



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

---

# **Application Notes for Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to support Vodafone Netherlands Office Voice and Vodafone Netherlands OneVoice Corporate SIP Trunk Services - Issue 1.0**

## **Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone Netherlands Office Voice, Vodafone Netherlands OneVoice Corporate SIP Trunk Services and an Avaya SIP enabled enterprise solution. The Vodafone Netherlands Office Voice trunk is used for calls to and from fixed line PSTN locations, Vodafone Netherlands OneVoice Corporate trunk is used for calls to and from mobile telephone numbers as well as providing the ability for enterprise users to reach Vodafone mobile telephone numbers assigned to their account by dialing a four digit short code. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Vodafone Netherlands are a member of the DevConnect Service Provider program.

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

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone Netherlands and an Avaya SIP enabled enterprise solution using Vodafone Netherlands Office Voice and Vodafone Netherlands OneVoice Corporate SIP Trunk Services. These services are offered in conjunction with each other as a total solution, for clarity these services will be collectively referred to in this document as Vodafone Netherlands SIP Trunk Solution. The Avaya solution consists of Avaya Aura® Session Border Controller (AASBC), Avaya Aura® Session Manager and Avaya Aura® Communication Manager Evolution Server. Customers using this Avaya SIP enabled Enterprise solution with Vodafone Netherlands SIP Trunk Solution are able to place and receive calls via standards-based SIP trunks as an alternative to legacy analog or digital trunks.

The Vodafone Netherlands SIP Trunk Solution referenced within these Application Notes is designed for business customers. The solution provides two connections to the enterprise, Vodafone Netherlands Office Voice is a fixed line SIP trunk and Vodafone Netherlands OneVoice Corporate is a mobile SIP trunk. The Vodafone Netherlands Office Voice trunk is used for calls to and from fixed line PSTN locations, Vodafone Netherlands OneVoice Corporate trunk is used for calls to and from mobile telephone numbers as well as providing the ability for enterprise users to reach Vodafone mobile telephone numbers assigned to their account by dialing a four digit short code.

## 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 AASBC. The enterprise site was configured to use the SIP Trunk Solution provided by Vodafone Netherlands.

### 2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming PSTN calls to various phone types. Phone types included SIP, H.323 and digital telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing calls from the enterprise site were completed via Vodafone Netherlands to PSTN destinations.
- Outgoing calls from the enterprise to the PSTN were made from SIP, H.323 and Digital telephones.
- Inbound and outbound PSTN calls to/from the Avaya one-X® Communicator soft phone.
- Calls to Emergency Services (112)
- Calls using G.729, and G.711A codec's.
- Fax calls to/from a fax machine at the enterprise to a PSTN connected fax machine.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones.

- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Vodafone Netherlands requiring Avaya response and sent by Avaya requiring Vodafone Netherlands response.

## 2.2. Test Results

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

- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- T.38 Fax calls were unsuccessful when transiting the Netherlands Public Switch Telephone Network (PSTN) due to baud rate alterations occurring mid call. Fax calls using G.711A pass-through were successful.
- Queued ACD calls disconnect if they are not answered within 60 seconds. The Communication Manager sends a SIP 182 message when a call is queued. Vodafone Netherlands do not use the SIP 182 message to cancel any SIP timers but do cancel their SIP timers upon receipt of a SIP 200 message. To workaround this, a null announcement is used at the beginning of the ACD vector to force Communication Manager to answer the call in the vector and send a SIP 200 message.

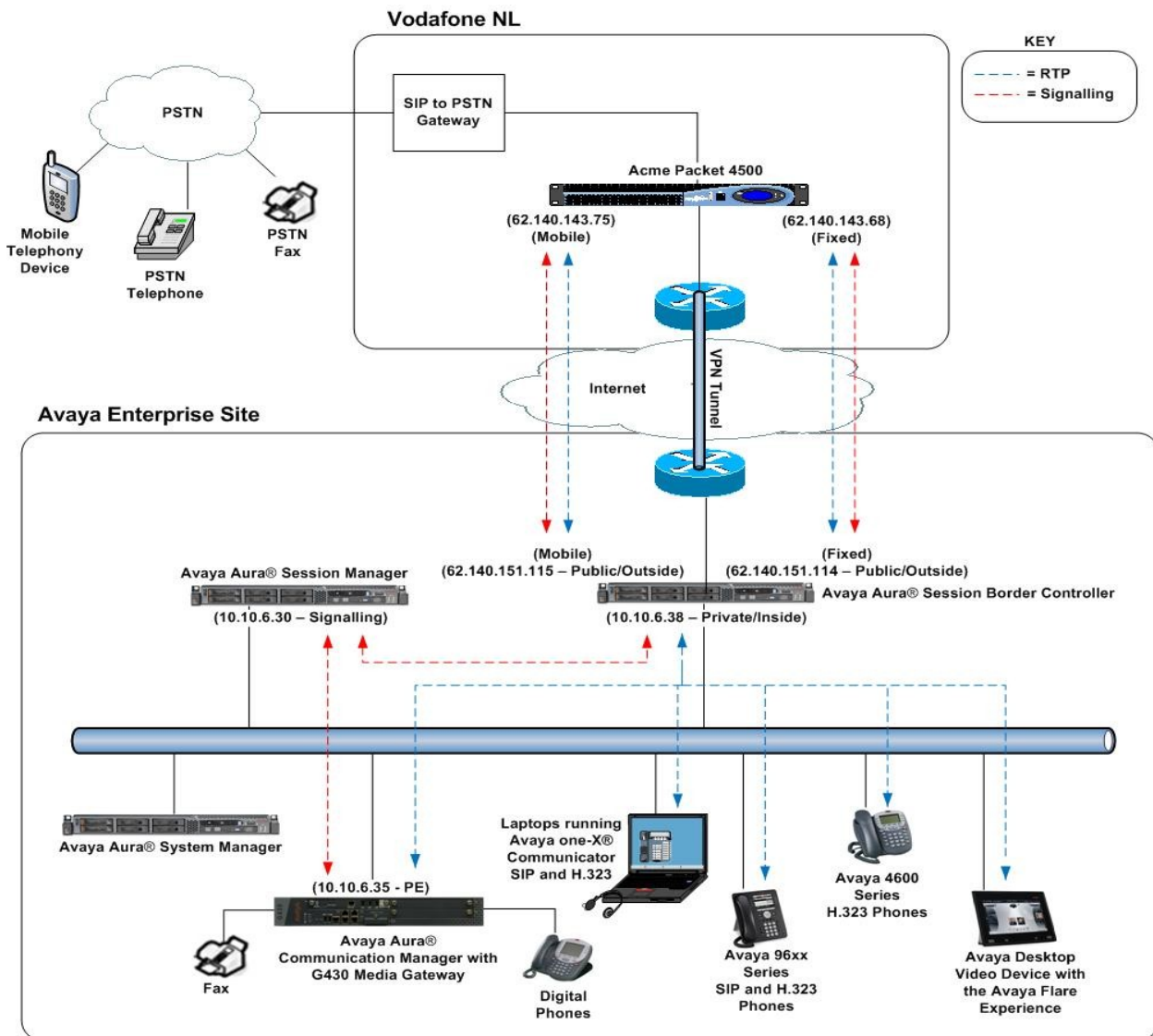
## 2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on Vodafone Netherlands SIP trunk services, contact Vodafone Netherlands support at [http://www.vodafone.nl/zakelijk/totaal\\_oplossingen/vast\\_en\\_mobiel/](http://www.vodafone.nl/zakelijk/totaal_oplossingen/vast_en_mobiel/).

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an enterprise site connected to the Vodafone Netherlands SIP Trunk Solution. The Vodafone Netherlands Office Voice connection is represented in **Figure 1** as (Fixed) and the Vodafone Netherlands OneVoice Corporate connection is represented in **Figure 1** as (Mobile). Located at the enterprise site are an AASBC, Session Manager and Communication Manager. Endpoints are Avaya 96x0 series and Avaya 96x1 series IP telephones (with SIP and H.323 firmware), Avaya 46xx series IP telephones (with H.323 firmware), one-X Communicator (SIP and H.323), Avaya Digital telephones and an Analogue fax machine. Also included in the test configuration was an Avaya Desktop Video Device incorporating the Avaya Flare experience.



