming Calls to SM**, click on Add. An additional row will appear. This allows information to be entered for the manipulation of numbers coming from the Communication Manager. This is where the calling party number is translated from the extension number to national format for calls routing out to the PSTN.

The screenshot below shows a translation for each calling party number. This is not normally necessary where the extension number forms part of the national number. When this is the case, a simple prefix is required.

- Under **Matching Pattern** enter the minimum number of digits to identify the extension number as required. During test, this was the full extension number as each extension was translated to a national number. If the extension number forms part of the DDI number, a single digit will suffice.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the extension number.
- Under **Delete Digits** enter the number of digits to delete if the full extension number does not form part of the national number, during test all had to be deleted.
- Under **Insert Digits** enter the prefix required to make up the full national number. During test, this was the entire number
- Under **Address to Modify** choose **origination** from the drop down box to apply this rule to the From and P-Asserted-ID headers only.

**Digit Conversion for Incoming Calls to SM**

Add Remove

9 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*2000	*4	*4		*4	011385nnnn0	origination		
<input type="checkbox"/>	*2298	*4	*4		*4	011385nnnn3	origination		
<input type="checkbox"/>	*2316	*4	*4		*4	011385nnnn5	origination		
<input type="checkbox"/>	*2346	*4	*4		*4	011385nnnn2	origination		
<input type="checkbox"/>	*2396	*4	*4		*4	011385nnnn1	origination		
<input type="checkbox"/>	*2400	*4	*4		*4	011385nnnn6	origination		
<input type="checkbox"/>	*2402	*4	*4		*4	011385nnnn6	origination		
<input type="checkbox"/>	*2460	*4	*4		*4	011385nnnn7	origination		
<input type="checkbox"/>	*2611	*4	*4		*4	011385nnnn4	origination		

Select : All, None

**Note:** In the above screenshots the DDI numbers are partially obscured.

Scroll down further and in the section **Digit Conversion for Outgoing Calls from SM**, click on Add. An additional row will appear. This allows information to be entered for the manipulation of numbers going from the Session Manager to the Communication Manager. This is where the incoming number is translated from national format to the extension number as defined in the Communication Manager.

The screenshot below shows a translation for each DDI number. This is not normally necessary where the extension number forms part of the national number. When this is the case, only the digits up to the extension number need to be analysed and removed.

- Under **Matching Pattern** enter the DDI number as received from the network.
- Under **Min** and **Max** enter the Minimum and Maximum digits of the incoming DDI number.
- Under **Delete Digits** enter the number of digits to delete to leave only the extension number remaining, during test all had to be deleted as the extension number did not form part of the national number.
- Under **Insert Digits** enter digits to be inserted. During test, this was the full extension number. If the extension number forms part of the DDI number, there will be no entry required here.
- Under **Address to Modify** choose **destination** from the drop down box to apply this rule to the To and Request URI headers only.

Digit Conversion for Outgoing Calls from SM

AddRemove

10 ItemsRefresh

Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* +	* 10	* 15		* 1	00	origination ▼		
<input type="checkbox"/>	* 011385nnnn0	* 11	* 11		* 11	2000	destination ▼		
<input type="checkbox"/>	* 011385nnnn1	* 11	* 11		* 11	2396	destination ▼		
<input type="checkbox"/>	* 011385nnnn2	* 11	* 11		* 11	2346	destination ▼		
<input type="checkbox"/>	* 011385nnnn3	* 11	* 11		* 11	2298	destination ▼		
<input type="checkbox"/>	* 011385nnnn4	* 11	* 11		* 11	2611	destination ▼		
<input type="checkbox"/>	* 011385nnnn5	* 11	* 11		* 11	2316	destination ▼		
<input type="checkbox"/>	* 011385nnnn6	* 11	* 11		* 11	2400	destination ▼		
<input type="checkbox"/>	* 011385nnnn7	* 11	* 11		* 11	2460	destination ▼		
<input type="checkbox"/>	* 011385nnnn8	* 11	* 11		* 11	2501	destination ▼		

111

Select : All, None

**Note:** included in the above configuration is a conversion to remove the leading “+” from the P-Asserted-ID and To headers and insert the international dialling prefix of 00. This was done during test so that the P-Asserted-ID of incoming calls from the EC500 mobile phone would match the entry in the **off-pbx-telephone station-mapping** table defined in **Section 5.10**

## 6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. In the Magnetic North Network, two network SBCs are provided as the interface to the enterprise equipment. These are Nextone (Genband S3) SBCs and for the purposes of this document have been designated as A and B. A SIP Entity is required for each.

To add a SIP Entity, select **SIP Entities** on the left panel menu, and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of the Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **SIP Trunk** for the Avaya SBCE SIP entity
- In the **Adaptation** field (not available for the Session Manager SIP Entity), select the appropriate Adaptation from the drop down menu
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are four SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya Aura® Communication Manager SIP Entity
- Two Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entities

### 6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface.

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb navigation at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The 'Name' field is 'Session Manager BGVM1' and the 'FQDN or IP Address' field is '10.10.79.61'. The 'Type' dropdown is set to 'Session Manager'. The 'Notes' field is empty. The 'Location' dropdown is set to 'Galway'. The 'Outbound Proxy' dropdown is empty. The 'Time Zone' dropdown is set to 'Europe/Dublin'. The 'Credential name' field is empty. The 'SIP Link Monitoring' section at the bottom has a dropdown set to 'Use Session Manager Configuration'.

