



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

---

# **Application Notes for Configuring Avaya Aura® Communication Manager R6.3, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R7.0 to support TeleWare SIP Trunk Service - Issue 1.0**

### **Abstract**

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between the TeleWare 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. TeleWare is a member of the DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 TeleWare SIP Trunk service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of the following: Avaya Aura® Communication Manager R6.3 (Communication Manager); Avaya Aura® Session Manager R6.3 (Session Manager); Avaya Session Border Controller for Enterprise R7.0 (Avaya SBCE). Note that the shortened names shown in brackets will be used throughout the remainder of the document. Customers using this Avaya SIP-enabled enterprise solution with the TeleWare SIP Trunk service 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 connect to the TeleWare SIP Trunk service.

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 TeleWare SIP Trunk, calls made to SIP and H.323 telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the TeleWare SIP Trunk to PSTN destinations, calls made from SIP and H.323 telephones.
- Inbound and outbound PSTN calls to/from an Avaya one-X® Communicator soft phone and Avaya Communicator for Windows client.
- Calls using the G.711MU Law, G.711A Law and G.729 codecs. The G.729 included support for annex B.
- 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 between the Avaya SBCE and the SIP and H.323 telephones.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by the TeleWare SIP Trunk requiring Avaya response and sent by Avaya requiring TeleWare response.

## 2.2. Test Results

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

- Empty INVITE messages are used by Communication Manager for changing the media path (Shuffling) and call hold but are not supported by the TeleWare network. This was resolved by setting the Avaya SBCE to insert an SDP into empty INVITE messages.
- The TeleWare network is not failing inbound calls that have no matching codec. When the Communication Manager responds to the 180 Ringing with 488 Not Acceptable Here, the network sends another INVITE.
- No inbound toll-free access was available for testing.
- Access to Directory Enquiries was not tested as it was not available from TeleWare Lab environment.
- Emergency Services calls were not tested as no test call was booked with the Emergency Services Operator
- The TeleWare network does not send a display name, i.e. “Anonymous”, so SIP phones were changed to “display calling party number only” by changing the 46xxsettings file.
- There was no ringback on the calling PSTN phone when forwarding a call. This was resolved by turning off Initial IP-IP Direct Media on Communication Manager which allows the establishment of Early Media.
- After resolving the previous issue, there was still no ringback on the calling phone when forwarding calls to PSTN destinations. This was resolved by TeleWare.
- There was no response from the network to the re-INVITE sent after leg 2 of the transferred call was answered. This was resolved by removing proprietary SIP headers.
- Fax calls were failing due to a format of the SDP for T.38 that could not be handled by Communication Manager. The SDP was formatted such that “t38” appeared twice in the Media Description. This was resolved by TeleWare.
- The Calling Party Number was not correctly displayed on mobile phones when testing EC500. This was a general issue during testing and was due to the called and calling parties being international numbers (Ireland).
- When testing Avaya one-X Communicator connected via SIP, it was noted that there was no ringback on outbound calls when in “Other Phone” mode. Another Galway Lab PSTN phone was used for the “Other Phone”. This appears to be a general issue and not related to interoperability with the TeleWare network.
- When testing the network response to a Busy Trunk or a signalling failure, it was noted that an announcement was played from the TeleWare network saying “The other person has hung up”. This may not always be appropriate for this type of call failure.

## 2.3. Support

For technical support on TeleWare products please contact:

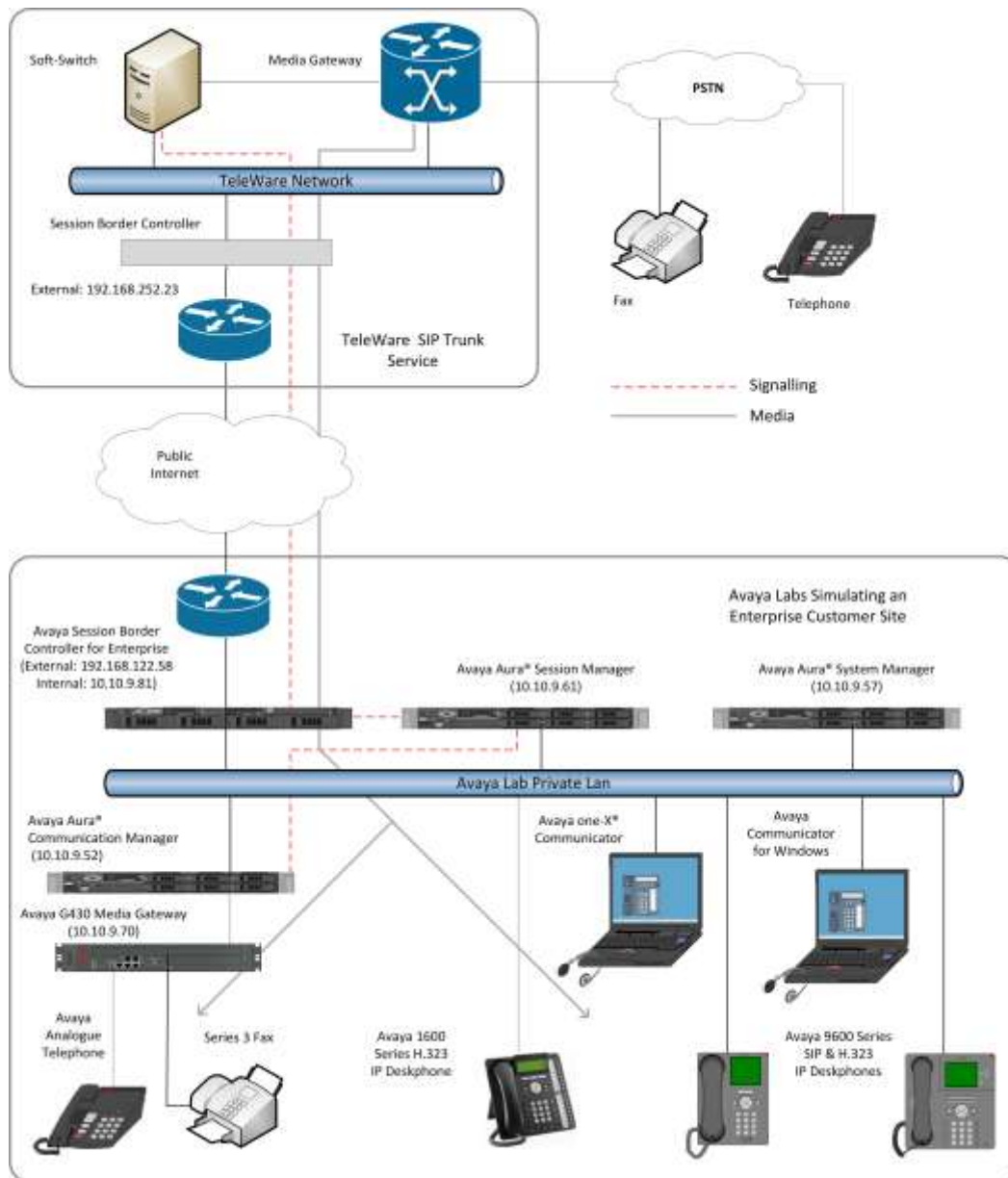
Email: [Help.desk@teleware.com](mailto:Help.desk@teleware.com)

Tel: +44 1845 521 084

Web: [www.teleware.com](http://www.teleware.com)

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an Enterprise site connected to the TeleWare SIP Trunk service. Located at the Enterprise site is an Avaya SBCE, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 16xx series IP telephones (with H.323 firmware), Avaya analogue telephones and an analogue fax machine. Also included in the test configuration was an Avaya one-X® Communicator soft phone and Avaya Communicator for Windows running on laptop PCs.