**Figure 1: Avaya SIP Telephony Solution using Vodafone Netherlands Office Voice and Vodafone Netherlands OneVoice Corporate services**

## 4. Equipment and Software Validated

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

<b>Avaya</b>	
<b>Equipment</b>	<b>Software</b>
Avaya S8300 Media Server	Avaya Aura® Communication Manager R6.0.1 (R016x.00.1.510.1) Service Pack 3 (19009) (System Platform 6.0.3.1.3)
Avaya G430 Media Gateway MM712 MM711	FW 31.19.2 HW07 FW14 HW33 FW95
Avaya S8800 Media Server	Avaya Aura® Session Manager R6.1 Service Pack 3 (6.1.3.0.613006)
Avaya S8800 Media Server	Avaya Aura® System Manager R6.1 Service Pack 3 (6.1.0.0.7345-615.112) (System Platform 6.0.2.0.5)
Avaya S8800 Media Server	Avaya Aura® Session Border ControllerR 6.1 (System Platform 6.0.3.0.3, Template E362P4)
Avaya 9620 Phone (H.323)	S3.102S
Avaya 9641 Phone (H.323)	S6.010f
Avaya 4621 Phone (H.323)	2.9.2
Avaya 9620 Phone (SIP)	2.6.4
Avaya 9641 Phone (SIP)	6.1.3
Avaya Desktop Video Device, A175, Incorporating the Avaya Flare experience	1.0.2
Avaya one-X® Communicator (SIP)	Avaya one-X® Communicator 6.0.1.16-SP1-25226
Digital Phone 2410	N/A
<b>Vodafone Netherlands</b>	
Vodafone Office Voice	1.0
Vodafone OneVoice Corporate	1.0
Acme Packet 4250	SC6.1.0 MR-2 Patch 9 (Build 542)

## 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 Signaling associated with Vodafone Netherlands SIP Trunk Solution. For incoming calls, the Session Manager receives SIP messages from the AASBC 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 signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the AASBC; the AASBC then sends the SIP messages to the Vodafone Netherlands 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 Avaya S8300 Server 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 Vodafone Netherlands network, and any other SIP trunks used.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	10
Maximum Concurrently Registered IP Stations:		18000	4
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		113	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		18000	0
Maximum Video Capable IP Softphones:		0	0
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>24</b>
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	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? y
    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? n
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 signaling group between Communication Manager and Session Manager. In the **IP Node Names** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SessionMgr** and **10.10.6.30** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the processor interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
display node-names ip
                                IP NODE NAMES

  Name      IP Address
procr       10.10.6.35
SessionMgr  10.10.6.30
default     0.0.0.0
```

### 5.3. Administer IP Network Region

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

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

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1      Authoritative Domain: avaya.com
Name: Main NR
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
      Codec Set: 1      Inter-region IP-IP Direct Audio: yes
      UDP Port Min: 2048      IP Audio Hairpinning? n
      UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
      Audio PHB Value: 46
      Video PHB Value: 26
```

### 5.4. Administer IP Codec Set

Open the **IP Codec Set** form for the codec set specified in the **IP Network Region** form. Enter the list of audio codec's eligible to be used in order of preference. For the interoperability test the codec's supported by Vodafone Netherlands were configured, namely G.729 and G.711A. During compliance testing, other codec set configurations were also verified.

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

On **Page 2** of the codec set form set the **Fax Mode** to **pass-through** as shown below.

```
change ip-codec-set 1                                         Page 2 of 2
                                                                IP Codec Set
                                                                Allow Direct-IP Multimedia? n
                                                                Redundancy
FAX      Mode      pass-through      0
Modem    off      0
TDD/TTY  US      3
Clear-channel n      0
```



## 5.5. Administer SIP Signaling Groups

This signaling group (and associated trunk group) will be used for inbound and outbound PSTN calls to Vodafone Netherlands SIP Trunk Solution and will be configured using TLS (Transport Layer Security) and the default TLS port of 5061. Configure the **Signaling Group** using the **add signaling-group x** command as follows:

- Set the **Group Type** field to **sip**.
- The **Transport Method** field is set to **tls** (Transport Layer Security).
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Set the **Near-end Node Name** to the processor interface (node name **procr**). This value is taken from the **IP Node Names** form shown in **Section 5.2**.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SessionMngr**), also shown in **Section 5.2**.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.3**. This field logically establishes the **far-end** for calls using this signaling group as network region 1
- Leave the **Far-end Domain** field blank to accept any domain from the far end.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The default values for the other fields may be used.

```
add signaling-group 2
                                SIGNALING GROUP

Group Number: 2                Group Type: sip
IMS Enabled? n                 Transport Method: tls
Q-SIP? n                      SIP Enabled LSP? n
IP Video? n                   Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y     Peer Server: SM

Near-end Node Name: procr      Far-end Node Name: SessionMngr
Near-end Listen Port: 5061     Far-end Listen Port: 5061
                                Far-end Network Region: 1

Far-end Domain:

Incoming Dialog Loopbacks: eliminate
DTMF over IP: rtp-payload      Bypass If IP Threshold Exceeded? n
                                RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3
                                Direct IP-IP Audio Connections? y
                                IP Audio Hairpinning? n
                                Enable Layer 3 Test? y
                                Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n
                                Alternate Route Timer(sec): 6
```

## 5.6. Administer SIP Trunk Group

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

- Set the **Group Type** field to **sip**.
- Choose a descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **tie**.
- Specify the signaling 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: SIP TLS SM	COR: 1	TN: 1	TAC: 702
Direction: two-way	Outgoing Display? y		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: tie	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 Vodafone Netherlands to prevent unnecessary SIP messages during call setup. Also note that the value for **Redirect On OPTIM Failure** was set to **8000** to allow additional set-up time for calls destined for an EC500 destination.

add trunk-group 2		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto		Redirect On OPTIM Failure: 8000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			

On **Page 3** set the **Numbering Format** field to **public**.

add trunk-group 2		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: both	Maintenance Tests? y	
Numbering Format: public			
UUI Treatment: service-provider			
Replace Restricted Numbers? n			
Replace Unavailable Numbers? n			

On **Page 4** set the **Mark Users as Phone** to **y**, this field inserts a parameter to SIP requests indicating to any receiving SIP entity that the user part of the request URI should be treated as a telephone number. Set **Telephone Event Payload Type** to **101** the value preferred by Vodafone Netherlands. As Vodafone Netherlands do not support The P-Asserted Identity header the **Identity for Calling Party Display** field was set to **From** so that the Communication Manager will use the value in the From header for the calling party display on enterprise telephones.

add trunk-group 2	Page 4 of 21
PROTOCOL VARIATIONS	
<b>Mark Users as Phone? y</b> Prepend '+' to Calling Number? n Send Transferring Party Information? n Network Call Redirection? n Send Diversion Header? n Support Request History? n <b>Telephone Event Payload Type: 101</b>  Convert 180 to 183 for Early Media? n Always Use re-INVITE for Display Updates? n <b>Identity for Calling Party Display: From</b> Enable Q-SIP? n	

## 5.7. Administer Calling Party Number Information

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **5-digit** extension beginning with **59** will send the calling party number **+3188003xxxx** to Vodafone Netherlands SIP Trunk Solution, where **x** is the last 4 digits of the 5-digit extension. This calling party number will be sent in the SIP From and Contact headers, and displayed on display-equipped PSTN telephones.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext	Ext	Trk	CPN	Total	
Len	Code	Grp(s)	Prefix	CPN	
				Len	
5	59	2	3188003	11	Total Administered: 1
					Maximum Entries: 240

## 5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to Vodafone Netherlands SIP Trunk Service. In the sample configuration, the single digit 9 is used as the ARS access code. Avaya telephone users will dial 9 to reach an outside line. Use the **change feature-access-codes** command to configure or observe 9 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:	
Answer Back Access Code:	
Auto Alternate Routing (AAR) Access Code: 7	
<b>Auto Route Selection (ARS) - Access Code 1: 9</b>	
Access Code 2:	

Use the **change ars analysis x** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns is illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning **00** or **210**. Calls are sent to **Route Pattern 2**.

<b>change ars analysis 0</b>	Page 1 of 2
ARS DIGIT ANALYSIS TABLE	
Location: all	
Percent Full: 1	
Dialed String	Total Min Max Route Pattern Call Type Node Num ANI Req'd
00	9 11 2 pubu n
210	4 4 2 pubu n

Use the **change route-pattern x** command 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**.