SIP Entity Details	
<b>General</b>	
* Name:	Session Manager BGVM1
* FQDN or IP Address:	10.10.79.61
Type:	Session Manager
Notes:	
Location:	Galway
Outbound Proxy:	
Time Zone:	Europe/Dublin
Credential name:	
<b>SIP Link Monitoring</b>	
SIP Link Monitoring:	Use Session Manager Configuration

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

- In the **Port** field enter the port number on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select the domain added in **Section 6.2** as the default domain

**Port**

TCP Failover port:

TLS Failover port:

Port	Protocol	Default Domain	Notes
5060	TCP	avaya.com	
5060	UDP	avaya.com	
5061	TLS	avaya.com	

Select : All, None

### 6.5.2. Avaya Aura® Communication Manager SIP Entity

The following screen shows the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the **Location** to that defined in **Section 6.3**, the Adaptation to that defined in **Section 6.4** and the **Time Zone** to the appropriate time zone.

Home / Elements / Routing / SIP Entities

**SIP Entity Details**

**General**

\* **Name:** CM\_VM1

\* **FQDN or IP Address:** 10.10.79.52

**Type:** CM

**Notes:**

**Adaptation:** Magnetic North

**Location:** Galway

**Time Zone:** Europe/Dublin

**Override Port & Transport with DNS SRV:** ☐

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

**Credential name:**

**Call Detail Recording:** none



Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

This screenshot shows two configuration sections for a SIP Entity. The first section, 'Loop Detection', contains a 'Loop Detection Mode' dropdown menu set to 'Off'. The second section, 'SIP Link Monitoring', contains a 'SIP Link Monitoring' dropdown menu set to 'Use Session Manager Configuration'.

### 6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows one of the SIP Entities for the Avaya SBCE. Two SIP Entities were used for the two interfaces established so that routing could take place to both of the Nextone SBCs. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

This screenshot shows the 'SIP Entity Details' configuration page in the Avaya SBCE. The page has a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. It includes 'Commit' and 'Cancel' buttons. The 'General' section contains the following fields: 'Name' (ASBCE\_Live\_A), 'FQDN or IP Address' (10.10.9.75), 'Type' (SIP Trunk), 'Notes' (empty), 'Adaptation' (empty), 'Location' (Galway), and 'Time Zone' (Europe/Dublin). There is an 'Override Port & Transport with DNS SRV' checkbox. The 'SIP Timer B/F (in seconds)' is set to 4. The 'Credential name' field is empty. The 'Call Detail Recording' dropdown is set to 'egress'. The 'Loop Detection' section at the bottom has 'Loop Detection Mode' set to 'Off'. The 'SIP Link Monitoring' section at the bottom has 'SIP Link Monitoring' set to 'Use Session Manager Configuration'.

Configure the other SIP Entity with the details of the alternative signalling interface established on the Avaya SBCE.



A summary of all the SIP Entities is shown in the following screenshot:

Home / Elements / Routing / SIP Entities				
SIP Entities				
<input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Duplicate"/> <input type="button" value="More Actions"/>				
9 Items Refresh Filter: Enable				
<input type="checkbox"/>	Name	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	ASBCE_Live_A	10.10.9.75	SIP Trunk	
<input type="checkbox"/>	ASBCE_Live_B	10.10.9.76	SIP Trunk	
<input type="checkbox"/>	CM_VM1	10.10.79.52	CM	
<input type="checkbox"/>	Messaging	10.10.2.82	Other	
<input type="checkbox"/>	Session Manager BGVM1	10.10.79.61	Session Manager	
Select : All, None				

## 6.6. Administer Entity Links

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

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **Session Manager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

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

Home / Elements / Routing / Entity Links									
Entity Links									
<input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Duplicate"/> <input type="button" value="More Actions"/>									
7 Items Refresh Filter: Enable									
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	ASBCE_Live_A_Link	Session Manager BGVM1	TCP	5060	ASBCE_Live_A	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	ASBCE_Live_B_Link	Session Manager BGVM1	TCP	5060	ASBCE_Live_B	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CM_VM1_Link	Session Manager BGVM1	TCP	5060	CM_VM1	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging_Link	Session Manager BGVM1	TCP	5060	Messaging	5060	trusted	<input type="checkbox"/>	
Select : All, None									

**Note:** The **Messaging\_Link** Entity Link is used for the Avaya Aura ® Messaging system and is not described in this document.

## 6.7. Administer Routing Policies

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

Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies
- Under **Time of Day**, click **Add**, and then select the time range

The following screen shows the routing policy for Communication Manager.

The screenshot displays the 'Routing Policy Details' page in a web application. The breadcrumb trail at the top is 'Home / Elements / Routing / Routing Policies'. The page is divided into three main sections: 'General', 'SIP Entity as Destination', and 'Time of Day'.

**General Section:** Contains fields for 'Name' (set to 'Internal\_CM\_VM1'), 'Disabled' (checkbox), 'Retries' (set to 0), and 'Notes' (empty text area). 'Commit' and 'Cancel' buttons are at the top right.

**SIP Entity as Destination Section:** Features a 'Select' button above a table listing available SIP entities.

Name	FQDN or IP Address	Type	Notes
CM_VM1	10.10.79.52	CM	

**Time of Day Section:** Includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below is a table for defining time ranges.

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

At the bottom, there is a 'Select : All, None' option.

The routing and fallback for the two SBCs is configured on the Session Manager, with two server flows configured on the Avaya SBCE for routing to each network SBC. There is an interface configured on the Avaya SBCE for each of these server flows, and a corresponding SIP Entity, Entity Link and Routing Policy is required on the Session Manager for each of these interfaces.

A full description of the configuration of the interfaces and server flows on the Avaya SBCE is provided in **Section 7**.

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed on to the PSTN via network SBC A.