**Figure 1: Test Setup TeleWare 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
<b>Avaya</b>	
Avaya Aura® Session Manager	6.3.14.0.631402
Avaya Aura® System Manager	6.3.13.10.3336
Avaya Aura® Communication Manager	6.3.111 0-22460
Avaya Session Border Controller for Enterprise	7.0.1-03-8739
Avaya G430 Media Gateway	36.17.0
Avaya 9600 series Handsets:	
SIP 96x0	2_6_15_0
SIP 9608	6.5.0 R17
H.323 96x0	3.2.6A
H.323 9608	6.6.1.15 V474
H.323 1616	1.380B
Avaya One-X Communicator	6.2.10.03-FP10
Avaya Communicator for Windows	2.1.3.80
Avaya 2400 Series Digital Handsets	N/A
Analogue Handset	N/A
Analogue Fax	N/A
<b>TeleWare</b>	
ACME SBC	E3.6.0.M4P3, Build: 51172, Branch: 360m4p3
Teleware Intelligent Soft Pabx (TWISP)	Version 3.0.3.7

## 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 TeleWare SIP Trunk service. For incoming calls, Session Manager receives SIP messages from the 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 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 TeleWare 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 TeleWare SIP Trunk service 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	0
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		41000	0
Maximum Video Capable IP Softphones:		18000	0
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>20</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		522	0
Maximum TN2501 VAL Boards:		128	0
Maximum Media Gateway VAL Sources:		250	1
Maximum TN2602 Boards with 80 VoIP Channels:		128	0
Maximum TN2602 Boards with 320 VoIP Channels:		128	0
Maximum Number of Expanded Meet-me Conference Ports:		300	0

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

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

## 5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signalling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for Session Manager. In this case, **SM100** and **10.10.9.61** are the **Name** and **IP Address** for Session Manager SIP interface. Also note the **procr** IP address 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	
SM-BGVM1	10.10.79.61	
<b>SM100</b>	<b>10.10.9.61</b>	
default	0.0.0.0	
<b>procr</b>	<b>10.10.9.52</b>	
procr6	::	

### 5.3. Administer IP Network Region

Use the **change ip-network-region n** command where **n** is the chosen value of the configuration for the SIP Trunk. 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 direct media is used on a PSTN call, 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 **2** is used.
- The rest of the fields can be left at default values.

```
change ip-network-region 2                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2
Location: 1           Authoritative Domain: avaya.com
Name: Trunk           Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 2          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
```

**Note:** In the test configuration, ip-network-region 1 was used within the enterprise and ip-network-region 2 was used for the SIP Trunk. In the configuration of the G430 and Avaya Media Server (not shown) ip-network-region 1 was used in such a way that either one could be selected at call set-up.



## 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 n** where **n** is the chosen value of the configuration for the SIP Trunk. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codecs supported by TeleWare were configured, namely **G.711MU**, **G.711A** and **G.729B**.

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

TeleWare 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**. Note that the screenshot shows **t.38-G711-fallback**, this was tested for one of the incoming fax test cases.
- Leave **ECM** at default value of **y** for Error Correction.

change ip-codec-set 2				Page 2 of 2
IP CODEC SET				
Allow Direct-IP Multimedia? n				
	Mode	Redundancy	ECM:	Packet Size (ms)
<b>FAX</b>	<b>t.38-G711-fallback</b>	<b>0</b>	<b>y</b>	
Modem	off	0		
TDD/TTY	US	3		
H.323 Clear-channel	n	0		
SIP 64K Data	n	0		20

**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 TeleWare SIP Trunk service. During test, this was configured to use TCP and port 5062 though it's recommended to use TLS and port 5061 in the live environment to enhance security.

Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set **Group Type** to **sip**.
- Set **Transport Method** to **tcp**.
- Set **Peer Detection Enabled** to **y** allowing 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 Session Manager interface (node name **SM100** as defined in the **IP Node Names** form shown in **Section 5.2**).
- Set **Near-end Listen Port** and **Far-end Listen Port** as required. The standard value for TCP is **5060**.
- 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 region **2**).
- Leave **Far-end Domain** blank (allows Communication Manager to accept calls from any SIP domain on the associated trunk).
- Set **Direct IP-IP Audio Connections** to **y** to avoid unnecessary use of MGW resources
- Set **Initial IP-IP Direct Media** to **n** to facilitate the use of Early Media to avoid ringback issues.
- Leave **DTMF over IP** at default value of **rtp-payload** (Enables **RFC2833** for DTMF transmission from Communication Manager).

The default values for the other fields may be used.

change signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
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		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr		Far-end Node Name: SM100
Near-end Listen Port: 5060		Far-end Listen Port: 5060
		Far-end Network Region: 2
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 n** command, where **n** is an available trunk group for the SIP Trunk. 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** if the Diversion header is to be supported.
- 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 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: VM SM	COR: 1	TN: 1	TAC: 102
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 2	
		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 TeleWare to prevent unnecessary SIP messages during call setup. During testing, a value of **300** was used that sets Min-SE to 600 in the SIP signalling.

add trunk-group 2		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): 300			
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to **private**. This allows delivery of CLI in national format with leading “0” as required by TeleWare.

add trunk-group 2		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
<b>Numbering Format: private</b>		
UI Treatment: service-provider		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		

**Note:** If E.164 numbering is to be used, set the **Numbering Format** to **public**. This will allow CLI to be sent in E.164 format with leading “+”.

On **Page 4** of this form:

- Set **Support Request History** to **y** to provide History information to TeleWare.
- Set the **Telephone Event Payload Type** to **101** to match the value preferred by TeleWare (this Payload Type is not applied to calls from SIP end-points).
- Set **Always Use re-INVITE for Display Updates** to **y** so that INVITE messages are used instead of UPDATE messages which are not supported by TeleWare.
- Set **Identity for Calling Party Display** to **From** to ensure that where CLI for incoming calls is withheld, it is not displayed on Communication Manager extension.

add trunk-group 2		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? n		
<b>Support Request History? y</b>		
<b>Telephone Event Payload Type: 101</b>		
Convert 180 to 183 for Early Media? n		
<b>Always Use re-INVITE for Display Updates? y</b>		
<b>Identity for Calling Party Display: From</b>		
Block Sending Calling Party Location in INVITE? n		
Accept Redirect to Blank User Destination? n		
Enable Q-SIP? n		

## 5.7. Administer Calling Party Number Information

Use the **change private-numbering** command to configure Communication Manager to send the calling party number in the format required. During testing, calling party numbers were sent as national numbers with leading “0”. These calling party numbers are sent in the SIP From, Contact and PAI headers. The numbers are displayed on display-equipped PSTN telephones with any reformatting performed in the network.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2	1		4	Total Administered: 8
4	2000	2	018968nnnn0	11	Maximum Entries: 540
4	2290	2	018968nnnn5	11	
4	2292	2	018968nnnn2	11	
4	2316	2	018968nnnn3	11	
4	2391	2	018968nnnn1	11	
4	2396	2	018968nnnn4	11	
4	2401	2	018968nnnn6	11	

**Note:** During testing the extension numbers were reformatted to national numbers for Trunk Group 2 only. The numbers were analysed for Trunk Group 1 but not reformatted.

There are instances where numbers in the public numbering table are used, in particular the Contact header in SIP responses to INVITE messages from the TeleWare network. These can be left as extension numbers with no ill effect, but if it is required that they are sent as the DDI numbers, use the **change public-unknown-numbering** command. Specify the numbers as the full E.164 numbers, the leading “+” used in SIP is automatically added to all numbers specified in the public numbering table.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	2	1		4	Total Administered: 5
4	2000	2	4418968nnnn0	12	Maximum Entries: 9999
4	2292	2	4418968nnnn2	12	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
4	2391	2	4418968nnnn1	12	
4	2401	2	4418968nnnn6	12	

## 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 the TeleWare network. The single digit **9** was used as the ARS access code providing a facility for telephone users to dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure a digit as the **Auto Route Selection (ARS) - Access Code 1**.

<b>change feature-access-codes</b>	Page 1 of 10
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code: *69	
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code: 8	
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>	
Access Code 2:	

Use the **change ars analysis** command to configure the routing of dialled digits following the first digit **9**.

A small sample of dial patterns are shown here as an example. Further administration of ARS is beyond the scope of this document. The example entries shown will match outgoing calls to international numbers beginning 00 and national numbers beginning with 0. Note that exact maximum number lengths should be used where possible to reduce post-dial delay. Calls are sent to **Route Pattern 2**.

change ars analysis 0						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all					Percent Full: 0		
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Req'd
0		8	14	2	pubu		n
00		13	17	2	pubu		n
00353		10	14	2	pubu		n
0044		12	14	2	pubu		n
0083		8	14	2	pubu		n
01		7	14	2	pubu		n
01989		5	7	2	pubu		n
02		7	9	2	pubu		n
0800		11	11	2	pubu		n
118		5	6	2	pubu		n
1405		4	4	2	pubu		n

Use the **change route-pattern n** command, where **n** is an available route pattern, to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **2** is used to route calls to trunk group **2**. **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 **lev0-pvt** to ensure that a leading "+" was not prefixed to the called party number.

change route-pattern 2													Page 1 of 3				
Pattern Number: 2													Pattern Name: SIP Trunk				
SCCAN? n													Secure SIP? n				
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC			
No			Mrk	Lmt	List	Del	Digits						QSIG				
													Intw				
1:	2	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							lev0-pvt		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 Communication Manager extensions. The incoming digits sent in the INVITE message from TeleWare can be manipulated as necessary to route calls to the desired extension. Use the **change inc-call-handling-trmt trunk-group x** command where **x** is the Trunk Group defined in **Section 5.6**. In the example shown, **11** digits are received. All digits are deleted and the extension number is inserted. Note that some of the DDI digits have been obscured.

change inc-call-handling-trmt trunk-group 2					Page	1 of	3
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	11	018968nnnn0	11	2000			
public-ntwrk	11	018968nnnn1	11	2391			
public-ntwrk	11	018968nnnn2	11	2292			
public-ntwrk	11	018968nnnn3	11	2316			
public-ntwrk	11	018968nnnn4	11	2396			
public-ntwrk	11	018968nnnn5	11	2290			
public-ntwrk	11	018968nnnn6	11	2501			
public-ntwrk							
public-ntwrk							

## 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 2292. Use the command **change off-pbx-telephone station-mapping x** where **x** is Communication Manager station.