<b>change route-pattern 2</b>	Page 1 of 3
Pattern Number: 2 Pattern Name: sip trk to SM6	
SCCAN? n Secure SIP? n	
<b>Grp</b>	DCS/ IXC
<b>No</b>	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	none
2: y y y y y n n rest	none

## 5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from Vodafone Netherlands can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by Vodafone Netherlands correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers +3188003xxxx to a 5 digit extension by deleting 8 of the incoming digits and inserting a 5 to create a valid extension.

change inc-call-handling-trmt trunk-group 2				Page	1 of	3
INCOMING CALL HANDLING TREATMENT						
Service/	Number	Number	Del	Insert		
Feature	Len	Digits				
tie	12	+3188003	8	5		

## 5.10. EC500 Configuration

When EC500 is enabled on the Communication Manager station, a call to that station will generate a new outbound call from Communication Manager to the configured EC500 destination, typically a mobile phone. The following screen shows an example EC500 configuration for the user with station extension 59022. Use the command **change off-pbx-telephone station mapping x** where **x** is the Communication Manager station.

- The **Station Extension** field will automatically populate
- For **Application** enter **EC500**
- Enter a **Dial Prefix** (e.g., 9) if required by the routing configuration
- For the **Phone Number** field enter the phone that will also be called (e.g., **00353861111111**)
- Set the **Trunk Selection** to **ars** so that the ARS tables will be used to determine how Communication Manager will route to the Phone Number destination.
- Set the **Config Set** to **1**
- Other parameters can retain default value

change off-pbx-telephone station-mapping 59022							Page	1 of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station	Application	Dial	CC	Phone Number	Trunk	Config	Dual		
Extension		Prefix			Selection	Set	Mode		
59022	EC500	-		00353861111111	ars	1			
		-							
		-							

## 5.11. ACD Call Routing

The general configuration of the Communication Manager ACD including skill groups and ACD agents is outside the scope of these application notes and presumed to have been previously completed and is not discussed here. The focus of this section is the configuration of the call vector used during testing to route ACD voice calls. To add a new ACD call flow use the command **change vector x** where **x** is an available vector. To ensure that calls received by the vector illustrated in the screen below are answered by Communication Manager, the vector use's an announcement at the beginning of the vector to answer the incoming call (see **Section 2.2**) and then queues to **skill 1** where skill 1 is a hunt group staffed by ACD agents.

```
change vector 45                                     Page 1 of 6
                                     CALL VECTOR
      Number: 45                                Name: test queue
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
      Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
      Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
      Variables? y      3.0 Enhanced? y
01 announcement 1500
02 queue-to      skill 1      pri m
03 wait-time      60      mins hearing ringback
04 goto step      3                        if unconditionally
05 stop
06
```

Save Communication Manager changes by entering the command **save translations** to make them permanent.

## 6. Configuring Avaya Aura® Session Manager

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

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

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

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

**AVAYA** Avaya Aura™ System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Users	Elements	Services
<b>Administrators</b> Manage Administrative Users	<b>Application Management</b> Manage applications and application certificates	<b>Backup and Restore</b> Backup and restore System Manager database
<b>Groups &amp; Roles</b> Manage groups, roles and assign roles to users	<b>Communication Manager</b> Manage Communication Manager objects	<b>Configurations</b> Manage system wide configurations
<b>Subscribers</b> Manage users and shared resources associated with CS1000, including LDAP/file import and export	<b>Conferencing</b> Conferencing	<b>Events</b> Manage alarms, view and harvest logs
<b>Synchronize and Import</b> Synchronize users with the enterprise directory, import users from file	<b>Inventory</b> Manage, discover, and navigate to elements, update element software	<b>Licenses</b> View and configure licenses
<b>UCM Roles</b> Manage UCM Roles, assign roles to users	<b>Messaging</b> Manage Messaging System objects	<b>Replication</b> Track data replication nodes, repair replication nodes
<b>User Management</b> Manage users, shared user resources and provision users	<b>Presence</b> Presence	<b>Scheduler</b> Schedule, track, cancel, update and delete jobs
	<b>Routing</b> Network Routing Policy	<b>Security</b> Manage Security Certificates
	<b>SIP AS 8.1</b> SIP AS 8.1	<b>Templates</b> Manage Templates for Communication Manager and Messaging System objects
	<b>Session Manager</b> Session Manager Element Manager	<b>UCM Services</b> Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

## 6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu (not shown) 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 (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes (Not shown). The screen below shows the SIP domain that was previously configured.

**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

**Routing** x **Home**

**Home / Elements / Routing / Domains - Domain Management**

**Domain Management** [Help ?](#)

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

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

Select : All, None



## 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. Under **General**, in the **Name** field enter an informative name for the location and optionally a description for the location in the **Notes** field. 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 simulated enterprise.

**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) [Home](#)

**Routing** **Home / Elements / Routing / Locations - Location Details**

**Location Details** [Help ?](#) [Commit](#) [Cancel](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.  
See Session Manager -> Session Manager Administration -> Global Setting

**General**

\* **Name:**   
**Notes:**

**Overall Managed Bandwidth**

**Managed Bandwidth Units:**   
**Total Bandwidth:**

**Per-Call Bandwidth Parameters**

\* **Default Audio Bandwidth:**

**Location Pattern**

[Add](#) [Remove](#)

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*10.10.6.*	

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 the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following fields will need to be populated 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 signaling 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 **Gateway** for the AASBC SIP entity.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Session Border Controller SIP Entity

### 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 signaling interface.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

\* Name: sesmgr02

\* FQDN or IP Address: 10.10.6.30

Type: Session Manager

Notes:

Location: Enterprise

Outbound Proxy:

Time Zone: Etc/GMT

Credential name:

SIP Link Monitoring: Use Session Manager Configuration

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

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

Port

Add Remove

3 Items Refresh

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

Select: All, None

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

The following screens show the SIP entity for Communication Manager which is configured as an Evolution Server. The **FQDN or IP Address** field is set to the IP address of the interface on Communication Manager that will be providing SIP signaling (see **Figure 1**).

The screenshot displays the Avaya Aura® System Manager 6.1 interface. The left sidebar shows a navigation menu with 'Routing' selected. The main content area is titled 'SIP Entity Details' and 'General'. The 'Name' field is 'EvolutionSvr'. The 'FQDN or IP Address' field is '10.10.6.35'. The 'Type' is 'CM'. The 'Location' is 'Enterprise' and the 'Time Zone' is 'Etc/GMT'. The 'SIP Timer B/F (in seconds)' is '4'. The 'Call Detail Recording' is 'none'. The 'SIP Link Monitoring' is 'Use Session Manager Configuration'. The 'Override Port & Transport with DNS SRV' checkbox is unchecked.

### 6.4.3. Avaya Aura® Session Border Controller SIP Entity

The following screen shows the SIP Entity for the AASBC. The **FQDN or IP Address** field is set to the IP address of the AASBC private network interface (see **Figure 1**).

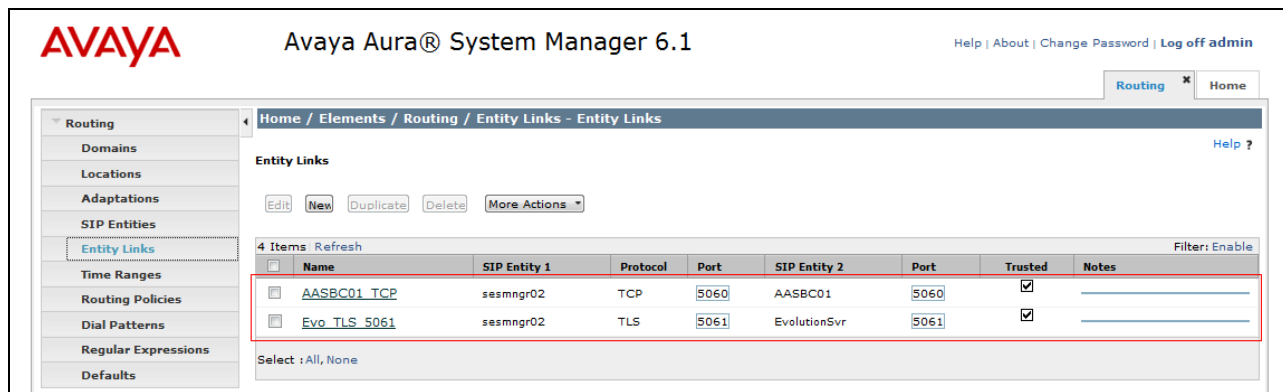
The screenshot displays the Avaya Aura® System Manager 6.1 interface. The left sidebar shows a navigation menu with 'Routing' selected. The main content area is titled 'SIP Entity Details' and 'General'. The 'Name' field is 'AASBC01'. The 'FQDN or IP Address' field is '10.10.6.38'. The 'Type' is 'Gateway'. The 'Location' is 'Enterprise' and the 'Time Zone' is 'Etc/GMT'. The 'SIP Timer B/F (in seconds)' is '4'. The 'Call Detail Recording' is 'none'. The 'SIP Link Monitoring' is 'Use Session Manager Configuration'. The 'Override Port & Transport with DNS SRV' checkbox is unchecked.

