



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 Netia SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the Netia 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. Netia 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 the Netia SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise R6.2 (Avaya SBCE), Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager Evolution Server R6.3. Customers using this Avaya SIP-enabled enterprise solution with Netia 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 Netia.

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 Netia, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via Netia SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones.
- Calls using the G.729, G.711A 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.
- 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.
- Secure transport of media within the enterprise using SRTP and transport of signalling using TLS.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Netia SIP Trunk requiring Avaya response and sent by Avaya requiring Netia response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Netia SIP Trunk Service with the following observations:

- Calls were coming in originally with a Max Forwards value of 9. While this was fine for H.323 phones, it didn't work for SIP phones. Netia increased the value to 20 which solved the problem.
- When there was no matching codec on an incoming call, the CM sent a "488 Not Acceptable Here". The network re-attempted the call a number of times and there was a delay of a few seconds before a tone was heard by the caller.
- When there was no matching codec on an outgoing call, the network sent a "487 Request Terminated" after 32 seconds. During that time no tone was heard by the caller.
- 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.
- No Privacy header was received on incoming calls where the calling party number was restricted. The enterprise equipment displayed the user portion of the From header which was "anonymous" and an acceptable indicator under these conditions.
- Outbound T.38 fax calls were unreliable with only 6 pages of a 10 page document sent. This is a common problem in the test network that uses multiple SIP to TDM hops and is not considered to be a serious issue.
- EC 500 Confirmed Answer did not function correctly as the call was not answered on the mobile even when keys were pressed. This function is not considered to be critical
- One-X Communicator ceased to function correctly when connected via SIP and the "Other Phone Mode" tests were not completed. Fault report ONEXC-8777 has been raised to deal with this issue. All calls were successful when One-X Communicator was connected using H.323.
- Media was lost on calls that exceeded 30 minutes in duration. An Avaya SBCE fault was identified and JIRA ticket AURORA-1733 raised, a GA build that includes a fix for this issue is expected by the end of December 2013.

2.3. Support

For technical support on Netia products please contact with Netia helpline 48801802803 or by email to biznes@netia.pl.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to Netia 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 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 Flare for Windows running on a laptop PC. Within the enterprise, TLS was used for secure signalling transport and SRTP for media.