- The **Station Extension** field will automatically populate with station extension.
- For **Application** enter **EC500**.
- Enter a **Dial Prefix** if required by the routing configuration, none was required during testing.
- For the **Phone Number** enter the phone that will also be called (e.g. **003538941nnnn7**).
- Set the **Trunk Selection** to **ars** so that the ARS table will be used for routing.
- Set the **Config Set** to **1**.

change off-pbx-telephone station-mapping 2292							Page 1 of 3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION							
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode
2292	OPS	-		2292	aar	1	
2292	EC500	-		003538941nnnn7	ars	1	

**Note:** The phone number shown is for a mobile phone in the Avaya Lab. To use facilities such as Feature Name Extension (FNE) for calls coming in from EC500 mobile phones, the calling party number received in Communication Manager must exactly match the number specified in the above table.

The additional line in the previous screenshot with **Application** of **OPS** is standard on SIP endpoints where the phone is registered to the Session Manager and is essentially “Off PBX”.

Save Communication Manager configuration by entering **save translation**.



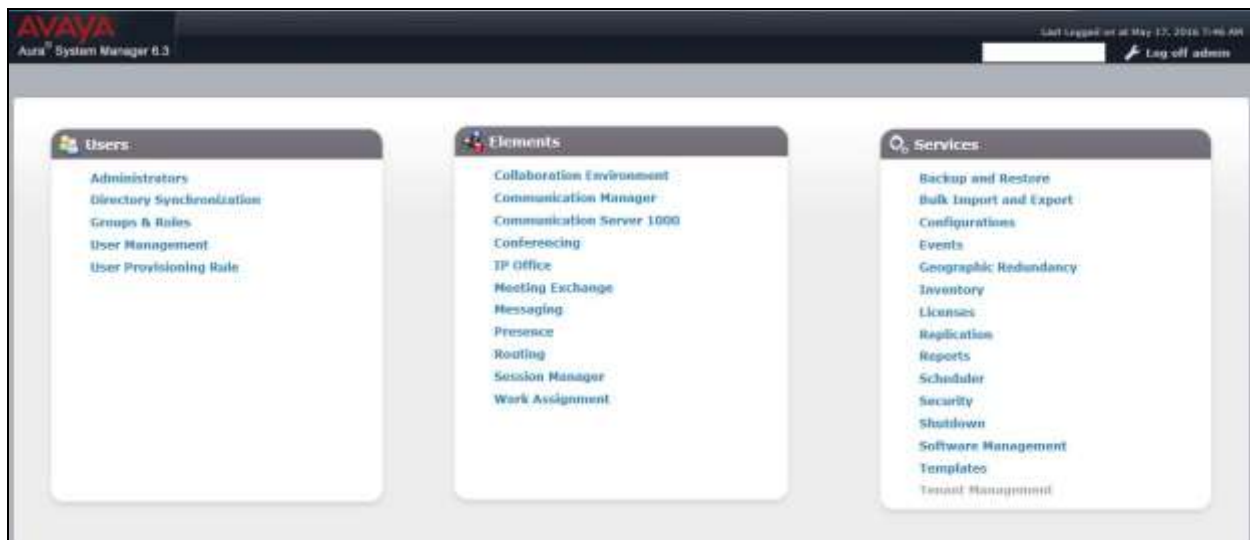
## 6. Configuring Avaya Aura® Session Manager

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 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.



## 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 TeleWare; 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.



**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

Location Details Commit Cancel

**General**

\* Name:

Notes:

**Dial Plan Transparency in Survivable Mode**

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

**Per-Call Bandwidth Parameters**

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

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

\* Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:  Kbit/sec

**Alarm Threshold**

Overall Alarm Threshold:  %

Multimedia Alarm Threshold:  %

\* Latency before Overall Alarm Trigger:  Minutes

\* Latency before Multimedia Alarm Trigger:  Minutes

**Location Pattern**

3 Items

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.2.*	
<input type="checkbox"/>	* 10.10.3.*	
<input type="checkbox"/>	* 10.10.9.*	

Select : All, None

## 6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to 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 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 if required (not used in this case).
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are four SIP Entities:

- Avaya Aura® Session Manager SIP Entity.
- Avaya Aura® Communication Manager SIP Entity for the SIP Endpoints
- Avaya Aura® Communication Manager SIP Entity for the SIP Trunk
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity for PSTN destinations.

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

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

The screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The form contains the following fields:

- Name:** Session Manager
- FQDN or IP Address:** 10.10.9.61
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text area)
- Location:** Galway (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- Credential name:** (empty text area)

Below the 'General' tab is the 'SIP Link Monitoring' section, which contains a single dropdown menu labeled 'SIP Link Monitoring' set to '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.

The screenshot shows a configuration window titled "Port". At the top, there are input fields for "TCP Failover port:" and "TLS Failover port:", each followed by a text box. Below these are "Add" and "Remove" buttons. The main part of the window is a table with the following columns: "Port", "Protocol", "Default Domain", and "Notes". The table contains three rows of data:

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

At the bottom left, there is a "Select" dropdown menu with options "All" and "None". At the top right of the table area, there is a "Filter: Enable" button.

#### 6.4.2. Avaya Aura® Communication Manager SIP Entities

The following screen shows one of the SIP entities for Communication Manager which is configured as an Evolution Server. This SIP Entity is used for the SIP Trunk. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signalling. Set the **Location** to that defined in **Section 6.3**.

The screenshot shows the "SIP Entity Details" configuration page. The breadcrumb navigation at the top is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details". There are "Commit" and "Cancel" buttons at the top right. The "General" tab is selected. The configuration fields are as follows:

- Name:** CM\_Trunk
- FQDN or IP Address:** 10.10.9.52
- Type:** CM
- Notes:** (empty text box)
- Adaptation:** (empty dropdown menu)
- Location:** Galway
- Time Zone:** Europe/Dublin
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text box)
- Call Detail Recording:** none

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

This screenshot shows the configuration options for a SIP Entity. It includes sections for 'Loop Detection' and 'SIP Link Monitoring'. The 'Loop Detection Mode' is set to 'Off'. The 'SIP Link Monitoring' is set to 'Use Session Manager Configuration'. There are checkboxes for 'Supports Call Admission Control' and 'Shared Bandwidth Manager', both of which are unchecked. Below these are two dropdown menus for 'Primary Session Manager Bandwidth Association' and 'Backup Session Manager Bandwidth Association'.

<b>Loop Detection</b>	Loop Detection Mode: Off
<b>SIP Link Monitoring</b>	SIP Link Monitoring: Use Session Manager Configuration
Supports Call Admission Control: <input type="checkbox"/>	
Shared Bandwidth Manager: <input type="checkbox"/>	
Primary Session Manager Bandwidth Association: [Dropdown]	
Backup Session Manager Bandwidth Association: [Dropdown]	

**Note:** A second SIP Entity for Communication Manager is required for SIP Endpoints. In the test environment this is named “CM\_Endpoints”.

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

The following screen shows the SIP Entity for the Avaya SBCE used for PSTN destinations. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface used for PSTN fixed calls (see **Figure 1**). Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.

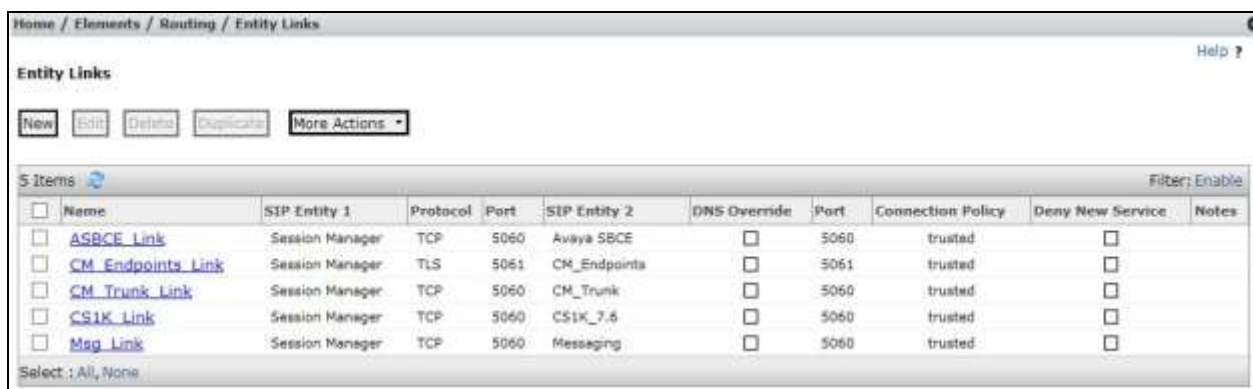
This screenshot shows the 'SIP Entity Details' configuration page. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

* Name:	Avaya SBCE
* FQDN or IP Address:	10.10.9.81
Type:	SIP Trunk
Notes:	
Adaptation:	[Dropdown]
Location:	Galway
Time Zone:	Europe/Dublin
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

## 6.5. 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 6.4**.
- 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.