## 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 and in the resulting screen 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 the SIP Entity for SessionManager i.e. **sesmgr02**.
- 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.

Click **Commit** to save changes (not shown). The following screen shows the Entity Links used in this configuration.



The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "Entity Links" and includes a breadcrumb trail: Home / Elements / Routing / Entity Links - Entity Links. Below the title are buttons for Edit, New, Duplicate, Delete, and More Actions. A table displays 4 items, with a "Filter: Enable" option. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. Two rows are highlighted with a red border:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
AASBC01 TCP	sesmgr02	TCP	5060	AASBC01	5060	<input checked="" type="checkbox"/>	
Evo TLS 5061	sesmgr02	TLS	5061	EvolutionSvr	5061	<input checked="" type="checkbox"/>	

Below the table, there is a "Select : All, None" option.

## 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 Communication Manager

The screenshot displays the Avaya Aura System Manager 6.1 interface. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes a breadcrumb trail: 'Home / Elements / Routing / Routing Policies - Routing Policy Details'. The 'General' tab is active, showing the 'Name' field with the value 'CallsToEvolutionSvr', a 'Disabled' checkbox, and a 'Notes' field with the text 'Calls to the Communication Mngr'. The 'SIP Entity as Destination' section has a 'Select' button. Below this is a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one entry: 'EvolutionSvr' with IP '10.10.6.35', Type 'CM', and Notes 'calls going to CM'. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. A table below shows a single time range entry: '24/7' with a ranking of '0', start time '00:00', end time '23:59', and notes 'Time Range 24/7'. The table has columns for days of the week (Mon-Sun) and checkboxes for each day, all of which are checked. The bottom of the 'Time of Day' section has a 'Select' dropdown set to 'All, None'.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing × Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Help ? Commit Cancel

General

\* Name: CallsToEvolutionSvr

Disabled: ☐

Notes: Calls to the Communication Mngr

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
EvolutionSvr	10.10.6.35	CM	calls going to CM

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

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

Select : All, None

The following screen shows the routing policy for the AASBC

**AVAYA**

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Help ?

Commit

Cancel

General

\* Name: CallsToSBC

Disabled: ☐

Notes: Calls routing to swisscom

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AASBC01	10.10.6.38	Gateway	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item Refresh

Filter: Enable

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

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 dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select **-ALL-** to allow calls from any domain to match the dial pattern

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown), under **Originating Location** select **ALL** and 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 AASBC which will route the calls out to the Vodafone Netherlands SIP Trunk Solution.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Dial Patterns - Dial Pattern Details'. It features a 'Dial Pattern Details' section with a 'General' tab. The 'General' tab includes fields for 'Pattern' (set to '+316'), 'Min' (set to '4'), and 'Max' (set to '36'). Below these are checkboxes for 'Emergency Call' and a dropdown for 'SIP Domain' (set to '-ALL-'). A 'Notes' field is also present. The 'Originating Locations and Routing Policies' section includes an 'Add' button and a table with one item. The table has columns: 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The single row shows '-ALL-' as the location, 'Any Locations' as notes, 'CallsToSBC' as the policy, rank '0', 'Routing Policy Disabled' as unchecked, 'AASBC01' as the destination, and an empty notes field. A 'Select : All, None' button is at the bottom of the table.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-	Any Locations	CallsToSBC	0	<input type="checkbox"/>	AASBC01	



The following screen shows an example dial pattern configured for Communication Manager.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

\* Pattern: +3188003902

\* Min: 11

\* Max: 36

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Calls to CM EVO

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-	Any Locations	CallsToEvolutionSvr	0	<input checked="" type="checkbox"/>	EvolutionSvr	Calls to the Communication Mngr

Select : All, None

## 6.8. Administer Avaya Aura® Communication Manager as a Managed Element

From the Home tab select Inventory from the menu. In the resulting tab from the left panel menu select **Manage Elements** and click **New** (not shown). On the **Application** tab, enter values in the following fields and use defaults for the remaining fields:

- In the **Name** field enter a descriptive name i.e. **EvolutionSvr**
- In the **Type** field select **CM** from the drop-down menu
- In the **Node** enter the IP address of the Communication Manager

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Inventory x Home

Home / Elements / Inventory / Manage Elements - View CM

View CM: EvolutionSvr

Application \* Attributes \*

Application

Name: EvolutionSvr

Type: CM

Description: 10.10.6.35

On the **Attributes** tab, under the **Attributes** heading, enter values in the following fields and use defaults for the remaining fields:

- In the **Login** field enter a login name for Communication Manager (SAT SSH login)
- In the **Password** field enter Password for Communication Manager (SAT SSH password)
- Select the **Is SSH Connection** check box if SSH is to be used
- In the **Port** field enter the port number to use for SAT access

Select **Commit**, this causes System Manager to synchronize with the Communication Manager in the background.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Inventory x Home

Home / Elements / Inventory / Manage Elements - View CM

View CM: EvolutionSvr

Application \* Attributes \*

SNMP Attributes

Version None V1 V3

Attributes

Login sysmgr02

Password \*\*\*\*\*

Is SSH Connection ☒

Port 5022

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

From the Home tab select Session Manager from the menu. In the resulting tab from the left panel menu select **Application Configuration → Applications** and click **New**

- In the **Name** field enter a name for the application
- In the **SIP Entity** field select the SIP entity for the Communication Manager i.e. **EvolutionSvr**
- In the **CM System for SIP Entity** field select the SIP entity for the Communication Manager

Select **Commit** to save the configuration.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

Home / Elements / Session Manager / Application Configuration / Applications - Applications

Application Editor

Application

\*Name CM\_Evo\_App

\*SIP Entity EvolutionSvr

\*CM System for SIP Entity EvolutionSvr Refresh View/Add CM Systems

Description

Commit Cancel

## 6.10. Administer Application Sequence for Communication Manager

From the left panel navigate to **Session Manager** → **Application Configuration** → **Application Sequences** and click on **New**.

- 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** to save the configuration.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, Applications, Application Sequences, Implicit Users, NRS Proxy Users, System Status, and System Tools. The main content area is titled 'Application Sequence Editor' and includes a breadcrumb trail: Home / Elements / Session Manager / Application Configuration / Application Sequences - Application Sequences. The 'Application Sequence' section has a 'Name' field containing 'CM\_Evo\_AppSeq' and a 'Description' field. Below this is the 'Applications in this Sequence' section, which includes buttons for 'Move First', 'Move Last', and 'Remove'. A table lists the applications in the sequence, with one item: 'CM\_Evo\_App' (Sequence Order 1, SIP Entity EvolutionSvr, Mandatory checked). The 'Available Applications' section at the bottom shows a table with one item: 'CM\_Evo\_App' (SIP Entity EvolutionSvr). The interface also includes 'Commit' and 'Cancel' buttons at the top right of the editor area.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Home

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

Help ?

### Application Sequence Editor

Commit Cancel

#### Application Sequence

\*Name

Description

#### Applications in this Sequence

Move First Move Last Remove

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

Select : All, None

#### Available Applications

1 Item Refresh Filter: Enable

Name	SIP Entity	Description
CM_Evo_App	EvolutionSvr	

## 6.11. Administer SIP Extensions

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

On the **Identity** tab:

- Enter the user's name in the **Last Name** and **First Name** fields
- In the **Login Name** field enter a unique system login name in the form of user@domain (e.g. **59027@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

**AVAYA** Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[User Management](#) \* [Home](#)

Home / Users / User Management / Manage Users - New User Profile [Help ?](#)

**New User Profile** [Commit](#) [Cancel](#)

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

**Identity** ▾

\* **Last Name:**

\* **First Name:**

**Middle Name:**

**Description:**

\* **Login Name:**

\* **Authentication Type:**  ▾

\* **Password:**

\* **Confirm Password:**

**Localized Display Name:**

On the **Communication Profile** tab enter a numeric **Communication Profile Password** and confirm it, then click on the show/hide button for **Communication Address** and click **New**. For the **Type** field select **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.

Identity \*

Communication Profile \*

Membership

Contacts

Communication Profile ▾

Communication Profile Password: .....

Confirm Password: .....