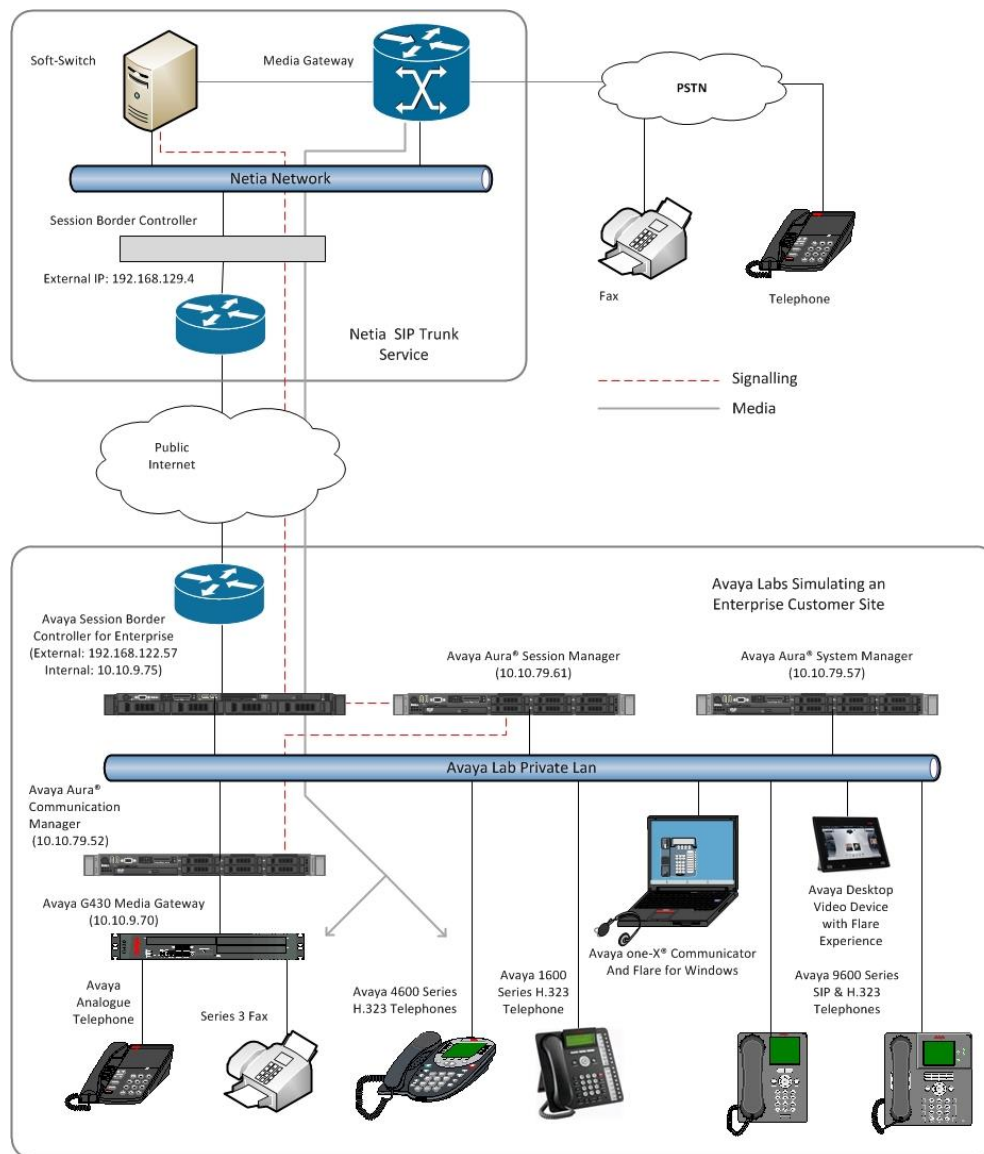


Figure 1: Test Setup Netia SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Dell PowerEdge R620 running Session Manager on VM Version 8	SM-6.3.2.0.632023-e50-00
Dell PowerEdge R620 running System Manager on VM Version 8	SMGR-6.3.0.8.5682-e50-64 (Build 5682)
Dell PowerEdge R620 running Communication Manager on VM Version 8	R016x.03.0.124.0
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 96x0 Phone (H.323)	3.200
Avaya A175 Desktop Video Device (SIP)	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
Analogue Handset	NA
Analogue Fax	NA
Netia	
Acme Packet Net-Net 4500 SBC	SCX6.2.0 MR-10 GA (Build 1030)
Broadworks Platform	Release 14.0, Service Pack 9
TSS TelephonySoftSwitch	4.0 version 9.0, patch 7.1

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 Netia 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 Netia 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 Netia SIP Trunk network, and any other SIP trunks used.

display system-parameters customer-options		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
Maximum Administered SIP Trunks:		24000	10
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** by typing **change ip-codec-set 1**. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by Netia were configured, namely **G.729A**, **G.711A** and **G.711MU**. If SRTP is to be used for media within the enterprise, select the encryption. For the interoperability test, **1-srtp-aescm128-hmac80** was selected.

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.729A	n	2	20
2: G.711A	n	2	20
3: G.711MU	n	2	20
4:			
5:			
6:			
7:			
Media Encryption			
1:	1-srtp-aescm128-hmac80		
2:			
3:			

Netia 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			
	Mode	Redundancy	
FAX	t.38-standard	0	ECM: y
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	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 Netia SIP Trunk network. During test, this was configured to use TLS and port 5061 to represent the security requirements for signalling that may be in place at the customer's site. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tls**.
- Set **Enforce SIPS URI for SRTP?** to **n** as SRTP and TLS are only used within the enterprise and are not to be used end to end.
- 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 **5061** (Commonly used TLS 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: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
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: 5061	Far-end Listen Port: 5061	
	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? y	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 Netia 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 national number with no leading zeros. This format was successfully verified in the network.

add trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UII 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 calls will be sent in the **Diversion Header**.
- Set **Send Diversion Header** to **y** as this header is used in the Avaya SBCE to insert the DDI number of the extension into the From field for verification in the network.
- Set the **Telephone Event Payload Type** to **98** to match the value preferred by Netia (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	
Send Transferring Party Information? n	
Network Call Redirection? n	
	Send Diversion Header? y
	Support Request History? n
	Telephone Event Payload Type: 98
	Convert 180 to 183 for Early Media? n
	Always Use re-INVITE for Display Updates? n
	Identity for Calling Party Display: From
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 national number with no leading zeros as the format expected in the network for calling party number verification. This calling party number is sent in the SIP From, Contact and PAI headers as well as the Diversion header for forwarded calls. The number is displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext	Ext	Trk	Private	Total	
Len	Code	Grp(s)	Prefix	Len	
4	2000	1	2235nnnn1	9	Total Administered: 8
4	2208	1	2235nnnn4	9	Maximum Entries: 540
4	2316	1	2235nnnn6	9	
4	2346	1	2235nnnn3	9	
4	2396	1	2235nnnn2	9	
4	2402	1	2235nnnn7	9	
4	2460	1	2235nnnn8	9	
4	2611	1	2235nnnn5	9	

Note: The private numbers in the above screenshot have been modified for security.

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 Netia 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**.

change feature-access-codes		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		
Auto Route Selection (ARS) - Access Code 1: 9		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	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	
118	3	6	1	pubu		n	
8	8	9	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		
														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				unk-unk	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:	y	y	y	y	y	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 Netia 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 to ensure that the message waiting indicator is successfully sent to SIP extensions when a voice mail message is available and unread.