<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	<a href="#">ASBCE Link</a>	Session Manager	TCP	5060	Avaya SBCE	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">CM_Endpoints Link</a>	Session Manager	TLS	5061	CM_Endpoints	<input type="checkbox"/>	5061	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">CM_Trunk Link</a>	Session Manager	TCP	5060	CM_Trunk	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">CS1K Link</a>	Session Manager	TCP	5060	CS1K_7.6	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	<a href="#">Msg Link</a>	Session Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

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

**Note:** There are two Entity Links for Communication Manager, one for the SIP Endpoints and the other for the SIP Trunk. These are differentiated by port number.

## 6.6. 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 calls inbound from the SIP Trunk to Communication Manager.

Home / Elements / Routing / Routing Policies Help ?

**Routing Policy Details** Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM_Trunk	10.10.9.52	CM	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item 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 PSTN destinations via the TeleWare SIP Trunk.

Home / Elements / Routing / Routing Policies Help ?

**Routing Policy Details** Commit Cancel

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.9.61	SIP Trunk	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item 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



## 6.7. 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 6.6**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for the Avaya SBCE which will analyse the leading zero of the called party number and route the calls to PSTN destinations via TeleWare SIP Trunk.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

Help ?

General

\* Pattern: 0

\* Min: 8

\* Max: 16

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

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		to_AvayaSBCE	0	<input type="checkbox"/>	Avaya SBCE	

Select : All, None

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

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel Help ?

**General**

\* Pattern: 016968nnnn

\* Min: 11

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

**Originating Locations and Routing Policies**

Add Remove

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"/>	Gateway		CM_Trunk	0	<input type="checkbox"/>	CM_Trunk	

Select : All, None

**Note:** The above configuration is used to analyse the DDI numbers assigned to the extensions on Communication Manager. Some of the digits of the pattern to be matched have been obscured.

## 6.8. 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 Communication Manager.
- In the **CM System for SIP Entity** field select the SIP entity for Communication Manager and select **Commit** to save the configuration.

Home / Elements / Session Manager / Application Configuration / Applications

**Application Editor** Commit Cancel

**Application**

\*Name: CM\_App

\*SIP Entity: CM\_Endpoints

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

Description:

**Note:** The Application described here and the Application Sequence described in the next section are likely to have been defined during installation. The configuration is shown here for reference. Note also that the Communication Manager SIP Entity selected is that set up specifically for SIP endpoints. In the test environment there is also a Communication Manager SIP Entity that is used specifically for the SIP Trunk and is not to be used in this case.

## 6.9. 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**.

Home / Elements / Session Manager / Application Configuration / Application Sequences

**Application Sequence Editor** Commit Cancel

**Application Sequence**

\*Name:

Description:

**Applications in this Sequence**

Move First Move Last Remove

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	***	CM_App	CM_Endpoints	<input checked="" type="checkbox"/>	

Select: All, None

**Available Applications**

1 Item Filter: Enable

Name	SIP Entity	Description
+ CM_App	CM_Endpoints	

\*Required Commit Cancel

## 6.10. Administer SIP Extensions

The SIP extensions are likely to have been defined during installation. The configuration shown in this section is for reference. SIP extensions are registered with 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. **2292@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 'New User Profile' form in the Avaya User Management interface. The form is divided into tabs: Identity, Communication Profile, Membership, and Contacts. The Identity tab is active, showing fields for User Provisioning Rule, Last Name, First Name, Login Name, Authentication Type, Password, Confirm Password, Localized Display Name, Endpoint Display Name, Title, Language Preference, Time Zone, Employee ID, Department, and Company. The form is pre-filled with example data: Last Name: SIP, First Name: 9608, Login Name: 2292@avaya.com, Authentication Type: Basic, Password: 9608, Confirm Password: 9608, Language Preference: English (United Kingdom), Time Zone: (+1:0)GMT : Dublin, Edinburgh.

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

The screenshot shows the 'Communication Profile' tab in a configuration window. At the top, there are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' section has two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these is a 'Name' section with a 'Primary' radio button selected and a 'Default' checkbox checked. The 'Communication Address' section is expanded, showing a table with columns 'Type', 'Handle', and 'Domain'. The table is currently empty, displaying 'No Records found'. There are 'New', 'Edit', and 'Delete' buttons at the top of the table.

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.

This screenshot shows the 'Communication Address' configuration window after clicking 'New'. The table now has one entry. The 'Type' field is set to 'Avaya SIP'. The 'Fully Qualified Address' field is populated with '2292' and the domain is set to 'avaya.com'. The 'Add' and 'Cancel' buttons are visible at the bottom right.

Type	Handle	Domain
Avaya SIP	2292	avaya.com

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 6.9**.
- Select the appropriate application sequence from the drop-down menu in the **Termination Sequence** field configured in **Section 6.9**.
- Select the appropriate location from the drop-down menu in the **Home Location** field.

☒ **Session Manager Profile** ▼

**SIP Registration**

- \* Primary Session Manager Session Manager ▼
- Secondary Session Manager (None) ▼
- Survivability Server (None) ▼
- Max. Simultaneous Devices 1 ▼
- Block New Registration When Maximum Registrations Active? ☐

**Application Sequences**

- Origination Sequence cm-app-seq ▼
- Termination Sequence cm-app-seq ▼

**Call Routing Settings**

- \* Home Location Galway ▼
- Conference Factory Set (None) ▼

**Call History Settings**

- Enable Centralized Call History? ☐

Expand the **Endpoint Profile** section.

- Select Communication Manager Element 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 Communication Manager user configuration automatically.

The screenshot shows the 'CM Endpoint Profile' configuration form. It includes fields for System (Communication Manager), Profile Type (Endpoint), Extension (2292), Template (9608SIP\_DEFAULT\_CM\_6\_3), Set Type (9608SIP), Security Code, Port (IP), Voice Mail Number, Preferred Handle (None), and checkboxes for 'Delete Endpoint on Unassign of Endpoint from User or on Delete User' and 'Override Endpoint Name and Localized Name'. There is also a 'Use Existing Endpoints' checkbox and an 'Endpoint Editor' button.

☒ **CM Endpoint Profile** ▼

\* System  ▼

\* Profile Type  ▼

Use Existing Endpoints ☐

\* Extension

\* Template  ▼

Set Type

Security Code

Port

Voice Mail Number

Preferred Handle  ▼

Enhanced Callr-Info display for 1-line phones ☐

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

Override Endpoint Name and Localized Name ☒



## 7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya 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 the appropriate username and password.



The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, 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." Below this is another disclaimer: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." Below that is a statement: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom is the copyright notice: "© 2011 - 2015 Avaya Inc. All rights reserved."

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 image shows the dashboard of the Avaya Session Border Controller for Enterprise. At the top is a navigation bar with links: Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below the navigation bar is the title "Session Border Controller for Enterprise" and the Avaya logo. On the left is a sidebar menu with the following items: Dashboard, Administration, Backup/Restore, System Management (with sub-items: Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings). The main content area is titled "Dashboard" and contains several sections: "Information" (with fields for System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged In at, and Failed Login Attempts), "Installed Devices" (with a table showing EMS and GSSCP\_VS), "Alarms (past 24 hours)" (showing "None found"), and "Incidents (past 24 hours)" (showing "None found").



## 7.2. Define Network Management

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 physical 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 for the external interfaces in the dialogue box:

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the external interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the external physical interface to be used from the **Interface** drop down menu. In the test environment, this was **B1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the external IP address of the Avaya SBCE on the SIP trunk in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

A screenshot of the 'Add Network' dialog box in the Avaya SBCE web interface. The dialog has a title bar 'Add Network' with a close button 'X'. It contains several input fields: 'Name' (text box with 'External'), 'Default Gateway' (text box with '192.168.122.7'), 'Subnet Mask' (text box with '255.255.255.128'), and 'Interface' (dropdown menu with 'B1' selected). Below these fields is an 'Add' button. At the bottom of the dialog, there is a table with three columns: 'IP Address', 'Public IP', and 'Gateway Override'. The 'IP Address' column has a text box with '192.168.122.58'. The 'Public IP' column has a dropdown menu with 'Use IP Address' selected. The 'Gateway Override' column has a dropdown menu with 'Use Default' selected. To the right of this table is a 'Delete' button. At the very bottom of the dialog is a 'Finish' button.

Click on **Add** to define the internal interface. Enter details in the dialogue box (not shown):

- Enter a descriptive name in the **Name** field.
- Enter the default gateway IP address for the internal interfaces in the **Default Gateway** field.
- Enter the subnet mask in the **Subnet Mask** field.
- Select the internal physical interface to be used from the **Interface** drop down menu. In the test environment, this was **A1**.
- Click on **Add** and an additional row will appear allowing an IP address to be entered.
- Enter the internal IP address for the Avaya SBCE in the **IP Address** field and leave the **Public IP** and **Gateway Override** fields blank.
- Click on **Finish** to complete the interface definition.