Home / Elements / Routing / Routing Policies Help ?

**Routing Policy Details** Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
ASBCE_Live_A	10.10.9.75	SIP Trunk	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

Provide an additional Routing Policy for network SBC B. The following screenshot shows a summary of the routing policies provided.

Home / Elements / Routing / Routing Policies Help ?

**Routing Policies**

New Edit Delete Duplicate More Actions

7 Items Refresh Filter: Enable

Name	Disabled	Retries	Destination	Notes
<a href="#">Internal_CM_VM1</a>	<input type="checkbox"/>	0	CM_VM1	
<a href="#">Messaging</a>	<input type="checkbox"/>	0	Messaging	
<a href="#">PSTN_MN_Live_A</a>	<input type="checkbox"/>	0	ASBCE_Live_A	
<a href="#">PSTN_MN_Live_B</a>	<input type="checkbox"/>	0	ASBCE_Live_B	

Select : All, None

**Note:** The **Messaging\_Link** Routing Policy is used for the Avaya Aura ® Messaging system and is not described in this document.

## 6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched
- In the **Min** field enter the minimum length of the dialled number

- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown)
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the Magnetic North network via network SBC A with fallback via network SBC B.

Home / Elements / Routing / Dial Patterns Help ?

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		PSTN_MN_Live_A		<input type="checkbox"/>	ASBCE_Live_A	
<input type="checkbox"/>	-ALL-		PSTN_MN_Live_B		<input type="checkbox"/>	ASBCE_Live_B	

**Note:** The above dial plan will result in failover to the alternative SBC in the case of call failure. This includes failures such as “486 Busy Here” and “404 Not Found”

The following screen shows the test dial pattern configured for Communication Manager.

Home / Elements / Routing / Dial Patterns Help ?

**Dial Pattern Details** Commit Cancel

**General**

\* **Pattern:** 011385nnnn

\* **Min:** 10

\* **Max:** 11

**Emergency Call:** ☐

**Emergency Priority:** 1

**Emergency Type:**

**SIP Domain:** -ALL-

**Notes:**

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		Internal_CM_VM1		<input type="checkbox"/>	CM_VM1	

**Note:** The least significant four digits of the pattern to be matched have been obscured.

## 6.9. Administer Application for Avaya Aura® Communication Manager

From the **Home** tab select **Session Manager** from the menu. In the resulting tab from the left panel menu select **Application Configuration** → **Applications** and click **New** (not shown).

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager and select **Commit** to save the configuration.

Home / Elements / Session Manager / Application Configuration / Applications

**Application Editor** Commit Cancel

**Application**

\* **Name** CMV1\_App

\* **SIP Entity** CM\_VM1

\* **CM System for SIP Entity** CM\_VM1 Refresh [View/Add CM Systems](#)

**Description**

## 6.10. Administer Application Sequence for Avaya Aura® Communication Manager

From the left panel navigate to **Session Manager → Application Configuration → Application Sequences** and click on **New** (not shown).

- In the **Name** field enter a descriptive name
- Under **Available Applications**, click the + sign in front of the appropriate application instance. When the screen refreshes the application should be displayed under the **Applications in this Sequence** heading. Select **Commit**.

The screenshot shows the 'Application Sequence Editor' window. At the top, the breadcrumb navigation is 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The window title is 'Application Sequence Editor' with 'Commit' and 'Cancel' buttons. Below the title, there's a section for 'Application Sequence' with fields for '\*Name' (containing 'CMV1\_App\_Seq') and 'Description'. Below this is a section for 'Applications in this Sequence' with 'Move First', 'Move Last', and 'Remove' buttons. A table shows 1 item in the sequence:

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
1	CMV1_App	CM_VM1	<input checked="" type="checkbox"/>	

Below the table, it says 'Select : All, None'. At the bottom, there's a section for 'Available Applications' with a 'Refresh' button and a 'Filter: Enable' link. A table shows 2 items:

Name	SIP Entity	Description
+ CM-App	Communication Manager BG1	Dell R610 Rack 3
+ CMV1_App	CM_VM1	

## 6.11. Administer SIP Extensions

SIP extensions are registered with the Session Manager and use Communication Manager for their feature and configuration settings. From the **Home** tab select **User Management** from the menu. Then select **Manage Users** and click **New** (not shown).

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain e.g. **2460@avaya.com** which is used to create the user's primary handle
- The **Authentication Type** should be **Basic**
- In the **Password/Confirm Password** fields enter an alphanumeric password
- Set the **Language Preference** and **Time Zone** as required

The screenshot shows the 'Identity' tab of a configuration form for SIP extensions. The form has a tabbed interface with 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is active, showing a list of fields for user configuration. Fields marked with a red asterisk (\*) are required. The 'Login Name' field contains '2460@avaya.com'. The 'Authentication Type' is set to 'Basic'. The 'Password' and 'Confirm Password' fields are masked with dots. The 'Time Zone' is set to '(+1:0)GMT : Dublin, Edinburgh'. Other fields like 'Last Name', 'First Name', 'Middle Name', 'Description', 'Localized Display Name', 'Endpoint Display Name', 'Title', 'Employee ID', 'Department', and 'Company' are empty.

Field	Value
* Last Name	Windows
* First Name	Flare
Middle Name	
Description	
* Login Name	2460@avaya.com
* Authentication Type	Basic
Password	••••••••
Confirm Password	••••••••
Localized Display Name	
Endpoint Display Name	
Title	
Language Preference	English (United Kingdom)
Time Zone	(+1:0)GMT : Dublin, Edinburgh
Employee ID	
Department	
Company	



On the **Communication Profile** tab, enter a numeric **Communication Profile Password** and confirm it.