5.10. EC500 Configuration

When EC500 is enabled on a 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. **0035389434nnnn**).
- 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 Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2396	EC500	-		0035389434nnnn	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 the Communication Manager configuration by entering **save translation**.

6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The Session Manager is configured by opening a web browser to 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 and 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 November 14, 2013 9:03 AM
Help | About | Change Password | Log off admin

Users	Elements	Services
Administrators Manage Administrative Users	Communication Manager Manage Communication Manager 5.2 and higher elements	Backup and Restore Backup and restore System Manager database
Directory Synchronization Synchronize users with the enterprise directory	Communication Server 1000 Manage Communication Server 1000 elements	Bulk Import and Export Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others
Groups & Roles Manage groups, roles and assign roles to users	Conferencing Manage Conferencing Multimedia Server objects	Configurations Manage system wide configurations
User Management Manage users, shared user resources and provision users	IP Office Manage IP Office elements	Events Manage alarms, view and harvest logs
	Meeting Exchange Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements	Geographic Redundancy Manage Geographic Redundancy
	Messaging Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging	Inventory Manage, discover, and navigate to elements
	Presence Presence	Licenses View and configure licenses
	Routing Session Manager Routing Administration	Replication Track data replication nodes, repair replication nodes
		Scheduler 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 of the enterprise site or a name agreed with Netia; this will be the same as specified in the Authoritative Domain specified in the IP Network Region on 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.

Home / Elements / Routing / Domains

Domain Management

New Edit Delete Duplicate More Actions

1 Item Refresh

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

Select : All, None

Note: If the existing domain name used in the enterprise equipment does not match that used in the network, a Session Manager adaptation can be used to change it (see **Section 6.4**).

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 test enterprise.

Home / Elements / Routing / Locations

Help ?

Commit Cancel

Location Details

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): 2000 Kbit/Sec

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

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

2 Items Refresh Filter: Enable

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

6.4. Administer Adaptations

Calls from Netia are received at the enterprise in national format with no leading “0” on the Request URI. An Adaptation specific to Netia is used to convert the called number to an extension number as defined in the Communication Manager before onward routing to Communication Manager SIP Entity and removes the requirement for incoming digit manipulation on Communication Manager. The adaptation is also used to modify the domain name between that used in the enterprise equipment and that used in the network.

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** with a value of **true**. This will apply the adaptation to the From and To headers as well as the Request URI. Enter **iodstd** with a value of the domain name of the enterprise, in this case **avaya.com**. This applies to incoming calls only and will change the domain name in the URI of Request-Line header. Enter **osrcd** with a value of the domain name of the network, in this case **netiasa.integralnet.pl**. This applies to outgoing calls only and will change the domain name in the URI of the origination headers, in particular the From and P-Asserted-Identity headers.

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel

General

* **Adaptation name:**

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Note: The full entry in the Module parameter field above is **fromto=true osrcd=netiasa.integralnet.pl iodstd=avaya.com**

Scroll down and in the section **Digit Conversion for Incoming Calls to SM**, click on **Add**. An additional row will appear (not shown). This allows information to be entered for the manipulation of numbers coming from the network. This is where the called party number is translated from national format to the extension number for termination of calls on Communication Manager.

The screenshot below shows a translation for each called 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 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-Line headers only.

Digit Conversion for Incoming Calls to SM

Add Remove

8 Items Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*2235nnnn1	*9	*9		*9	2000	destination		
<input type="checkbox"/>	*2235nnnn2	*9	*9		*9	2396	destination		
<input type="checkbox"/>	*2235nnnn3	*9	*9		*9	2346	destination		
<input type="checkbox"/>	*2235nnnn4	*9	*9		*9	2208	destination		
<input type="checkbox"/>	*2235nnnn5	*9	*9		*9	2611	destination		
<input type="checkbox"/>	*2235nnnn6	*9	*9		*9	2316	destination		
<input type="checkbox"/>	*2235nnnn7	*9	*9		*9	2402	destination		
<input type="checkbox"/>	*2235nnnn8	*9	*9		*9	2501	destination		

Select : All, None

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

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. 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 three SIP Entities:

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

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.

Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

* **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:

SIP Link Monitoring

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**.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name:

* FQDN or IP Address:

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds):

Credential name:

Call Detail Recording:

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

The screenshot shows two configuration sections. The first section, 'Loop Detection', has a 'Loop Detection Mode' dropdown menu set to 'Off'. The second section, 'SIP Link Monitoring', has 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 the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set the **Adaptation** to that defined in **Section 6.4**, the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

The screenshot shows the 'SIP Entity Details' configuration page for 'ASBCE_50'. The 'General' tab is selected. The 'Name' field is 'ASBCE_50' and the 'FQDN or IP Address' field is '10.10.9.75'. The 'Type' dropdown is set to 'SIP Trunk'. The 'Notes' field is empty. The 'Adaptation' dropdown is set to 'Netia_PSTN', the 'Location' dropdown is set to 'Galway', and the 'Time Zone' dropdown is set to 'Europe/Dublin'. The 'Override Port & Transport with DNS SRV' checkbox is unchecked. The 'SIP Timer B/F (in seconds)' field is set to '4'. The 'Credential name' field is empty. The 'Call Detail Recording' dropdown is set to 'egress'. The 'Commit' and 'Cancel' buttons are in the top right corner.