The following screenshot shows the completed Network Management configuration:



Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle the state. Change the state to **Enabled** where required.



**Note:** to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear that will indicate when the restart is complete.

## 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 TCP used for transport of signalling between Session Manager and the Avaya SBCE, and UDP for transport of signalling between the Avaya SBCE and the TeleWare SIP Trunk. This document shows the configuration for TCP and UDP, if additional security is required, it's recommended to use TLS and port 5061.

### 7.3.1. Signalling Interfaces

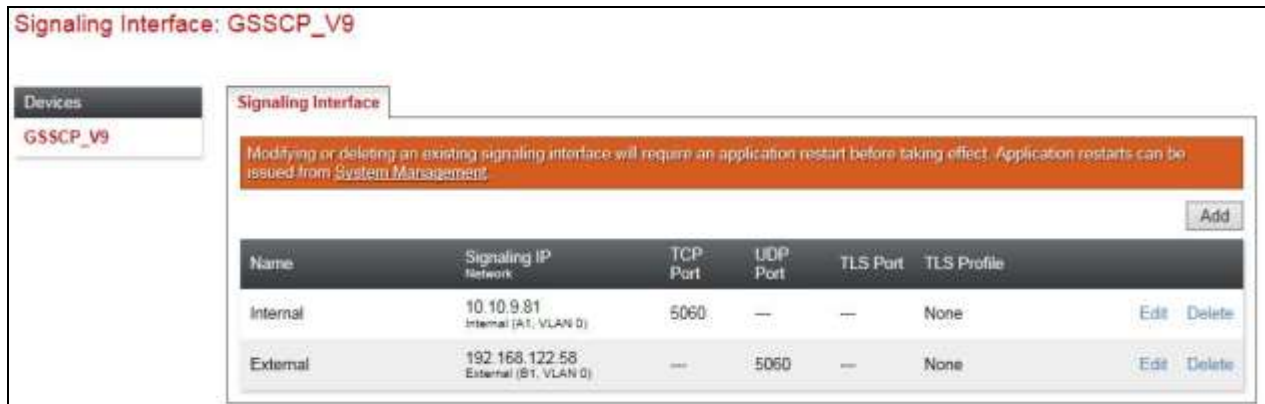
To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** (not shown) in the main menu on the left hand side. Details of transport protocol and ports for the external and internal SIP signalling are entered here.

- Select **Add** and enter details of the external signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external signalling interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **192.168.122.58** for the Avaya SBCE interface on the SIP Trunk.
- Enter the UDP port number in the **UDP Port** field, **5060** is used for the TeleWare SIP Trunk.

The internal signalling interface is defined in the same way; the dialogue box is not shown:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal signalling interface.
- In the **IP Address** drop down menus, select the internal network interface and IP address.
- Select **TCP** port number, **5060** is used for Session Manager.

The following screenshot shows details of the signalling interfaces:

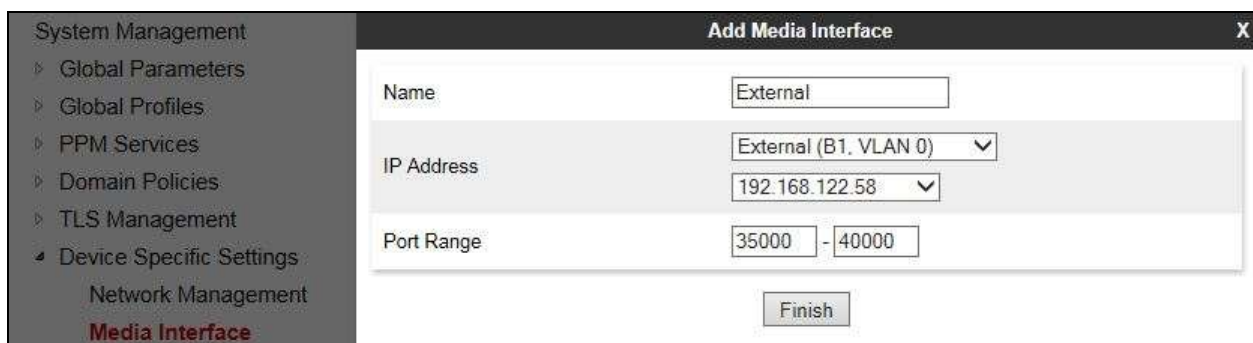


**Note:** In the test environment, the internal IP address was **10.10.9.81**.

### 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 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.

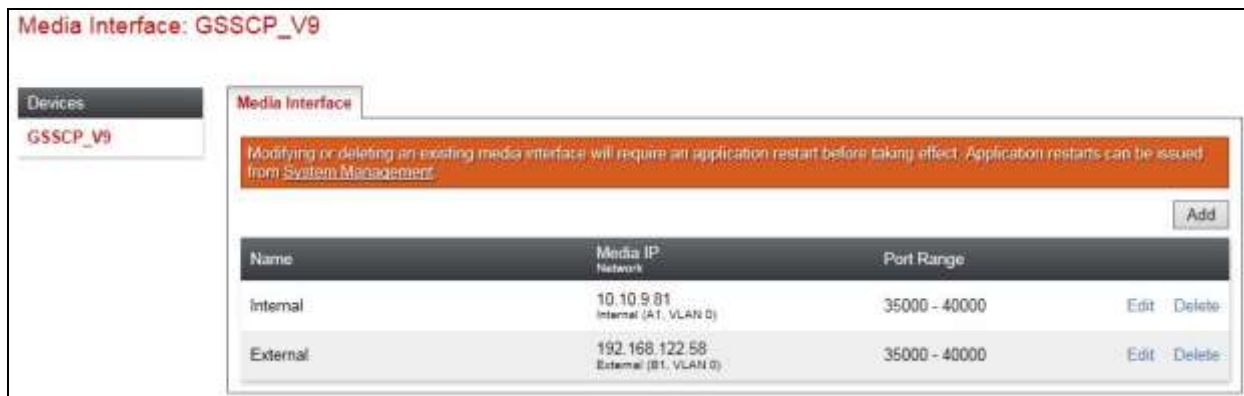
- Select **Add** and enter details of the external media interface in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- In the **IP Address** drop down menus, select the external network interface and IP address. Note that when the external network interface is selected, the bottom drop down menu is populated with the available IP addresses as defined in **Section 7.2**. In the test environment, this was IP address **192.168.122.58**.
- Define the **RTP Port Range** for the media path with the TeleWare SIP Trunk, during testing this was left at the default values of **35000** to **40000**.



The internal media interfaces are defined in the same way; the dialogue box is not shown:

- 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.
- In the **IP Address** drop down menus, select the internal network interface and IP address.

The following screenshot shows details of the media interfaces:

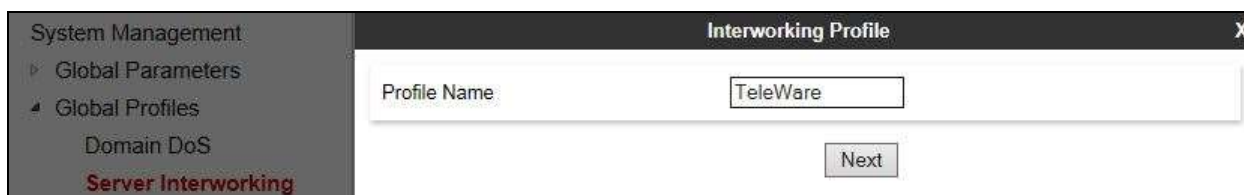


**Note:** In the test environment, the internal IP address was **10.10.9.81** and the port range was left at default values.

## 7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the TeleWare 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 TeleWare SIP Trunk service, click on **Add** (not shown). A pop-up menu is generated. In the **Name** field enter a descriptive name for the TeleWare network and click **Next**.



The Delayed SDP Handling in the Server Interworking is used to insert an SDP into a SIP INVITE that has no SDP. This is the case with Communication Manager shuffling and call hold. Shuffling is the Communication Manager function that changes the media path between a direct connection between the internal side of the SBC and the endpoint, and a connection via the Media Gateway or Media Server.

Check the **T.38 Support** and **Delayed SDP handling** boxes and click on **Next**.

Interworking Profile	
<b>General</b>	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input checked="" type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input checked="" type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Click on **Next** and **Next** again to go through the next two dialogue boxes. During testing, these were left at default values.

Interworking Profile	
<b>SIP Timers</b>	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Interworking Profile	
<b>Privacy</b>	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	



In the final dialogue box, leave the **Record Routes** at the default setting of **None** and ensure that the **Has Remote SBC** box is checked. Note that Avaya extensions are not supported for the SIP Trunk. Click on **Finish**

Repeat the process to define Server Interworking for Session Manager using the same parameter settings apart from **Delayed SDP Handling**. The following screenshot shows the **General** tab.