Identity \* **Communication Profile** \* Membership Contacts

Communication Profile ▾

Communication Profile Password: ●●●●●●

Confirm Password: ●●●●●●

New Delete Done Cancel

Name
Primary

Select : None

\* Name: Primary

Default : ☒

Communication Address ▾

New Edit Delete

Type	Handle	Domain
No Records found		

Expand the **Communication Address** section and click **New**. For the **Type** field select **Avaya SIP** from the drop-down menu. In the **Fully Qualified Address** field, enter an extension number and select the relevant domain from the drop-down menu. Click the **Add** button.

Communication Address ▾

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP ▾

\* Fully Qualified Address: 2460 @ avaya.com ▾

Add Cancel



Expand the **Session Manager Profile** section.

- Make sure the **Session Manager Profile** check box is checked
- Select the appropriate Session Manager instance from the drop-down menu in the **Primary Session Manager** field
- Select the appropriate application sequence from the drop-down menu in the **Origination Application Sequence** field configured in **Section 6.10**
- Select the appropriate application sequence from the drop-down menu in the **Termination Application Sequence** field configured in **Section 6.10**
- Select the appropriate location from the drop-down menu in the **Home Location** field

☒ **Session Manager Profile**

### SIP Registration

\* **Primary Session Manager**

Session Manager BGVM1

**Secondary Session Manager**

(None)

**Survivability Server**

(None)

**Max. Simultaneous Devices**

1

**Block New Registration When Maximum Registrations Active?**

☐

Primary	Secondary	Maximum
5	0	5

### Application Sequences

**Origination Sequence**

CMV1\_App\_Seq

**Termination Sequence**

CMV1\_App\_Seq

### Call Routing Settings

\* **Home Location**

Galway

**Conference Factory Set**

(None)

Expand the **Endpoint Profile** section.

- Select the Communication Manager SIP Entity from the **System** drop-down menu
- Select **Endpoint** from the drop-down menu for **Profile Type**
- Enter the extension in the **Extension** field
- Select the desired template from the **Template** drop-down menu
- In the **Port** field **IP** is automatically inserted
- Select the **Delete Endpoint on Unassign of Endpoint from User or on Delete User** check box
- Select **Commit** (Not Shown) to save changes and the System Manager will add the Communication Manager user configuration automatically

☒ **CM Endpoint Profile** ▼

\* **System**

CM\_VM1

▼

\* **Profile Type**

Endpoint

▼

Use Existing Endpoints

☐

\* **Extension**

2460

Endpoint Editor

\* **Template**

9630SIP\_DEFAULT\_CM\_6\_3

▼

**Set Type**

9630SIP

**Security Code**

**Port**

IP

**Voice Mail Number**

**Preferred Handle**

(None)

▼

Enhanced Callr-Info display for 1-line phones

☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User

☒

Override Endpoint Name

☒

## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

### 7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using username ucsec and the appropriate password.



The login screen features the Avaya logo on the left and a 'Log In' section on the right. The 'Log In' section includes fields for 'Username:' and 'Password:', a 'Log In' button, and a disclaimer paragraph.

**AVAYA**

**Log In**

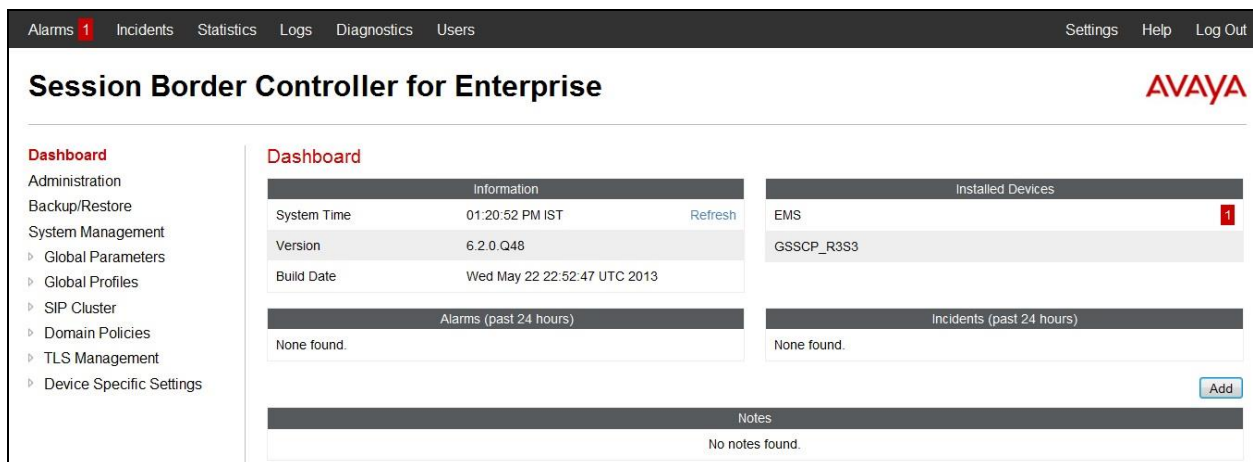
Username:

Password:

**Session Border Controller for Enterprise**

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



The dashboard has a top navigation bar with links: Alarms 1, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main content area is titled 'Session Border Controller for Enterprise' and features a left-hand menu and several data panels.

**Session Border Controller for Enterprise**

**Dashboard**

**Information**

System Time	01:20:52 PM IST	<a href="#">Refresh</a>
Version	6.2.0.Q48	
Build Date	Wed May 22 22:52:47 UTC 2013	

**Installed Devices**

EMS	1
GSSCP_R3S3	

**Alarms (past 24 hours)**

None found.