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								
New Edit Delete Duplicate More Actions								
4 Items Refresh Filter: Enable								
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	ASBCE_45_Link	Session Manager BGVM1	TLS	5061	ASBCE_45	5061	trusted	<input checked="" type="checkbox"/>
<input type="checkbox"/>	ASBCE_50_Link	Session Manager BGVM1	TLS	5061	ASBCE_50	5061	trusted	<input type="checkbox"/>
<input type="checkbox"/>	CM_VM1_Link	Session Manager BGVM1	TLS	5061	CM_VM1	5061	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.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CM_VM1	10.10.79.52	CM	

Time of Day

1 Item Refresh Filter: Enable

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

Select : All, None

The following screen shows the Routing Policy for the Avaya SBCE interface that will be routed to the PSTN via the Netia SIP Trunk.

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ASBCE_50	10.10.9.75	SIP Trunk	

Time of Day

1 Item Refresh Filter: Enable

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

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 PSTN via the Netia SIP Trunk.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 0

* Min: 8

* Max: 17

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-		PSTN_Netia		<input type="checkbox"/>	ASBCE_50	

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:**

* **Min:**

* **Max:**

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item 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"/>	Galway		Internal_VM79_CM	0	<input type="checkbox"/>	VM79_CM	

Select : All, None

Note: The above configuration is used where analysis of the incoming DDI number is required. If the Adaptation described in **Section 6.4** is used, this isn't necessary as the number is converted to an extension number. In this case, a dial pattern is required to route extension numbers. In test, the dial pattern is defined with a **Pattern** of **2** and a **Min** and **Max** value of **4**.

In the above screenshot, 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.

The screenshot shows the 'Application Editor' window. The breadcrumb trail at the top is 'Home / Elements / Session Manager / Application Configuration / Applications'. The form contains the following fields:

- Name:** CMV1_App
- SIP Entity:** CM_VM1 (selected from a dropdown)
- CM System for SIP Entity:** CM_VM1 (selected from a dropdown), with a 'Refresh' button and a link 'View/Add CM Systems'.
- Description:** (empty text field)

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

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. The breadcrumb trail at the top is 'Home / Elements / Session Manager / Application Configuration / Application Sequences'. The form contains the following sections:

- Application Sequence:**
 - Name:** CMV1_App_Seq
 - Description:** (empty text field)
- Applications in this Sequence:**
 - Buttons: Move First, Move Last, Remove
 - Table with 1 item:
- Available Applications:**
 - Buttons: Refresh, Filter: Enable
 - Table with 2 items:

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

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 header with four tabs: 'Identity' (selected), 'Communication Profile', 'Membership', and 'Contacts'. Below the header, the 'Identity' section is expanded. The form contains the following fields and controls:

- * Last Name:** Text input field with 'Windows' entered.
- * First Name:** Text input field with 'Flare' entered.
- Middle Name:** Text input field (empty).
- Description:** Text area with up and down arrow controls (empty).
- * Login Name:** Text input field with '2460@avaya.com' entered.
- * Authentication Type:** Dropdown menu with 'Basic' selected.
- Password:** Text input field with masked characters (dots).
- Confirm Password:** Text input field with masked characters (dots).
- Localized Display Name:** Text input field (empty).
- Endpoint Display Name:** Text input field (empty).
- Title:** Text input field (empty).
- Language Preference:** Dropdown menu with 'English (United Kingdom)' selected.
- Time Zone:** Dropdown menu with '(+1:0)GMT : Dublin, Edinburgh' selected.
- Employee ID:** Text input field (empty).
- Department:** Text input field (empty).
- Company:** Text input field (empty).

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 Sequence** field configured in **Section 6.10**.
- Select the appropriate application sequence from the drop-down menu in the **Termination 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.