## 7.5. Define Servers

A server definition is required for each server connected to the Avaya SBCE. The TeleWare SIP Trunk is connected as a Trunk Server. Session Manager is connected as a Call Server.

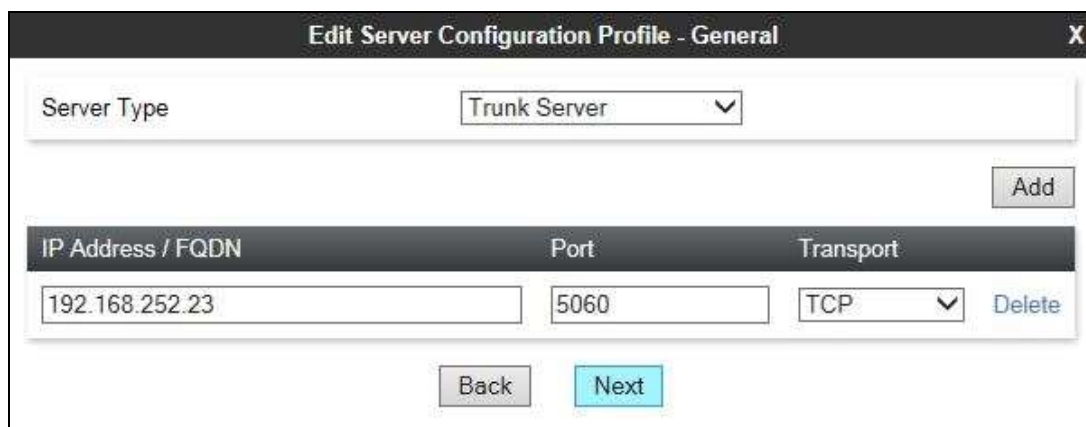
To define the TeleWare SIP Trunk Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. On the left is a sidebar menu with options: "Domain DoS", "Server Interworking", "Media Forking", "Routing", and "Server Configuration" (which is highlighted in red). The main area of the dialog has a text input field labeled "Profile Name" containing the text "NTWK". Below this field is a "Next" button.

Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the TeleWare SIP Trunk IP address.
- In the **Port** box, enter the port to be used for the SIP Trunk. The commonly used port for UDP is **5060**.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - General" with a close button (X) in the top right corner. The "Server Type" dropdown menu is set to "Trunk Server". There is an "Add" button to the right of the dropdown. Below this is a table with three columns: "IP Address / FQDN", "Port", and "Transport". The first row contains the values "192.168.252.23", "5060", and "TCP" (with a dropdown arrow). To the right of the table is a "Delete" button. At the bottom of the dialog are "Back" and "Next" buttons.

IP Address / FQDN	Port	Transport
192.168.252.23	5060	TCP



Click on **Next** and **Next** again. Leave the fields in the dialogue boxes at default values.

The image shows two side-by-side configuration dialog boxes. The left box is titled 'Add Server Configuration Profile - Authentication' and contains fields for 'Enable Authentication' (checkbox), 'User Name' (text box), 'Realm' (text box with a note '(Leave blank to detect from server challenge)'), 'Password' (text box), and 'Confirm Password' (text box). The right box is titled 'Add Server Configuration Profile - Heartbeat' and contains fields for 'Enable Heartbeat' (checkbox), 'Method' (dropdown menu with 'OPTIONS' selected), 'Frequency' (text box with 'seconds' unit), 'From URI' (text box), and 'To URI' (text box). Both boxes have 'Back' and 'Next' buttons at the bottom.

Click on **Next** again to get to the final dialogue box. This contains the **Advanced** settings:

- In the **Interworking Profile** drop down menu, select the **Interworking Profile** for TeleWare SIP Trunk defined in **Section 7.4**.
- Leave the other fields at default settings.
- Click **Finish**.

The image shows the 'Add Server Configuration Profile - Advanced' dialog box. It contains fields for 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (dropdown menu with 'TeleWare' selected), 'Signaling Manipulation Script' (dropdown menu with 'None' selected), 'Connection Type' (dropdown menu with 'SUBID' selected), and 'Securable' (checkbox). The 'Back' and 'Finish' buttons are at the bottom.

Use the process above to define the Call Server configuration for Session Manager if not already defined.

- Ensure that **Call Server** is selected in the **Server Type** drop down menu in the **General** dialogue box.
- Ensure that the Interworking Profile defined for Session Manager in **Section 7.4** is selected in the **Interworking Profile** drop down menu in the Advanced dialogue box

The following screenshot shows the **General** tab of the completed Server Configuration:

The screenshot shows the 'Server Configuration: CPE' window. On the left, there is a sidebar with 'Server Profiles' and 'CPE' (selected) and 'NTWK'. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing 'Server Type' as 'Call Server'. Below this is a table with columns 'IP Address / FQDN', 'Port', and 'Transport'. The table contains one row with the values '10.10.9.61', '5060', and 'TCP'. There are 'Add', 'Edit', 'Rename', 'Clone', and 'Delete' buttons.

IP Address / FQDN	Port	Transport
10.10.9.61	5060	TCP

The next screenshot shows the **Advanced** tab.

The screenshot shows the 'Server Configuration: CPE' window with the 'Advanced' tab selected. The settings are as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	ASM
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	<input type="checkbox"/>

## 7.6. Define Routing

Routing information is required for routing to the TeleWare SIP Trunk on the external side and Session Manager on the internal side. The IP addresses and ports defined here will be used as the destination addresses for signalling.

To define routing to TeleWare SIP Trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.

The screenshot shows the 'Routing Profile' dialog box. On the left, there is a sidebar with 'Global Profiles' and 'Routing' (selected). The main area has a 'Profile Name' field with the value 'WAN' and a 'Next' button.

Click on **Next** and enter details for the Routing Profile for the SIP Trunk:

- During testing, **Load Balancing** was not required and was left at the default value of **Priority**.
- Click on **Add** to specify an IP address for the SIP Trunk.
- Assign a priority in the **Priority / Weight** field, during testing **1** was used.
- Select the Server Configuration defined in **Section 7.5** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	NTWK	192.168.252.23:5060 (UDP)	None

Repeat the process for the Routing Profile for Session Manager: The following screenshot shows the completed configuration:

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.10.9.61	TCP

## 7.7. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop or external interfaces.

To define Topology Hiding for TeleWare SIP Trunk, navigate to **Global Profiles → Topology Hiding** in the main menu on the left hand side. Click on **Add** to bring up a dialogue box, assign an appropriate name and click on **Next** to configure Topology Hiding for each header as required:



The screenshot shows a window titled "Topology Hiding Profile" with a sidebar on the left containing menu items: "Server Interworking", "Media Forking", "Routing", "Server Configuration", and "Topology Hiding" (which is highlighted in red). The main area of the window has a "Profile Name" field containing the text "TeleWare" and a "Next" button.

Enter details in the **Topology Hiding Profile** pop-up menu.

- Click on **Add Header** and select from the **Header** drop down menu.
- Select **IP** or **IP/Domain** from the **Criteria** drop down menu depending on requirements. During testing the default **IP/Domain** was used for all headers that hides both domain names and IP addresses.
- Leave the **Replace Action** at the default value of **Auto** unless a specific domain name is required. In this case, select **Overwrite** and define a domain name in the **Overwrite Value** field.
- Topology hiding was defined for all headers where the function is available.



The screenshot shows the "Topology Hiding Profile" window after configuration. It features a table with the following columns: "Header", "Criteria", "Replace Action", and "Overwrite Value". The table contains one row with the values: "Request-Line" (selected from a dropdown), "IP/Domain" (selected from a dropdown), "Auto" (selected from a dropdown), and an empty "Overwrite Value" field. To the right of the table is a "Delete" button. Above the table is an "Add Header" button. Below the table are "Back" and "Finish" buttons.

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

The screenshot over the page shows the completed **Topology** Hiding configuration for the TeleWare SIP Trunk.

**Topology Hiding Profiles: TeleWare**

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco\_th\_profile

ASM

**TeleWare**

Click here to add a description

**Topology Hiding**

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

Edit

To define Topology hiding for Session Manager, follow the same process. This can be simplified by cloning the profile defined for TeleWare SIP Trunk. Do this by highlighting the profile defined for TeleWare and clicking on **Clone**. Enter an appropriate name for Session Manager and click on **Next** (not shown). Make any changes where required, in the test environment the settings were left at the same values.