**Incidents (past 24 hours)**

None found.

**Notes**

No notes found.

[Add](#)

## 7.2. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one interface assigned though there can be more than one IP address defined on each interface.

In the test configuration, two IP addresses were used on the internal interface so that different server flows could be assigned depending on which interface address the SIP messages were received on. These server flows were used to direct traffic to the two network SBCs separately.

To define the network information, navigate to **Device Specific Settings → Network Management** (not shown) in the main menu on the left hand side and click on **Add**. Enter details in the blank box that appears at the end of the list

- Define the two internal IP addresses with screening mask and assign to interface **A1**
- Select **Save** to save the information
- Click on **Add**
- Define the external IP address with screening mask and assign to interface **B1**
- Select **Save** to save the information
- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar (not shown)

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Alarms 2', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the Avaya logo. A left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. Under 'Device Specific Settings', 'Network Management' is highlighted. The main content area is titled 'Network Management: GSSCP\_R3S3' and has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.128), and 'B2 Netmask'. An 'Add' button is present. Below the input fields is a table with columns: IP Address, Public IP, Gateway, and Interface. The table contains three rows of data. The first row has IP Address 10.10.9.75, Public IP, Gateway 10.10.9.1, and Interface A1. The second row has IP Address 192.168.122.59, Public IP, Gateway 192.168.122.51, and Interface B1. The third row has IP Address 10.10.9.76, Public IP, Gateway 10.10.9.1, and Interface A1. Each row has a 'Delete' button next to the Interface column.

IP Address	Public IP	Gateway	Interface	
10.10.9.75		10.10.9.1	A1	Delete
192.168.122.59		192.168.122.51	B1	Delete
10.10.9.76		10.10.9.1	A1	Delete

Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.

Network Management: GSSCP\_R3S3

Devices	Network Configuration	Interface Configuration
GSSCP_R3S3		
Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

## 7.3. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

### 7.3.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** (not shown) in the main menu on the left hand side.

To enter details of transport protocol and ports for the SIP signalling on the internal interface to be used in the server flow for network SBC A:

- Select **Add** and enter details of the first internal signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the interface
- For **Signaling IP**, select one of the **internal** signalling interface IP addresses defined in **Section 7.2**
- Select **TCP** port number, **5060** is used for the Session Manager

To enter details of the for the SIP signalling on internal interface to be used in the server flow for network SBC B:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for interface
- For **Signaling IP**, select the other **internal** signalling interface IP address defined in **Section 7.2**
- Select **TCP** port number, **5060** is used for the Session Manager

To enter details of the external SIP signalling:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the external signalling interface
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.2**
- Select **TCP** port number, **5060** is used for the SIP Trunk

Signaling Interface: GSSCP\_R3S3

Devices  
**GSSCP\_R3S3**

Signaling Interface

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Live_A	10.10.9.75	5060	---	---	None	Edit	Delete
Ext_Sig	192.168.122.59	---	5060	---	None	Edit	Delete
Int_Live_B	10.10.9.76	5060	---	---	None	Edit	Delete

### 7.3.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings → Media Interface** (not shown) in the main menu on the left hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

- Select **Add** and enter details of the internal media interface in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the internal media path with the enterprise end-points
- Select **Add** and enter details of the external media interface in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the external media path.

Media Interface: GSSCP\_R3S3

Devices  
**GSSCP\_R3S3**

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP	Port Range		
Int_Med	10.10.9.75	35000 - 40000	Edit	Delete
Ext_Med	192.168.122.59	35000 - 40000	Edit	Delete

BG; Reviewed:  
SPOC 02/18/2014

Solution & Interoperability Test Lab Application Notes  
©2014 Avaya Inc. All Rights Reserved.

38 of 54  
MN\_CM63\_SM



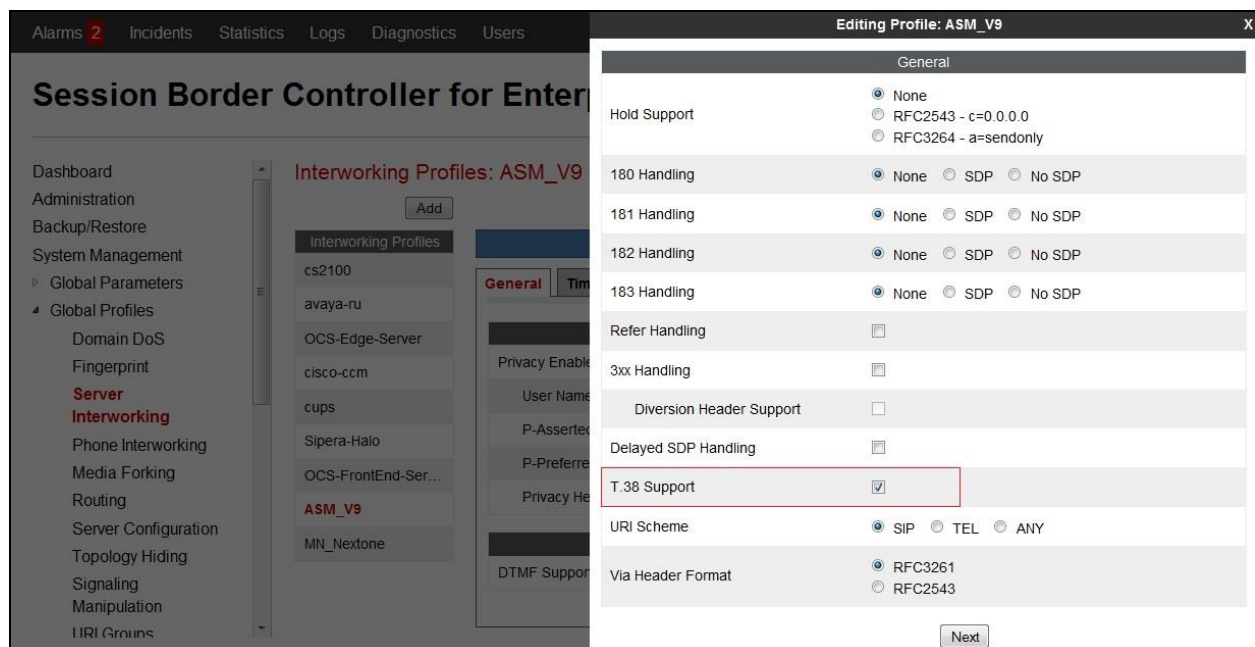
**Note:** During test the port ranges for the internal and external media interfaces were defined as the default values used by the Communication Manager,