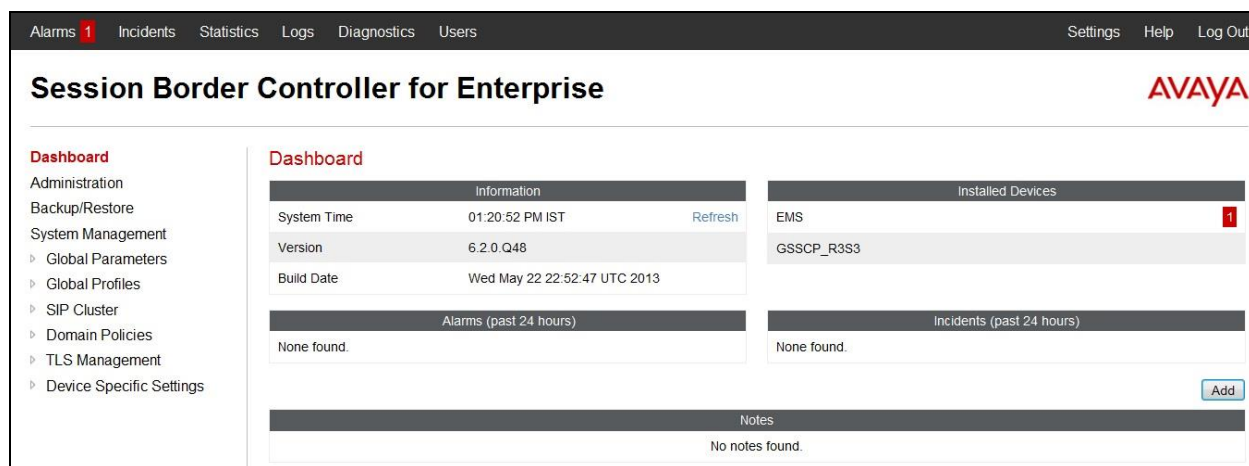
7.1. Access Avaya Session Border Controller for Enterprise

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. To the right, under the heading "Log In", are fields for "Username:" and "Password:". Below these fields is a "Log In" button. At the bottom right, there is a disclaimer: "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 header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand menu lists: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, Device Specific Settings), and a red "1" next to Alarms. The main content area is titled "Dashboard" and contains several sections: "Information" (System Time: 01:20:52 PM IST, Version: 6.2.0.Q48, Build Date: Wed May 22 22:52:47 UTC 2013), "Installed Devices" (EMS, GSSCP_R3S3), "Alarms (past 24 hours)" (None found), "Incidents (past 24 hours)" (None found), and "Notes" (No notes found). There is a "Refresh" button next to the System Time and an "Add" button at the bottom right.

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.

To define the network information, navigate to **Device Specific Settings → Network Management** 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 internal IP address 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).

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings
‣ **Network Management**
Media Interface
Signaling Interface

Network Management: GSSCP_R3S3

Devices
GSSCP_R3S3

Network Configuration Interface Configuration

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.

A1 Netmask: 255.255.255.0 A2 Netmask: B1 Netmask: 255.255.255.128 B2 Netmask:

Add Save Clear

IP Address	Public IP	Gateway	Interface	
10.10.9.75		10.10.9.1	A1	Delete
192.168.122.57		192.168.122.51	B1	Delete

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

Network Management: GSSCP_R3S3

Devices
GSSCP_R3S3

Network Configuration Interface Configuration

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. Testing was carried out with TLS used for transport of signalling between the Session Manager and the Avaya SBCE. This document shows the configuration for TLS, if another transport protocol is required, substitute it where TLS is specified.

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. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

- 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 the internal signalling interface.
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.2**.
- Select **TLS** port number, **5061** is used for the Session Manager.
- When the TLS port number is defined, an additional field (not shown) becomes available for **TLS Profile**, select the predefined Avaya profile **AvayaSBCServer**.
- 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 **UDP** port number, **5060** is used for the Netia SIP Trunk.

Signaling Interface: GSSCP_R3S3

Devices
GSSCP_R3S3

Signaling Interface

Add

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.9.75	---	---	5061	AvayaSBCServer	Edit Delete
Ext_Sig	192.168.122.57	---	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** 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 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 media path with Netia SIP Trunk.

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	Edit	Delete
Int_Med	10.10.9.75	35000 - 40000	Edit	Delete
Ext_Med	192.168.122.57	35000 - 40000	Edit	Delete

Note: During test the port ranges for the internal and external media interfaces were left at default values.

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, Netia 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 **ASM** 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).

The screenshot displays the Avaya SBCE configuration interface. On the left, the main menu shows 'Global Profiles' selected, with 'Server Interworking' highlighted in red. The 'Interworking Profiles: ASM' list shows 'avaya-ru' selected. The 'Editing Profile: ASM' dialog box is open, showing the 'General' tab. The 'General' tab contains various configuration options for the 'ASM' profile. The options include: 'Hold Support' (radio buttons for None, RFC2543 - c=0.0.0.0, RFC3264 - a=sendonly), '180 Handling' (radio buttons for None, SDP, No SDP), '181 Handling' (radio buttons for None, SDP, No SDP), '182 Handling' (radio buttons for None, SDP, No SDP), '183 Handling' (radio buttons for None, SDP, No SDP), 'Refer Handling' (checkbox), '3xx Handling' (checkbox), 'Diversion Header Support' (checkbox), 'Delayed SDP Handling' (checkbox), 'T.38 Support' (checkbox, checked), 'URI Scheme' (radio buttons for SIP, TEL, ANY), and 'Via Header Format' (radio buttons for RFC3261, RFC2543). A 'Next' button is at the bottom right of the dialog box.