**Topology Hiding Profiles: ASM**

Add Rename Clone Delete

Topology Hiding Profiles

default

cisco\_th\_profile

**ASM**

TeleWare

Click here to add a description

**Topology Hiding**

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

Edit

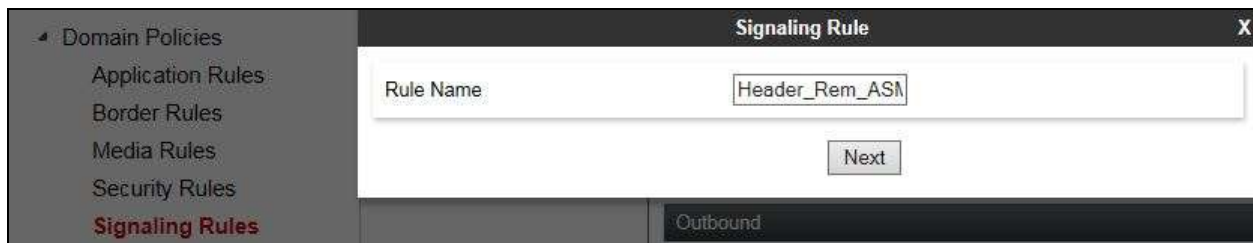
## 7.8. End Point Policy Groups

End Point Policy Groups are used to bring together a number of different rules for use in a server flow described in **Section 7.9**. The Teleware SIP Trunk was tested with signalling rules to remove both Avaya proprietary and TeleWare proprietary SIP headers. This was not necessary for the effective functioning of the SIP Trunk but was used to reduce the SIP message size.

## 7.8.1. Signalling Rules

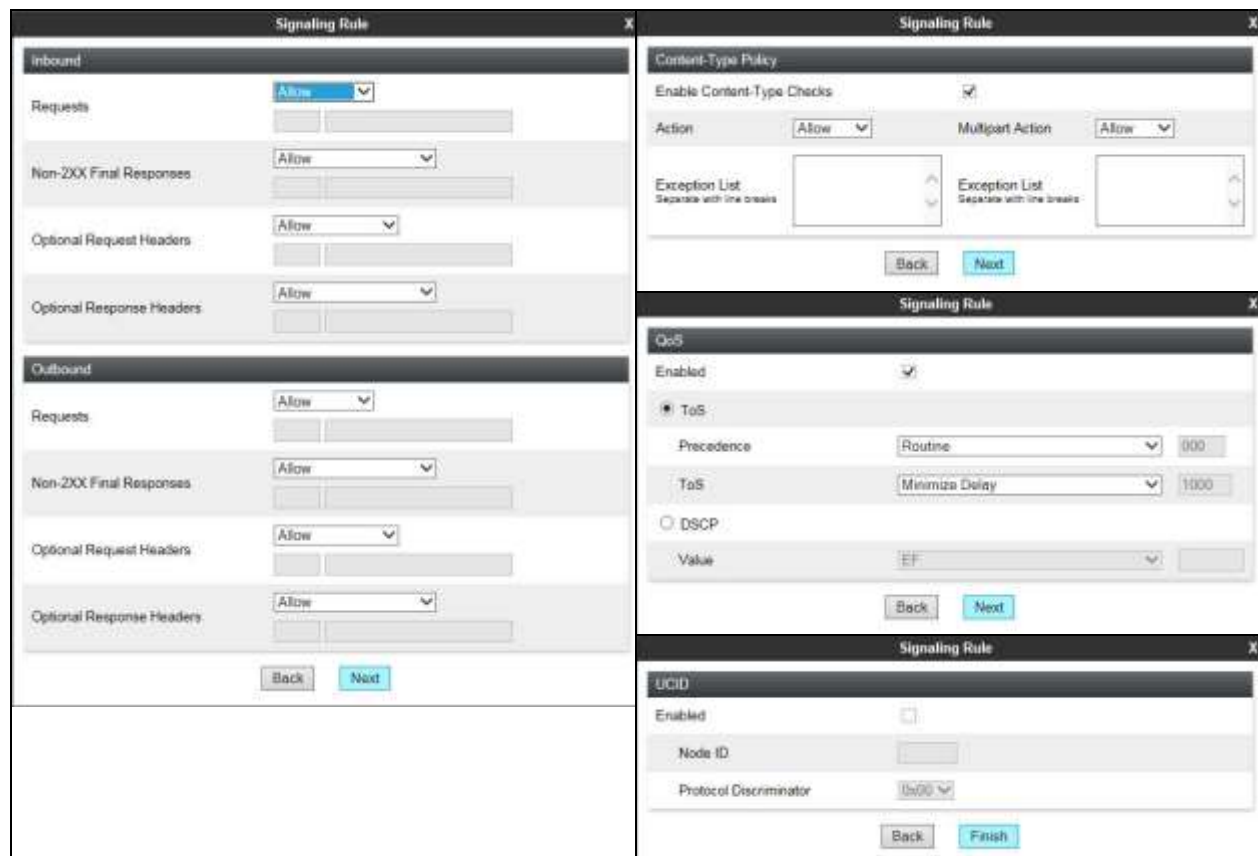
Signalling rules are a mechanism on the Avaya SBCE to handle any non-standard signalling that may be encountered on the SIP Trunk of a particular Service Provider. In the case of the Teleware SIP Trunk, this was the transmission of proprietary and unnecessary SIP message headers in the SIP messages.

To define a signalling rule to remove Avaya proprietary headers, navigate to **Domain Policies** → **Signaling Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Signaling Rule pop-up box. In the **Rule Name** field enter a descriptive name for the signalling rule, in this case **Header\_Rem\_ASM**.



The screenshot shows the 'Signaling Rule' configuration window. On the left, a sidebar lists 'Domain Policies' with sub-items: 'Application Rules', 'Border Rules', 'Media Rules', 'Security Rules', and 'Signaling Rules' (highlighted in red). The main panel shows the 'Rule Name' field containing 'Header\_Rem\_ASM' and a 'Next' button. Below the main panel, there is a tab labeled 'Outbound'.

Click on **Next** 3 times leaving the settings at default values then click on **Finish**.



The image displays three sequential screenshots of the 'Signaling Rule' configuration window, showing the progression through different sections:

- Inbound Section:** Shows settings for 'Requests', 'Non-2XX Final Responses', 'Optional Request Headers', and 'Optional Response Headers'. Each has a dropdown menu set to 'Allow' and a text input field.
- Content-Type Policy Section:** Shows 'Enable Content-Type Checks' checked, 'Action' set to 'Allow', and 'Multipart Action' set to 'Allow'. There are also 'Exception List' fields.
- QoS Section:** Shows 'Enabled' checked, 'ToS' selected with 'Precedence' set to 'Routine' and 'Value' set to '1000'. 'DSCP' is unselected with 'Value' set to 'EF'.

Each screenshot includes 'Back' and 'Next' buttons. The final screenshot also includes a 'Finish' button.

Once the rule is created, it is edited to provide the required functionality. To edit the rule, navigate to **Domain Policies → Signaling Rules** in the main menu on the left hand side and highlight the rule.

- Click on the **Request Headers** tab and then click on **Add In Header Control** (not shown).
- Either select a standard header from the **Header Name** drop down menu or check the **Proprietary Request Header** box and enter the name manually. The example shows **P-Location**.
- Select **ALL** from the **Method Name** drop down menu.
- Check the **Forbidden** button in the **Header Criteria** menu.
- Select **Remove Header** from the **Presence Action** drop down menu.

**Add Header Control**

Proprietary Request Header ☒

Header Name

Method Name

Header Criteria ☒ Forbidden ☐ Mandatory ☐ Optional

Presence Action

Apply the above to the following SIP Headers: Av-Global-Session-ID; Endpoint-View; P-AV-Message-Id; P-Charging-Vector; P-Location: The following screenshot shows the applied Request Header removal:

**Signaling Rules: Header\_Rem\_ASM**

Filter By Device:

Click here to add a description

General Requests Responses **Request Headers** Response Headers Signalling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	Edit	Delete
1	Av-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete



The same is required for Response Headers. In addition to applying the rule to the Request Headers listed previously which would be applied primarily to INVITE messages, the rule must also be applied to the response codes where the headers may be present. Response Headers are defined in the same way as Request Headers. The screenshot shows the additional drop down menu for **Response Code**. SIP header “Av-Global-Session-ID” is shown as an example. Click **Finish** to complete.

**Add Header Control**

Proprietary Response Header ☒

Header Name

Response Code

Method Name

Header Criteria  
☒ Forbidden  
☐ Mandatory  
☐ Optional

Presence Action

The screenshot below shows the applied Response Header removal:

**Signaling Rules: Header\_Rem\_ASM**

Click here to add a description

**General** **Requests** **Responses** **Request Headers** **Response Headers** **Signaling QoS** **UCID**

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Av-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Av-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Av-Global-Session-ID	4XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	P-Location	4XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete



Repeat the previous procedure to create a rule to remove TeleWare proprietary headers. In this case, the rule was named **Header\_Rem\_TeleWare**. The following screenshot shows the Request Headers:

Signaling Rules: Header\_Rem\_TeleWare

Buttons: Add, Filter By Device..., Rename, Clone, Delete

Click here to add a description

Tabs: General, Requests, Responses, **Request Headers**, Response Headers, Signaling QoS, UCID

Buttons: Add In Header Control, Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	TWID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	TWOriginator	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

The next screenshot shows the Response Headers:

Signaling Rules: Header\_Rem\_TeleWare

Buttons: Add, Filter By Device..., Rename, Clone, Delete

Click here to add a description

Tabs: General, Requests, Responses, Request Headers, **Response Headers**, Signaling QoS, UCID

Buttons: Add In Header Control, Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	TWID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	TWID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	TWOriginator	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	TWOriginator	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

## 7.8.2. End Point Policy Groups

End Point Policy Groups are required to implement the signalling rules. To define one for use in the SIP Trunk server flow to remove TeleWare proprietary headers, navigate to **Domain Policies** → **End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up box.