## 7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Magnetic North's SIP Trunk is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the main menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM9** was used
- In the **General** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box then click **Next** and **Finish** (not shown)



- In the **Advanced** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Uncheck the **AVAYA Extensions** box

Editing Profile: ASM_V9	
Record Routes	<input checked="" type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversions Manipulation	<input type="checkbox"/>
Diversions Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>

To define Server Interworking for Magnetic North's SIP Trunk, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the **Clone Name** field enter a descriptive name for server interworking profile for Magnetic North and click **Finish** – in test **MN\_Nextone** was used
- Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box
- Select **Next** three times and **Finish**

## 7.5. Define Servers

Servers are defined for each server connected to the Avaya SBCE. In this case, the Magnetic North network is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** (not shown) in the main menu on the left hand side.



Click on **Add** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined on the Communication Manager in **Section 5.2**
- Check **TCP** in **Supported Transports**
- Define the **TCP** port for SIP signalling, **5060** is used for the Session Manager and click **Finish**

The screenshot shows the 'Edit Server Configuration Profile - General' window. On the left, a sidebar lists 'Server Profiles' with 'ASM\_V9' selected. The main area has tabs for 'General' and 'Advanced'. The 'General' tab is active, showing fields for 'Server Type' (Call Server), 'IP Addresses / Supported FQDNs' (10.10.79.61), 'Supported Transports' (TCP checked), and ports (TCP: 5060, UDP: , TLS: ). A 'Finish' button is at the bottom.

- Select the **Advanced** tab (not shown)
- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for the Session Manager defined in **Section 7.4**
- Click **Finish**

The screenshot shows the 'Edit Server Configuration Profile - Advanced' window. It contains checkboxes for 'Enable DoS Protection' and 'Enable Grooming', both unchecked. The 'Interworking Profile' dropdown is set to 'ASM\_V9'. The 'Signaling Manipulation Script' dropdown is set to 'None'. The 'TCP Connection Type' section has three radio buttons: 'SUBID' (selected), 'PORTID', and 'MAPPING'. A 'Finish' button is at the bottom.

To define the first network SBC (Nextone A) as a Trunk Server, navigate to **Global Profiles** → **Server Configuration** in the main menu on the left hand side. Click on **Add** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the network SBC, in test **Nextone\_Live\_A** was used, and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the first network SBC
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for the Magnetic North network

**Edit Server Configuration Profile - General**

Server Type: Trunk Server

IP Addresses / Supported FQDNs: 192.168.141.10

Supported Transports: ☐ TCP, ☒ UDP, ☐ TLS

TCP Port:

UDP Port: 5060

TLS Port:

Finish

- Click **Next** again then select the **Interworking Profile** for the Magnetic North network defined in **Section 7.4** from the drop down menu

**Edit Server Configuration Profile - Advanced**

Enable DoS Protection: ☐

Enable Grooming: ☐

Interworking Profile: MN\_Nextone

Signaling Manipulation Script: None

UDP Connection Type: ☒ SUBID, ☐ PORTID, ☐ MAPPING

Finish

To define the second network SBC (Nextone B) as a Trunk Server, navigate to **Global Profiles** → **Server Configuration** in the main menu on the left hand side. Click on **Add** and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the network SBC, in test **Nextone\_Live\_B** was used, and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the second network SBC
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for the Magnetic North network

The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. It has a title bar with 'Edit Server Configuration Profile - General' and a close button 'X'. The dialog contains several fields: 'Server Type' is a dropdown menu set to 'Trunk Server'; 'IP Addresses / Supported FQDNs' is a text box containing '192.168.141.18' with a small note 'Separate entries with commas'; 'Supported Transports' has three checkboxes: 'TCP' (unchecked), 'UDP' (checked), and 'TLS' (unchecked); 'TCP Port' is an empty text box; 'UDP Port' is a text box containing '5060'; 'TLS Port' is an empty text box; and a 'Finish' button at the bottom.

- Click **Next** again then select the **Interworking Profile** for the Magnetic North network defined in **Section 7.4** from the drop down menu

The screenshot shows the 'Edit Server Configuration Profile - Advanced' dialog box. It has a title bar with 'Edit Server Configuration Profile - Advanced' and a close button 'X'. The dialog contains several fields: 'Enable DoS Protection' is a checkbox (unchecked); 'Enable Grooming' is a checkbox (unchecked); 'Interworking Profile' is a dropdown menu set to 'MN\_Nextone'; 'Signaling Manipulation Script' is a dropdown menu set to 'None'; 'UDP Connection Type' has three radio buttons: 'SUBID' (selected), 'PORTID' (unchecked), and 'MAPPING' (unchecked); and a 'Finish' button at the bottom.