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

The screenshot shows a window titled "Editing Profile: ASM" with a close button (X) in the top right corner. The window contains a list of configuration options, each with a checkbox or radio button. The "AVAYA Extensions" option is highlighted with a red rectangle. The options are as follows:

Option	Value
Record Routes	<input 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"/> (highlighted)
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion 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 Netia 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 Netia SIP Trunk and click **Finish** – in test **Netia** was used
- Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box
- Select **Next** three times and **Finish**

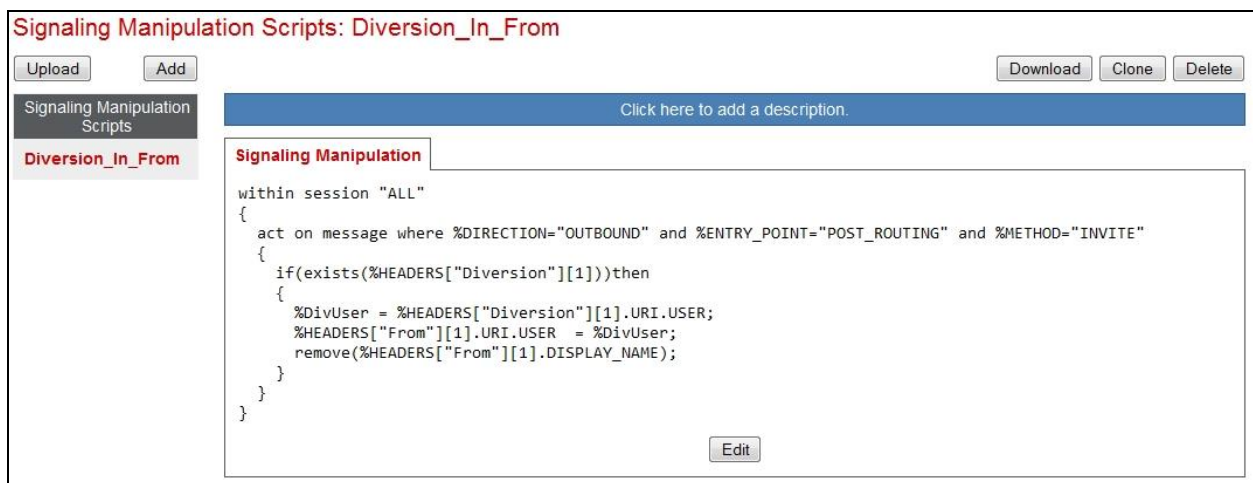
7.5. Define Signalling Manipulation

Signalling manipulation is required in some cases to ensure effective interworking. In the case of Netia, an issue existed where forwarded calls were not completing as the number in the From header was the original calling party number as opposed to the diverting number. As outgoing calls are verified in the network based on the number in the From field, verification was failing. The solution was to include the Diversion header in the INVITE for leg 2 and to use signalling manipulation to copy the number into the From header.