New

Delete

Done

Cancel

Name
Primary

Select : None

\* Name: Primary

Default : ☒

Communication Address ▾

New

Edit

Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP ▾

\* Fully Qualified Address: 59027 @ avaya.com ▾

Add

Cancel

Click the show/hide button next to **Session Manager Profile**:

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

☒ **Session Manager Profile** ▼

\* **Primary Session Manager**

sesmgr02 ▼

Primary	Secondary	Maximum
7	0	7

**Secondary Session Manager**

(None) ▼

Primary	Secondary	Maximum

**Origination Application Sequence**

CM\_Evo\_AppSeq ▼

**Termination Application Sequence**

CM\_Evo\_AppSeq ▼

**Survivability Server**

(None) ▼

\* **Home Location**

Enterprise ▼

Click the show/hide button next to **Endpoint Profile**.

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

The screenshot shows the 'Endpoint Profile' configuration form. At the top, there is a section header 'Endpoint Profile' with a checkmark and a dropdown arrow. Below this, the form contains several fields and options:

- \* System:** A dropdown menu with 'EvolutionSvr' selected.
- \* Profile Type:** A dropdown menu with 'Endpoint' selected.
- Use Existing Endpoints:** A checkbox that is currently unchecked.
- \* Extension:** A text input field containing '59027' and a magnifying glass icon. To its right is a button labeled 'Endpoint Editor'.
- \* Template:** A dropdown menu with 'DEFAULT\_9640SIP\_CM\_6\_0' selected.
- Set Type:** A text input field containing '9640SIP'.
- Security Code:** A text input field containing six dots '.....'.
- \* Port:** A text input field containing 'IP' and a magnifying glass icon.
- Voice Mail Number:** An empty text input field.
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:** A checkbox that is checked, located within a red-bordered box.

## 7. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the AASBC. This configuration is done in two parts. The first part is done during the AASBC installation via the installation wizard. These Application Notes will not cover the AASBC installation in its entirety but will include the use of the installation wizard. For information on installing the System Platform and the loading of the AASBC template see [1] & [2]. The second part of the configuration is done after the installation is complete using the AASBC web interface.

### 7.1. Installation Wizard

During the installation of the AASBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the AASBC. The first screen of the installation wizard is the Network Settings screen. Fill in the fields as described below and shown in the following screen:

- In the **IP Address** field enter the IP address of the private side of the AASBC
- In the **Hostname** field enter a host name for the AASBC
- Specify a domain in the **Domain** and **Default Domain** fields

Click **Next Step** (not shown) to continue

The screenshot displays the Avaya Aura Session Border Controller (AASBC) Network Settings configuration screen. The interface includes a sidebar with navigation options and a main content area for network settings.

**AVAYA**

**Home**

**Configuration**

- Installation
  - Load
  - Network Settings
  - Logins
  - VPN Access
  - SBC
  - Summary
  - Save

**Network Settings**

Enter network settings

Domain-0 IP Address: 10.10.6.36

CDom IP Address: 10.10.6.37

Gateway IP Address: 10.10.6.1

Network Mask: 255.255.255.0

Primary DNS: 10.10.6.10

Secondary DNS (Optional):

Default Search List (Optional):

HTTPS Proxy (Optional) [IP Address:Port Number]:

Virtual Machine	IP Address	Hostname	Domain
SBC	10.10.6.38	AASBC01Vlan6	avaya.com (Optional)

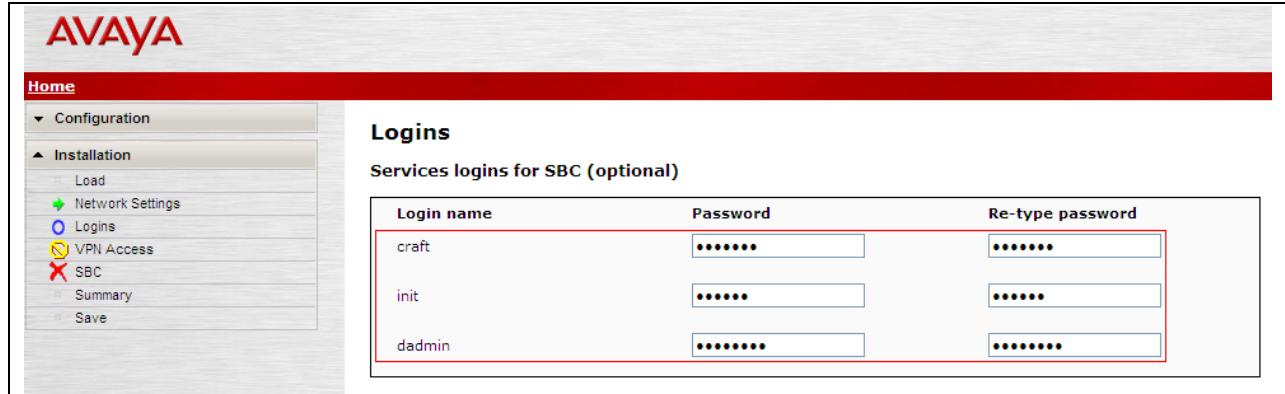
**Default Domain**

avaya.com (Optional)

Apply to all VMs

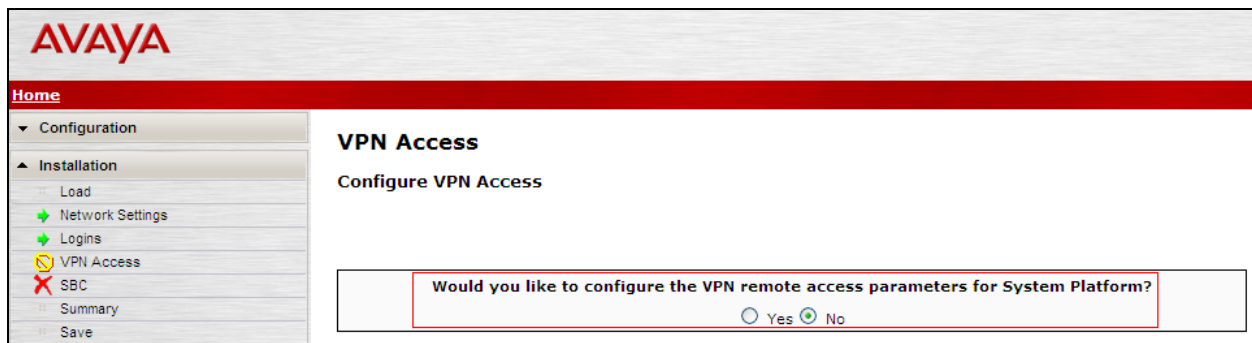


From the **Logins** screen specify passwords for the services logins to the AASBC



Login name	Password	Re-type password
craft	.....	.....
init	.....	.....
dadmin	.....	.....

VPN remote access to the AASBC was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?**



Would you like to configure the VPN remote access parameters for System Platform?

☐ Yes ☒ No

On the **SBC** screen, in the **SIP Service Provider Data** section fill in the fields as described below and shown in the following screen:

- In the **Service Provider** select the name of the Service Provider to which the AASBC will connect. This will allow the wizard to select a configuration file customized for this Service Provider. At the time of the compliance test, a customized configuration file did not exist for Vodafone Netherlands. Thus, **Generic** was chosen
- In the **Port** field enter the port number that Vodafone Netherlands uses to listen for SIP traffic
- In the **IP Address1** field enter the IP addresses provided by Vodafone Netherlands for the Vodafone Office Voice SIP Trunk Service (fixed). The IP address for the Vodafone OneVoice Corporate SIP Trunk Service (mobile) used during testing will be added after the AASBC template is installed (**Section 7.3**)
- In the **Signaling/Media Network1** field enter the Vodafone Netherlands provided subnet where media traffic will originate. An additional subnet can be provided for **Signaling/Media Network2**
- In the **Media Netmask** field enter the netmask corresponding to the Media Network
- Scroll down to continue

The screenshot shows the Avaya SBC configuration interface. On the left is a navigation menu with options: Home, Configuration, Installation, Load, Network Settings, Logins, VPN Access, SBC (selected), Summary, and Save. The main area is titled 'SBC' and 'Session Border Controller Data'. A sub-section titled 'SIP Service Provider Data' contains the following fields:

Service Provider	Port	IP Address1	Signalling/Media Network1	Signalling/Media Netmask1	IP Address2 (Optional)	Signalling/Media Network2 (Optional)	Signalling/Media Netmask2 (Optional)	Hunting (Optional)
Generic	5060	62.140.143.68	62.140.143.0	255.255.255.0				

Further down on the same **SBC** screen, in the **SBC Network Data** section fill in the fields as described below:

- In the **Public IP Address** field enter the enterprise IP address that will be used for the Vodafone Netherlands Office Voice SIP Trunk Service on the public side of the AASBC
- In the **Public Net Mask** field enter the netmask associated with the public network to which the AASBC connects
- In the **Public Gateway** field enter the default gateway of the public network

In the **Enterprise SIP Server** section fill in the fields as described below:

- In the **SIP Domain** field enter the enterprise SIP domain
- In the **IP Address** field enter the IP address of the Enterprise SIP Server to which the AASBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface
- In the **Transport1** field select the transport protocol to be used for SIP traffic between the AASBC and Session Manager

Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to install the template with the values entered.