## 7.6. Define Routing

Routing information is required for routing to the Session Manager on the internal side and both network SBCs on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Session Manager, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the Session Manager, in this case **ASM\_V9**, and click **Next** (not shown)
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**

**Controller for Enterprise** **Edit Routing Rule**

Each URI group may only be used once per Routing Profile.

**Next Hop Routing**

URI Group: \*

Next Hop Server 1 (IP, IP:Port, Domain, or Domain:Port): 10.10.79.61

Next Hop Server 2 (IP, IP:Port, Domain, or Domain:Port):

Routing Priority based on Next Hop Server: ☒

Use Next Hop for In Dialog Messages: ☐

Ignore Route Header for Messages Outside Dialog: ☐

NAPTR: ☐

SRV: ☐

Outgoing Transport: ☐ TLS ☒ TCP ☐ UDP

**Finish**

To define routing to the first network SBC (Nextone A), navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the network SBC, in this case **MN\_LiveA\_Trunk** was used, and click **Next** (not shown)
- Enter the network SBC IP address and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**

To define routing to the second network SBC (Nextone B), navigate to **Global Profiles** → **Routing** in the main menu on the left hand side. Click on **Add** and enter details in the **Routing Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the network SBC, in this case **MN\_LiveB\_Trunk** was used, and click **Next**
- Enter the network SBC IP address and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**

The following screenshot shows a summary of the routing to the second network SBC

## 7.7. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP address. The default **Replace Action** is **Auto**; this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from the Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for the Session Manager, navigate to **Global Profiles → Topology Hiding** (not shown) in the main menu on the left hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- If the **Request-Line**, **Record-Route**, **SDP** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **To** and **From** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms (2), Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling, and Manipulation. The main content area is titled "Topology Hiding Profiles: ASM\_V9" and includes an "Add" button, a list of profiles (default, cisco\_th\_profile, ASM\_V9, MN\_SIP\_Trunk), and buttons for Rename, Clone, and Delete. Below the profile list is a table for "Topology Hiding" configuration. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The rows are: To (IP, Auto, ---), SDP (IP/Domain, Auto, ---), From (IP, Auto, ---), Via (IP/Domain, Auto, ---), Request-Line (IP/Domain, Auto, ---), and Record-Route (IP/Domain, Auto, ---). An "Edit" button is located at the bottom right of the table.

Header	Criteria	Replace Action	Overwrite Value
To	IP	Auto	---
SDP	IP/Domain	Auto	---
From	IP	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

**Note:** The use of **Auto** results in an IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names can be used for the enterprise and the SIP Trunk.



To define Topology Hiding for the Magnetic North network, navigate to **Global Profiles** → **Topology Hiding** in the main menu on the left hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Magnetic North's SIP Trunk and click **Next**
- If the **Request-Line**, **Record-Route**, **SDP** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **From** and **To** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**

Topology Hiding Profiles: MN\_SIP\_Trunk

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco\_th\_profile

ASM\_V9

**MN\_SIP\_Trunk**

Click here to add a description.

**Topology Hiding**

Header	Criteria	Replace Action	Overwrite Value
To	IP	Auto	---
SDP	IP/Domain	Auto	---
From	IP	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

Edit

## 7.8. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from the Session Manager to Magnetic North's SIP Trunk and incoming flows from Magnetic North's SIP Trunk to the Session Manager. This configuration ties all the previously entered information together so that signalling can be routed from the Session Manager to the PSTN via the Magnetic North network and vice versa.

Two server flows are required for outgoing traffic and two are required for incoming. This is so that traffic can be routed to both the network SBCs and can also be received from both network SBCs. As mentioned previously, the network SBCs have been designated as Nextone A and Nextone B for the purposes of the testing and documentation.

The screenshot at the end of the section shows a summary of the server flows created.

To define a Server Flow for the Session Manager to each of the network SBCs, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for the Session Manager, in this case **SM\_Live\_A** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.5** for the Session manager.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager is received on.
- In the **Signaling Interface** drop-down menu, select the first internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager from Nextone A is sent on.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**. This is the interface that media bound for the enterprise from Nextone A is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Nextone A defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.7** and click **Finish**.

Edit Flow: SM_Live_A	
Flow Name	SM_Live_A
Server Configuration	ASM_V9
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Live_A
Media Interface	Int_Med
End Point Policy Group	default-low
Routing Profile	MN_LiveA_Trunk
Topology Hiding Profile	ASM_V9
File Transfer Profile	None
<div>Finish</div>	

Repeat the above process for Nextone B selecting the specific Nextone B entries for **Signalling Interface** and **Routing Profile**.



To define Server Flows for the network SBCs (Nextone A and B), navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Nextone A, in this case **Trunk\_Live\_A** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.5** for Nextone A
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling from the Session Manager bound for Nextone A is received on.
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Nextone A from the Session manager is sent on.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**. This is the interface that media bound for the PSTN is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Magnetic North network defined in **Section 7.7** and click **Finish**.

Edit Flow: Trunk_Live_A	
Flow Name	Trunk_Live_A
Server Configuration	Nextone_Live_A
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Live_A
Signaling Interface	Ext_Sig
Media Interface	Ext_Med
End Point Policy Group	default-low
Routing Profile	ASM_V9
Topology Hiding Profile	MN_SIP_Trunk
File Transfer Profile	None
<div>Finish</div>	

Repeat the above process for Nextone B selecting the specific Nextone B entries for **Server Configuration** and **Received interface**.