To define the signalling manipulation to copy the number in the Diversion header into the From header in the INVITE messages for leg 2, navigate to **Global Profiles → Signaling Manipulation** in the main menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor. The title in the example is `Diversion_In_From`. The script text is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and
  %METHOD="INVITE"
  {
    if(exists(%HEADERS["Diversion"][1]))then
    {
      %DivUser = %HEADERS["Diversion"][1].URI.USER;
      %HEADERS["From"][1].URI.USER = %DivUser;
      remove(%HEADERS["From"][1].DISPLAY_NAME);
    }
  }
}
```

Once entered and saved, the script appears as shown in the following screenshot:



Note: This will only take effect when selected in the **Signalling Manipulation Script** drop down menu in the advanced Trunk Server settings. The Trunk server is defined in **Section 7.6** and is named **SP_Trunk_Server**.

7.6. Define Servers

A server definition is required for each server connected to the Avaya SBCE. In this case, Netia SIP Trunk 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** 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**.
- If TLS is to be used for the signalling transport between the Session Manager and the Avaya SBCE, check **TLS** in **Supported Transports**.
- Define the **TLS** port for SIP signalling, **5061** is used for the Session Manager and click **Finish**.

The screenshot shows a web-based configuration interface. On the left, a sidebar titled 'Server Profiles' contains two items: 'ASM_Call_Server' (highlighted in red) and 'SP_Trunk_Server'. Above this sidebar is an 'Add' button. The main area is a dialog box titled 'Edit Server Configuration Profile - General' with a close button 'X' in the top right corner. The dialog contains the following fields and controls:

- Server Type:** A dropdown menu set to 'Call Server'.
- IP Addresses / Supported FQDNs:** A text area containing '10.10.79.61'. Below the text area is the instruction 'Separate entries with commas'.
- Supported Transports:** Three checkboxes: 'TCP' (unchecked), 'UDP' (unchecked), and 'TLS' (checked).
- TCP Port:** An empty text input field.
- UDP Port:** An empty text input field.
- TLS Port:** A text input field containing '5061'.
- Finish:** A button at the bottom right of the dialog.

- 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**.
- If TLS is to be used between the Session Manager and the Avaya SBCE, select the **AvayaSBCCClient** predefined Avaya TLS client in the **TLS Client Profile** drop down menu.
- Click **Finish**.

To define Netia SIP Trunk 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 Netia SIP Trunk 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 Netia SIP Trunk
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for UPC

- Click **Next** and check the **Enable Authentication** box (not shown).
- Define the Authentication parameters as provided by Netia.

Edit Server Configuration Profile - Authentication

Enable Authentication ☒

User Name

Realm
(Leave blank to detect from server challenge)

Password

Confirm Password

Finish

- Click **Next** again then select the **Interworking Profile** for the Netia SIP Trunk defined in **Section 7.4** from the drop down menu.
- If required, select the **Signaling Manipulation Script** defined in **Section 7.5**.

Edit Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile

Signaling Manipulation Script

UDP Connection Type
☒ SUBID ☐ PORTID ☐ MAPPING

Finish

Note: See **Section 7.5** for the **Signalling Manipulation Script**.

7.7. Define Routing

Routing information is required for routing to the Session Manager on the internal side and Netia SIP Trunk 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 for TCP and UDP, and 5061 for TLS. 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 **Call Server**, and click **Next**.
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field.
- Select **TLS** for the **Outgoing Transport**.
- Click **Finish**.

The screenshot shows the 'Edit Routing Rule' dialog box. The left sidebar has a 'Routing Profiles: Call Server' section with an 'Add' button. The main area is titled 'Edit Routing Rule' and contains the following fields:

- URI Group**: A dropdown menu with a '*' icon.
- Next Hop Server 1**: A text field containing '10.10.79.61'.
- Next Hop Server 2**: A text field.
- Routing Priority based on Next Hop Server**: A checkbox that is checked.
- Use Next Hop for In Dialog Messages**: A checkbox that is unchecked.
- Ignore Route Header for Messages Outside Dialog**: A checkbox that is unchecked.
- NAPTR**: A checkbox that is unchecked.
- SRV**: A checkbox that is unchecked.
- Outgoing Transport**: Radio buttons for TLS (selected), TCP, and UDP.
- Finish**: A button at the bottom.

To define routing to Netia SIP Trunk, 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 Netia SIP Trunk, in this case a generic name of **Trunk Server** was used, and click **Next**.
- Enter the Netia SIP Trunk IP address and port in the **Next Hop Server 1** field.
- Select **UDP** for the **Outgoing Transport**.
- Click **Finish**.

Edit Routing Rule X

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

Next Hop Routing

URI Group * ▾

Next Hop Server 1 192.168.129.4
IP, IP:Port, Domain, or Domain:Port

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

7.8. 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 addresses. 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** 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**, **Via** and **To** 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 **SDP** 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**.

Topology Hiding Profiles: ASM

Buttons: Add, Rename, Clone, Delete

Topology Hiding Profiles: default, cisco_th_profile, **ASM**, Netia

Click here to add a description.

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

Edit

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 Netia SIP Trunk.

To define Topology Hiding for Netia SIP Trunk, 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 Netia SIP Trunk and click **Next**.
- If the **Request-Line**, **Record-Route**, **Via** and **To** 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 **SDP** 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).

Topology Hiding Profiles: Netia

Click here to add a description.

Topology Hiding

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

7.9. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.10**. The Netia SIP Trunk was tested with SRTP in the enterprise, and a Media Rule was required for conversion between SRTP and RTP.

7.9.1. Media Rules

Media rules are a mechanism on the Avaya SBCE to handle any unusual media handling scenarios that may be encountered for a particular Service Provider. In the case of Netia SIP Trunk, this was the conversion between SRTP and RTP.

To define the media rule, navigate to **Domain Policies** → **Media Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Media Rule pop-up box.

- In the **Rule Name** field enter a descriptive name for the Netia SIP Trunk media rule and click **Next** and **Next** again, then **Finish**.
- Click on the **Media Encryption** tab and then click on **Edit**.