Media Rules  
Security Rules  
Signaling Rules  
**End Point Policy Groups**

Policy Group X

Group Name: Trunk-def-low

Next

Click on **Next** to configure the Policy Set. Enter details as follows:.

- Leave the **Application Rule**, **Border Rule**, **Media Rule** and **Security Rule** at their default values.
- Select the **Signaling Rule** created in the previous section in the drop down menu, in this case **Header\_Rem\_TeleWare**.
- Click on **Finish**.

The screenshot shows a 'Policy Group' configuration window with a title bar and a close button (X). Inside, there are five rows, each with a label and a dropdown menu:

Rule Type	Selected Value
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Header_Rem_TeleWare

At the bottom of the window are two buttons: 'Back' and 'Finish'.

To define an End Point Policy Group for use in the Session Manager server flow to remove Avaya proprietary headers, repeat the previous process but with a different **Signaling Rule**, in this case **Header\_Rem\_ASM**. The following screenshot shows a completed End Point Policy Group:

The screenshot shows a 'Policy Groups: ASM-def-low' window. On the left is a list of policy groups, with 'ASM-def-low' highlighted in red. The main area contains a table with the following data:

Order	Application	Border	Media	Security	Signaling	
1	default-trunk	default	default-low-med	default-low	Header_Rem_ASM	Edit

Below the table is a 'Summary' button. At the top right of the main area are buttons for 'Rename', 'Clone', and 'Delete'.

## 7.9. Server Flows

Server Flows combine the previously defined profiles into two End Point Server Flows, one for the Session Manager and another for the TeleWare SIP Trunk. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the TeleWare SIP Trunk and vice versa. To define a Server Flow for the TeleWare 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 **Flow Name** field enter a descriptive name for the server flow for the TeleWare SIP Trunk, in the test environment **TeleWare** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for the TeleWare SIP Trunk defined in **Section 7.5**.
- 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 the 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 the 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 the SIP Trunk is sent on.
- In the **End Point Policy Group** drop-down menu, select the End Point Policy Group defined for the TeleWare SIP Trunk in **Section 7.8**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the TeleWare SIP Trunk defined in **Section 7.7** and click **Finish**.

The screenshot shows a dialog box titled "Add Flow" with a close button (X) in the top right corner. The dialog contains the following fields and values:

Field	Value
Flow Name	TeleWare
Server Configuration	NTWK
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Internal
Signaling Interface	External
Media Interface	External
End Point Policy Group	Trunk-def-low
Routing Profile	LAN
Topology Hiding Profile	TeleWare
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom of the dialog is a button labeled "Finish".

To define a Server Flow for 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 **Flow Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **CPE** was used.
- In the **Server Configuration** drop-down menu, select the server configuration for Session Manager defined in **Section 7.5**.
- 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 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 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 Session Manager is sent on.
- In the **End Point Policy Group** drop-down menu, select the End Point Policy Group defined for the Session Manager in **Section 7.8**.
- In the **Routing Profile** drop-down menu, select the routing profile of the TeleWare SIP Trunk defined in **Section 7.6**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.7** and click **Finish**.

The screenshot shows a dialog box titled "Edit Flow: CPE" with a close button (X) in the top right corner. The dialog contains the following fields and values:

Field	Value
Flow Name	CPE
Server Configuration	CPE
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	External
Signaling Interface	Internal
Media Interface	Internal
End Point Policy Group	ASM-def-low
Routing Profile	WAN
Topology Hiding Profile	ASM
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom center of the dialog is a button labeled "Finish".

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

End Point Flows: GSSCP\_V9

Devices  
GSSCP\_V9

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: CPE

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
<input type="text" value="1"/>	CPE	*	External	Internal	ASM-def-low	WAN	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

Server Configuration: NTWK

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
<input type="text" value="1"/>	TeleWare	*	Internal	External	Trunk-def-low	LAN	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

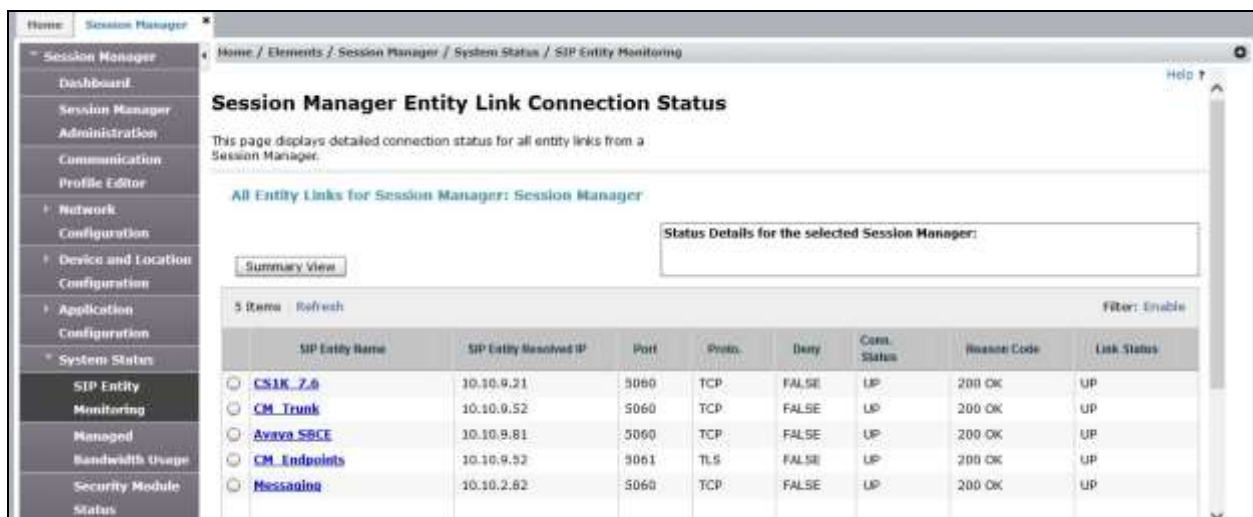
## 8. Configure the TeleWare SIP Trunk Equipment

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



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

status trunk 2			
TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00011	in-service/idle	no
0002/002	T00012	in-service/idle	no
0002/003	T00013	in-service/idle	no
0002/004	T00014	in-service/idle	no
0002/005	T00015	in-service/idle	no
0002/006	T00016	in-service/idle	no
0002/007	T00017	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 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**.

The screenshot displays the Avaya SBCE management interface. On the left, a sidebar lists various system management options, with 'Trace' highlighted at the bottom. The main content area is titled 'Trace: GSSCP\_V9'. Within this area, there is a 'Packet Capture' configuration window. This window has two tabs: 'Packet Capture' and 'Captures'. The 'Packet Capture' tab is currently selected, showing a form with the following fields: 'Status' (set to 'Ready'), 'Interface' (set to 'BT'), 'Local Address (IP Port)' (set to 'All'), 'Remote Address' (set to '\*'), 'Protocol' (set to 'All'), 'Maximum Number of Packets to Capture' (set to '10000'), and 'Capture Filename' (set to 'SIP\_Trunk\_Test.pcap'). Below these fields are two buttons: 'Start Capture' and 'Clear'.

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



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

## 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura ® Communication Manager R7.0, Avaya Aura ® Session Manager 7.0 and Avaya Session Border Controller for Enterprise R7.0 to the TeleWare SIP Trunk. The TeleWare SIP Trunk service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.



## 11. Additional References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3, May 2013.
- [2] *Administering Avaya Aura® System Platform*, Release 6.3, May 2013.
- [3] *Avaya Aura® Communication Manager using VMware® in the Virtualized Environment Deployment Guide*, May 2013
- [4] *Avaya Aura® Communication Manager 6.3 Documentation library*, August 2013.
- [5] *Avaya Aura® System Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [6] *Implementing Avaya Aura® System Manager* Release 6.3, May 2013
- [7] *Upgrading Avaya Aura® System Manager to 6.3.2*, May 2013.
- [8] *Administering Avaya Aura® System Manager* Release 6.3, May 2013
- [9] *Avaya Aura® Session Manager using VMware® in the Virtualized Environment Deployment Guide* Release 6.3 May 2013
- [10] *Implementing Avaya Aura® Session Manager* Release 6.3, May 2013
- [11] *Upgrading Avaya Aura® Session Manager* Release 6.3, May 2013
- [12] *Administering Avaya Aura® Session Manager* Release 6.3, June 2013,
- [13] *Deploying Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [14] *Upgrading Avaya Session Border Controller for Enterprise*, Release 7.0, August 2015
- [15] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Nov 2015
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

---

**©2016 Avaya Inc. All Rights Reserved.**

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

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