SBC Network Data			
Interface	IP Address	Net Mask	Gateway
Private (Management)	10.10.6.38	255.255.255.0	10.10.6.1
Public	62.140.151.114	255.255.255.240	62.140.151.113

Enterprise SIP Server		
<b>SIP Domain</b> avaya.com		
<b>IP Address1</b> 10.10.6.30	<b>Transport1</b> TCP	
<b>IP Address2 (Optional)</b> 	<b>Transport2 (Optional)</b> 	<b>Hunting (Optional)</b> 

## 7.2. Access Avaya Aura® Session Border Controller

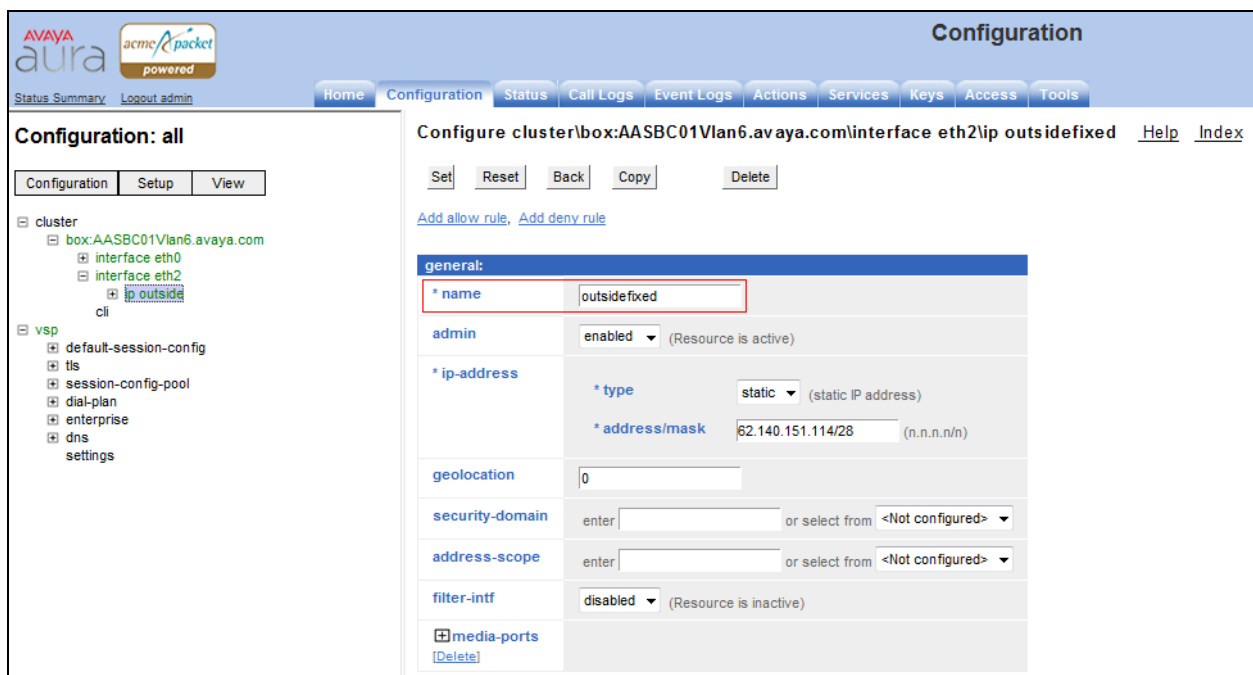
Access the AASBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 7.1**. Log in with the appropriate credentials.



The image shows a login page for 'Acme Packet Net-Net OS-E'. The title is 'Acme Packet Net-Net OS-E'. Below the title, it says 'To access the NNOS-E management interface, you must first log in. Please provide your user name and password.' There are two input fields: 'Username:' and 'Password:'. Below the 'Password:' field is a 'Login' button.

## 7.3. Configure Outside Interfaces

To allow two logical connections to be created between the enterprise and Vodafone Netherlands an additional IP address is created on the outside interface of the AASBC. Rename the IP address configuration created in **Section 7.1** by expanding **cluster** → **box:AASBC01Vlan6.avaya.com** → **interface eth2** → **ip outside** and enter a descriptive name in the **name** field. The name **outsidefixed** is used as this is the IP address that will be used for the Vodafone Office Voice SIP Trunk Service. Scroll down to continue.



The image shows the Avaya Aura Configuration page. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows the configuration tree with 'cluster' expanded, showing 'box:AASBC01Vlan6.avaya.com' and 'interface eth2'. The main content area is titled 'Configure cluster\box:AASBC01Vlan6.avaya.com\interface eth2\ip outsidefixed'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Add allow rule' and 'Add deny rule'. The configuration fields are as follows:

general:	
* name	outsidefixed
admin	enabled (Resource is active)
* ip-address	
* type	static (static IP address)
* address/mask	62.140.151.114/28 (n.n.n.n/n)
geolocation	0
security-domain	enter or select from <Not configured>
address-scope	enter or select from <Not configured>
filter-intf	disabled (Resource is inactive)
media-ports	[Delete]

Further down on the same screen in the **routing** section click the edit link relating to the **route external-sip-media-1** route.

<a href="#">+routing</a> <a href="#">[Delete]</a>	<b>route</b>					
	<a href="#">Edit</a> <a href="#">Delete</a>	route	admin	destination	gateway	metric
	<a href="#">Edit</a> <a href="#">Delete</a>	route Default	disabled	default	0.0.0.0	1
	<a href="#">Edit</a> <a href="#">Delete</a>	route external-sip-media-1	enabled	network 62.140.143.0/24	62.140.151.113	1
<a href="#">Add route</a>						

In the resulting screen in the **destination** section, select **host** from the **type** drop down menu. In the **address** field enter the IP address of the Vodafone Netherlands Office Voice SIP trunk service.

Configure cluster|box:AASBC01Vlan6.avaya.com|interface eth2|ip outside|fixed|routing|route external-sip-media-1
[Help](#) [Index](#)

Set Reset Back Copy Delete

**admin**
enabled (Resource is active)

**\* route-name**
external-sip-media-1

**\* destination**

**\* type**
host (host route)

**\* address**
62.140.143.68 (n.n.n.n)

**\* gateway**
62.140.151.113 (n.n.n.n)

**metric**
1 (from 0 to 1,000,default=1)

Set Reset Back Copy

To create another IP address configuration navigate to **box:AASBC01Vlan6.avaya.com** → **interface eth2** → **ip outsidefixed** and click **copy** (Not shown). In the resulting screen update the fields as shown below:

- In the **name** field enter a descriptive name. The name **outsidemobile** is used as this is the IP address that will be used for the Vodafone OneVoice Corporate SIP Trunk Service. Scroll down to continue.
- In the **address/mask** field enter the IP address that will be used on the public side of the AASBC for the Vodafone OneVoice Corporate SIP Trunk Service.

Scroll down to continue.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows a tree view with 'cluster' expanded, showing 'box:AASBC01Vlan6.avaya.com' and its interfaces. The main area is titled 'Configure cluster: box:AASBC01Vlan6.avaya.com / interface eth2 / ip outsidemobile'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Add allow rule' and 'Add deny rule'. The 'general' tab is active, showing fields for 'name' (outsidemobile), 'admin' (enabled), 'ip-address' (static, 62.140.151.115/28), 'geolocation' (0), 'security-domain' (enter or select from <Not configured>), 'address-scope' (enter or select from <Not configured>), and 'filter-intf' (disabled).

Further down on the same screen in the **routing** section click the edit link relating to the **route external-sip-media-1** route.

The screenshot shows the 'routing' section with a table of routes. The table has columns: route, admin, destination, gateway, and metric. Two routes are listed: 'route Default' (disabled, default, 0.0.0.0, 1) and 'route external-sip-media-1' (enabled, network 62.140.143.0/24, 62.140.151.113, 1). The 'route external-sip-media-1' row is highlighted with a red box.

route	admin	destination	gateway	metric
<a href="#">Edit</a> <a href="#">Delete</a> route Default	disabled	default	0.0.0.0	1
<a href="#">Edit</a> <a href="#">Delete</a> route external-sip-media-1	enabled	network 62.140.143.0/24	62.140.151.113	1

In the resulting screen in the **destination** section, select **host** from the drop down menu for **type**. In the **address** field enter the IP address of the Vodafone Netherlands OneVoice Corporate SIP trunk service.