- Select the **Preferred Format #1** from the drop down menu, in test **SRTP_AES_CM_128_HMAC_SHA1_80** was used.
- Video is not currently offered as part of the solution, but if required select the preferred format for video.
- Ensure **Interworking** is checked so that the conversion to RTP can take place.
- Leave **Capability Negotiation** unchecked as it is not required in this solution.
- Click **Finish**.

The screenshot displays the 'Session Border Controller for Enterprise' web interface. On the left, a navigation menu shows 'Domain Policies' expanded, with 'Media Rules' selected. The main panel shows 'Media Rules: Netia-low-med-enc' with a list of rules including 'default-low-med', 'default-low-med-enc', 'default-high', 'default-high-enc', 'avaya-low-med-enc', and 'Netia-low-med-enc'. The 'Netia-low-med-enc' rule is selected, and the 'Media Encryption' tab is active. The right-hand pane shows the configuration for this rule, divided into 'Audio Encryption', 'Video Encryption', and 'Miscellaneous' sections.

Audio Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input type="checkbox"/>
Interworking	<input checked="" type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

At the bottom right of the configuration pane is a 'Finish' button.

7.9.2. End Point Policy Group

An End Point Policy Group is required to implement the media rule. To define one for use in the Session Manager server flow, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name for the Session Manager Policy Group, in this case **Netia-def-low-enc**, and click **Next**.
- Leave the **Application Rule** and **Border Rule** at their default values.
- Select the **Media Rule** created in the previous section in the drop down menu.
- Leave the **Security Rule**, **Signalling Rule** and **Time of Day Rule** at their default values.

Policy Groups: Netia-def-low-enc

Add Filter By Device... Re

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc
- avaya-def-high-sub...
- avaya-def-high-ser...
- Netia-def-low-enc

Order A

1 def

Policy Group

Click here to add a description.

Click here to add a row description.

Edit Policy Set X

Application Rule default

Border Rule default

Media Rule Netia-low-med-enc

Security Rule default-low

Signaling Rule default

Time of Day Rule default

Finish

7.10. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the Netia SIP Trunk. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to Netia SIP Trunk and vice versa.

To define a Server Flow for the Session Manager, 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 **ASM Call Server** was used.
- In the **Transport** drop-down menu, select the transport to be used, in this case **TLS**.
- 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 internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for the Session Manager 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 Session Manager is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of Netia SIP Trunk defined in **Section 7.7**.
- In the **End Point Policy Group** drop down menu, select the policy group defined in **Section 7.9**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.8** and click **Finish**.

Edit Flow: ASM Call Server	
Flow Name	ASM Call Server
Server Configuration	ASM_Call_Server
URI Group	*
Transport	TLS
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Med
End Point Policy Group	Netia-deflow-enc
Routing Profile	Trunk Server
Topology Hiding Profile	ASM
File Transfer Profile	None
<div>Finish</div>	

To define a Server Flow for Netia SIP Trunk, 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 Netia SIP Trunk, in this case a generic name of **SP Trunk Server** was used.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**. This is the interface that signalling bound for Netia SIP Trunk 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 Netia SIP Trunk 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 Netia SIP Trunk is sent on.
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Netia SIP Trunk defined in **Section 7.8** and click **Finish**.

Edit Flow: SP Trunk Server	
Flow Name	SP Trunk Server
Server Configuration	SP_Trunk_Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Med
End Point Policy Group	default-low
Routing Profile	Call Server
Topology Hiding Profile	Netia
File Transfer Profile	None
<div>Finish</div>	

The information for all Server Flows is shown on a single screen on the Avaya SBCE.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar lists various configuration categories, with "End Point Flows" highlighted under "Device Specific Settings". The main content area is titled "End Point Flows: GSSCP_R3S3" and features a "Devices" tab with "GSSCP_R3S3" selected. Below this, there are tabs for "Subscriber Flows" and "Server Flows", with "Server Flows" being the active tab. An "Add" button is located in the top right of the Server Flows section. A blue banner提示 "Hover over a row to see its description." is present. Two tables are shown, each with a title: "Server Configuration: ASM Call Server" and "Server Configuration: SP Trunk Server". Both tables have columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The first table lists "ASM Call Server" with priority 1, URI Group "*", Received Interface "Ext_Sig", Signaling Interface "Int_Sig", End Point Policy Group "Netia-def-low-enc", and Routing Profile "Trunk Server". The second table lists "SP Trunk Server" with priority 1, URI Group "*", Received Interface "Int_Sig", Signaling Interface "Ext_Sig", End Point Policy Group "default-low", and Routing Profile "Call Server". Both tables include "View", "Clone", "Edit", and "Delete" links for each entry.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options

End Point Flows: GSSCP_R3S3

Devices
GSSCP_R3S3

Subscriber Flows Server Flows

Add

Hover over a row to see its description.

Server Configuration: ASM Call Server

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ASM Call Server	*	Ext_Sig	Int_Sig	Netia-def-low-enc	Trunk Server	View Clone Edit Delete

Server Configuration: SP Trunk Server

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SP Trunk Server	*	Int_Sig	Ext_Sig	default-low	Call Server	View Clone Edit Delete

8. Configure Netia SIP Trunk Equipment

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

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

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	CM_VM1	10.10.79.52	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	ASBCE_50	10.10.9.75	5061	TLS	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, 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 or **All** 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>All</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.

Trace: GSSCP_R3S3

Devices

GSSCP_R3S3

Call Trace

Packet Capture

Captures

Refresh

File Name	File Size (bytes)	Last Modified	
SIP_Trunk_Test_20131111160816.pcap	0	November 11, 2013 4:08:16 PM GMT	Delete

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 Netia 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 to Netia SIP Trunk Service. Netia 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**. At the time of writing, an ongoing issue remains with loss of media after 30 minutes on long duration calls. This is under investigation.

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.