Once the server flows have been configured, they appear on the main page as follows:

The screenshot shows the Avaya Session Border Controller for Enterprise main page. The top navigation bar includes Alarms (2), Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration options, with "End Point Flows" highlighted in red. The main content area is titled "End Point Flows: GSSCP\_R3S3". It features a "Devices" tab with "GSSCP\_R3S3" selected. Below this, there are two tabs: "Subscriber Flows" and "Server Flows". The "Server Flows" tab is active, showing a table of server configurations. The table has columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. There are two rows of server configurations: "SM\_Live\_A" and "SM\_Live\_B". Each row has a "View" button and a "Delete" button. Below the table, there are two sections for "Server Configuration: Nextone\_Live\_A" and "Server Configuration: Nextone\_Live\_B", each containing a table of server configurations with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. Each row in these tables has a "View" button and a "Delete" button.

For information, the server flows are shown in their entirety here:

The screenshot shows the "Server Flows" configuration page. At the top, there are two tabs: "Subscriber Flows" and "Server Flows", with "Server Flows" selected. Below the tabs, there is a blue bar with the text "Click here to add a row description." and an "Add" button. The main content area is titled "Server Configuration: ASM\_V9" and contains an "Update" button. Below this, there are three sections for "Server Configuration: Nextone\_Live\_A" and "Server Configuration: Nextone\_Live\_B", each containing a table of server configurations. The tables have columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. Each row in these tables has a "View" button and a "Delete" button.

## 8. Configure Magnetic North SIP Trunk Equipment

The configuration of the Magnetic North equipment used to support Magnetic North's SIP Trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Magnetic North equipment and system configuration please contact an authorised Magnetic North representative.

## 9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring** (not shown). Select the relevant SIP Entities from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

[Home](#) / [Elements](#) / [Session Manager](#) / [System Status](#) / [SIP Entity Monitoring](#)[Help ?](#)

### Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: [Session Manager BGVM1](#)

[Summary View](#)

Status Details for the selected Session Manager:

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

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">Messaging</a>	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">ASBCE Live B</a>	10.10.9.76	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">ASBCE Live A</a>	10.10.9.75	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">CM_VM1</a>	10.10.79.52	5060	TCP	FALSE	UP	200 OK	UP

2. From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in-service/idle**.

```
status trunk 1
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0001/001	T00001	in-service/idle	no
0001/002	T00002	in-service/idle	no
0001/003	T00003	in-service/idle	no
0001/004	T00004	in-service/idle	no
0001/005	T00005	in-service/idle	no
0001/006	T00006	in-service/idle	no
0001/007	T00007	in-service/idle	no
0001/008	T00008	in-service/idle	no
0001/009	T00009	in-service/idle	no
0001/010	T00010	in-service/idle	no

3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, use the Avaya SBCE trace facility to check that the OPTIONS requests sent from the Session Manager via the Avaya SBCE to the network SBCs are receiving a response.

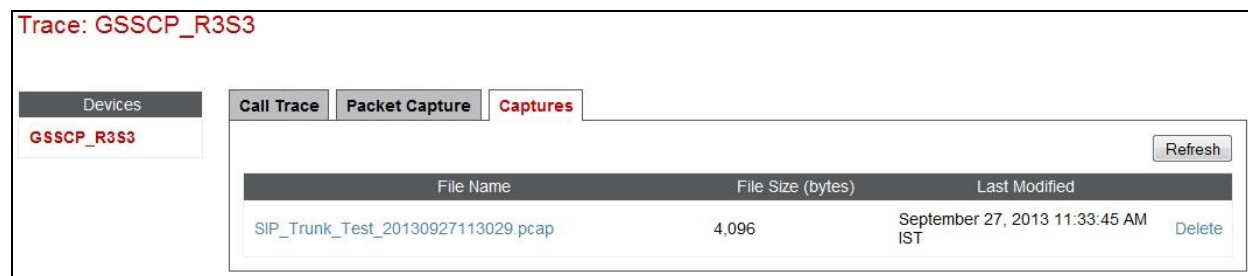
To define the trace on the Avaya SBCE, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the network SBC in the **Remote Address** field or enter a \* to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the **Capture Filename** field
- Click on **Start Capture**

Trace: GSSCP\_R3S3

Devices	Call Trace	Packet Capture	Captures
GSSCP_R3S3	<div> <div>Packet Capture Configuration</div> <div> <div>Status</div> <div>Ready</div> </div> <div> <div>Interface</div> <div>B1</div> </div> <div> <div>Local Address IP[:Port]</div> <div>192.168.122.59 : </div> </div> <div> <div>Remote Address *, *:Port, IP, IP:Port</div> <div>*</div> </div> <div> <div>Protocol</div> <div>UDP</div> </div> <div> <div>Maximum Number of Packets to Capture</div> <div>1000</div> </div> <div> <div>Capture Filename Using the name of an existing capture will overwrite it.</div> <div>SIP_Trunk_Test.pcap</div> </div> <div> <div>Start Capture</div> <div>Clear</div> </div> </div>		

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.



The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Magnetic North network.

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.3 as an Evolution Server, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2 to Magnetic North's SIP Trunk Service. Magnetic North's SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

## 11. Additional References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2013.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.
- [3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, May 2013
- [4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2013.
- [5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2013
- [7] *Upgrading Avaya Aura® System Manager to 6.3.2*, May 2013.
- [8] *Administering Avaya Aura® System Manager* Release 6.3, May 2013
- [9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2013
- [11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2013
- [12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2013,
- [13] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2 June 2013
- [14] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2 July 2013
- [15] *Administering Avaya Session Border Controller for Enterprise* Release 6.2 March 2013
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

---

**©2014 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).