Configure cluster\box:AASBC01Vlan6.avaya.com\interface eth2\ip outsidemobile\routing\route external-sip-media-1

[Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Copy](#) [Delete](#)

<b>admin</b>	enabled <input type="button" value="v"/> (Resource is active)
<b>* route-name</b>	external-sip-media-1
<b>* destination</b>	<div> <b>* type</b> <input type="button" value="v"/> host (host route)         </div> <div> <b>* address</b> <input type="text" value="62.140.143.75"/> (n.n.n.n)         </div>
<b>* gateway</b>	<input type="text" value="62.140.151.113"/> (n.n.n.n)
<b>metric</b>	<input type="text" value="1"/> (from 0 to 1,000,default=1)

[Set](#) [Reset](#) [Back](#) [Copy](#)

## 7.4. Session Config Pool

Navigate to **vsp** → **session-config-pool** → **entry ToTelco** and extend the entry in the **name** field to **ToTelcoFixed**.

AVAYA aura acme & packet powered

Status Summary Logout admin

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configuration: all

[Configuration](#) [Setup](#) [View](#)

cluster

- box:AASBC01Vlan6.avaya.com
  - interface eth0
  - interface eth2
    - ip outsidefixed
    - ip outsidemobile
  - cli

vsp

- default-session-config
- tls
- session-config-pool
  - entry ToTelco
  - entry ToPBX
  - entry Discard

Configure vsp\session-config-pool\entry ToTelco [Show advanced](#) [Help](#) [Index](#)

[Set](#) [Reset](#) [Back](#) [Copy](#) [Delete](#)

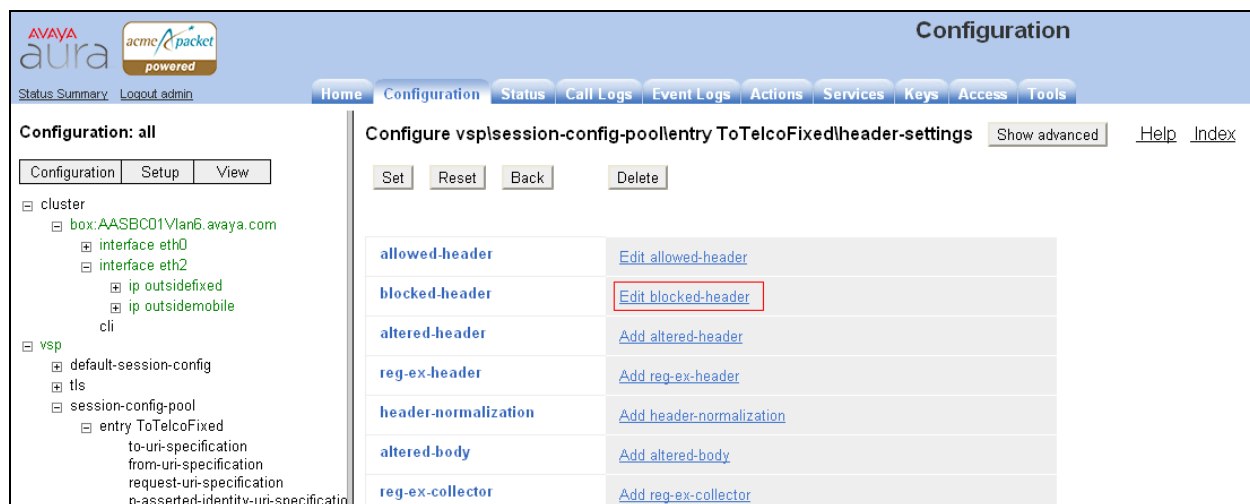
[Set QoS](#)

basic:

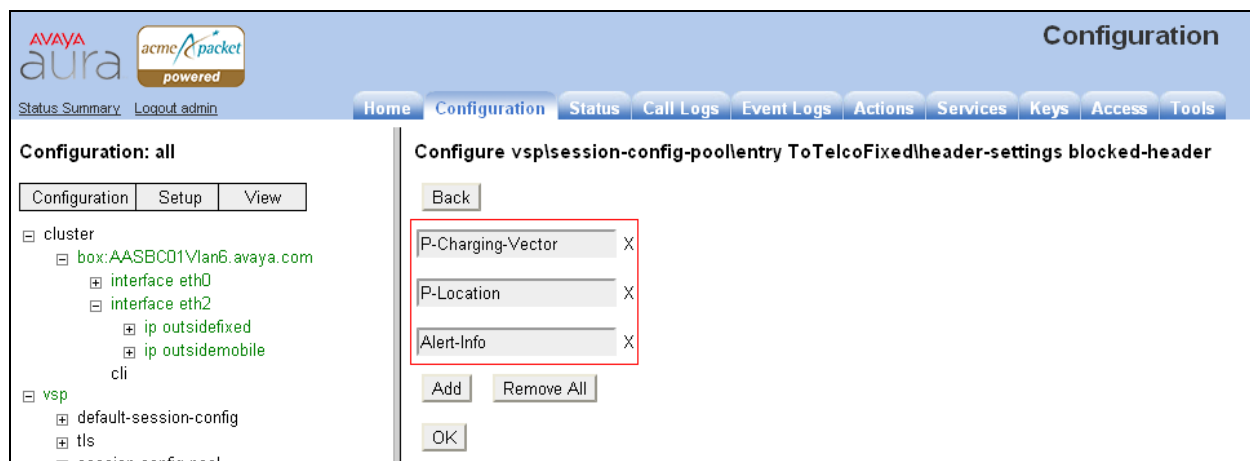
sip-directive	<a href="#">Configure</a>
sip-settings	<a href="#">Configure</a>
log-alert	<a href="#">Configure</a>
registration	<a href="#">Configure</a>
<b>* name</b>	<input type="text" value="ToTelcoFixed"/>

### 7.4.1. Stripping SIP Headers

The AASBC can be used to strip SIP headers to prevent the header from being sent to the public SIP Service Provider. To strip a SIP header navigate to **vsp** → **session-config-pool** → **entry ToTelco** → **header-settings** and click on the **Edit blocked-header** link.



In the resulting page click the **Add** button to open a new entry field and enter the name of the header to be removed, repeat this action for all the headers to be removed. Click the **OK** button when finished.





The following screen shows the headers being stripped during testing.

The screenshot shows the AVAYA aura configuration interface. The left sidebar displays a tree view of the configuration hierarchy: cluster > box:AASBC01Vlan6.avaya.com > interface eth0 > interface eth2 > ip outsidefixed > ip outsidemobile > cli. The main content area is titled 'Configure vspsession-config-poolentry ToTelcoFixedheader-settings'. It features a table with three rows: 'allowed-header', 'blocked-header', and 'altered-header'. The 'blocked-header' row is highlighted with a red box, and its value is 'P-Charging-Vector', 'P-Location', and 'Alert-Info'. The 'allowed-header' row is empty, and the 'altered-header' row is also empty. The 'blocked-header' row has a red box around it, and the 'allowed-header' row has a red box around it. The 'altered-header' row has a red box around it.

Navigate to **vsp** → **session-config-pool** → **entry ToTelco** → **from-uri-specification** and enter the IP address used on the public side of the AASBC for the Vodafone Netherlands Office Voice SIP trunk into the first host field. This will ensure that the host part of the From header is always set as the entered IP address. Click **Set** to save changes.

The screenshot shows the AVAYA aura configuration interface. The left sidebar displays a tree view of the configuration hierarchy: cluster > box:AASBC01Vlan6.avaya.com > interface eth0 > interface eth2 > ip outsidefixed > ip outsidemobile > cli. The main content area is titled 'Configure vspsession-config-poolentry ToTelcofrom-uri-specification'. It features a table with four rows: 'user', 'host', 'port', and 'display'. The 'host' row is highlighted with a red box, and its value is '62.140.143.114'. The 'user' row is empty, the 'port' row is empty, and the 'display' row is empty. The 'user-agent-aware-display-' row is also empty.

Navigate to **vsp** → **session-config-pool** → **entry ToTelco** and click **Copy** (not shown). This will produce an exact copy of the session config including the stripped SIP headers. In the resulting screen alter the entry in the **name** field to **ToTelcomobile**.

Configuration: all

Configuration Setup View

cluster

- box:AASBC01Vlan6.avaya.com
  - interface eth0
  - interface eth2
    - ip outsidefixed
    - ip outsidemobile
  - cli
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelcoFixed
    - entry ToPBX
    - entry Discard
    - entry ToTelcoMobile

Configure vspsession-config-poolentry ToTelcoMobile Show advanced Help Index

Set Reset Back Copy Delete

Set QoS

basic:

sip-directive Configure

sip-settings Configure

log-alert Configure

registration Configure

\* name ToTelcoMobile

Navigate to **vsp** → **session-config-pool** → **entry ToTelcomobile** → **from-uri-specification** and enter the IP address used on the public side of the AASBC for the Vodafone Netherlands OneVoice Corporate SIP trunk into the first **host** field. This will ensure that the host part of the From header is always set as the entered IP address. Click **Set** to save changes.

Configuration: all

Configuration Setup View

cluster

- box:AASBC01Vlan6.avaya.com
  - interface eth0
  - interface eth2
    - ip outsidefixed
    - ip outsidemobile
  - cli
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelcoFixed
    - entry ToPBX
    - entry Discard
    - entry ToTelcoMobile
      - to-uri-specification

Configure vspsession-config-poolentry ToTelcoMobilefrom-uri-specification Help Index

Set Reset Back Delete

user enter from-uri or select from from-uri (Net-Net OS-E uses the value from the incoming FROM URI.)

host enter 62.140.143.115 or select from 62.140.143.115

port enter from-uri or select from from-uri (Net-Net OS-E uses the value from the incoming FROM URI.)

display enter from-uri or select from from-uri (Net-Net OS-E uses the value from the incoming FROM URI.)

user-agent-aware-display disabled (Resource is inactive)

## 7.5. SIP Servers

Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway Telco** and alter the entry in the **name** field to **Telcofixed**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows a tree view with 'cluster' expanded, showing 'box:AASBC01Vlan6.avaya.com', 'vsp', 'default-session-config', 'tls', 'session-config-pool', 'dial-plan', 'enterprise', 'servers', 'dns', and 'settings'. Under 'servers', 'sip-gateway Telco' is selected. The main panel is titled 'Configure vspenterprise\servers\sip-gateway Telco'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from:" URI', and 'Change "to:" URI'. The 'general' section has a red box around the 'name' field, which contains 'Telcofixed'. Other fields include 'admin' (enabled), 'domain' (empty), and 'failover-detection' (ping).

Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway Telcofixed** and click **Copy** (Not shown). In the resulting screen alter the entry in the **name** field to **Telcomobile**. In the **outbound-session-config-pool-entry** field select the **ToTelcomobile** session config created in **Section 7.4** from the drop down menu. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface for 'sip-gateway Telcomobile'. The left sidebar is the same as the previous screenshot, but 'sip-gateway Telcomobile' is now selected under 'servers'. The main panel is titled 'Configure vspenterprise\servers\sip-gateway Telcomobile'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from:" URI', and 'Change "to:" URI'. The 'general' section has a red box around the 'name' field, which contains 'Telcomobile'. Other fields include 'admin' (enabled), 'domain' (empty), and 'failover-detection' (ping). The 'servers' section shows a 'server-pool' with a 'Delete' button. The 'policy' section has a red box around the 'outbound-session-config-pool-entry' field, which is set to 'vsp\session-config-pool\entry ToTelcoMobile'. There are 'Edit' and 'Create' buttons next to it.

Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway Telcomobile** → **server-pool** → **server Telco1** and enter the IP address provided by Vodafone Netherlands for the Vodafone Netherlands OneVoice Corporate SIP trunk connection in to the **host** field. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows a tree view of the configuration hierarchy: Configuration (all), cluster, vsp, default-session-config, tls, session-config-pool, dial-plan, enterprise, servers, sip-gateway PBX, sip-gateway Telcofixed, vsp/session-config-pool/entry, server-pool, server Telco1, sip-gateway Telcomobile, vsp/session-config-pool/entry, server-pool, server Telco1, dns, and settings. The main content area is titled 'Configure vspenterprise\servers\sip-gateway Telcomobile\server-pool\server Telco1'. It includes a 'Show advanced' button and a 'Help' link. Below the title bar are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The configuration is divided into two sections: 'General' and 'Policy'. The 'General' section contains fields for 'server-name' (Telco1), 'admin' (enabled), 'host' (62.140.143.75), 'transport' (UDP), and 'port' (5060). The 'Policy' section contains links for 'outbound-normalization' and 'inbound-normalization'.

General:	
* server-name	Telco1
admin	enabled (Resource is active)
* host	62.140.143.75 (host name or n.n.n.n)
transport	transport UDP (User Datagram Protocol)
port	5060 (at minimum 1, default=5060)

Policy:	
outbound-normalization	<a href="#">Add outbound-normalization</a>
inbound-normalization	<a href="#">Add inbound-normalization</a>

## 7.6. Dial Plan Configuration

The dial plan is used to define how calls route between SIP entities. For the compliance test four routes are required.

- The route **FromTelcofixed** will be used to route fixed calls from Vodafone Netherlands to the Session Manager.
- The route **FromPBXfixed** will be used to route fixed calls from the Session Manager to Vodafone Netherlands.
- The route **FromTelcomobile** will be used to route mobile calls from Vodafone Netherlands to the Session Manager.
- The route **FromPBXmobile** will be used to route mobile calls from the Session Manager to Vodafone Netherlands.

Navigate to **vsp → dial-plan → source-route FromTelco** and alter the entry in the **name** field to **FromTelcofixed**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy: **Configuration: all** > **cluster** > **box:AASBC01Vlan6.avaya.com** > **vsp** > **dial-plan** > **route Default** > **source-route FromTelcofixed**. The main content area is titled **Configure vsp\dial-plan\source-route FromTelcofixed**. It includes a **general** tab and a **name** field set to **FromTelcofixed**, which is highlighted with a red box. Other fields include **description**, **source-match**, **type** (set to **server**), **source-server** (set to **vsp\enterprise\servers\sip-gateway Telcofixed**), **peer** (set to **server**), **location-match-preferred** (set to **up-to-outbound-peer**), **priority** (set to **100**), **condition-list** (set to **Configure**), and **condition-list-match-secondary** (set to **false**). Buttons for **Set**, **Reset**, **Back**, **Copy**, and **Delete** are visible at the top of the configuration area.

Navigate to **vsp** → **dial-plan** → **source-route FromTelco** and click **Copy** (not shown). In the resulting screen alter the entry in the **name** field to **FromTelcomobile**. In the **source-server** field select the **Telcomobile** SIP server created in **Section 7.5**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'vsp' expanded and 'dial-plan' selected. The main area displays the configuration for 'source-route FromTelcomobile'. The 'general' tab is active, showing fields for 'name' (set to 'FromTelcomobile'), 'description', 'source-match', 'source-server' (set to 'vsp\enterprise\servers\sip-gateway Telcomobile'), 'peer' (type 'server', server 'vsp\enterprise\servers\sip-gateway PBX'), 'location-match-preferred' (set to 'up-to-outbound-peer'), and 'priority' (set to '100').

Navigate to **vsp** → **dial-plan** → **source-route FromTelco** and alter the entry in the **name** field to **FromPBXfixed**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'vsp' expanded and 'dial-plan' selected. The main area displays the configuration for 'source-route FromPBXfixed'. The 'general' tab is active, showing fields for 'name' (set to 'FromPBXfixed'), 'description', 'source-match', 'source-server' (set to 'vsp\enterprise\servers\sip-gateway PBX'), 'peer' (type 'server', server 'vsp\enterprise\servers\sip-gateway Telcofixed'), 'location-match-preferred' (set to 'up-to-outbound-peer'), and 'priority' (set to '100').

Navigate to **vsp** → **dial-plan** → **source-route FromPBXfixed** and click **Copy** (not shown). In the resulting screen update the fields as shown below:

- Alter the entry in the **name** field to **FromPBXmobile**.
- Under the **source-match** section, select **condition-list** from the drop down box in the **type** field.
- Under the peer section, in the **server** field select the **Telcomobile** SIP server created in **Section 7.5**

Click **Set** to save changes and then click the **configure** link under the **condition-list** section.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows a tree view with 'Configuration: all' expanded, and 'vsp' > 'dial-plan' > 'source-route FromPBXmobile' selected. The main area is titled 'Configure vsp\dial-plan\source-route FromPBXmobile'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The configuration fields are as follows:

general:	
* name	FromPBXmobile
description	
* source-match	* type: condition-list
peer	type: server (Peer is a SIP server) server: vsp\enterprise\servers\sip-gateway Telcomobile
location-match-preferred	up-to-outbound-peer (Outbound peer determines whether preferred)
priority	100 (from 0 to 999,999, default=100)
condition-list	Configure
condition-list-match-secondary	false

In the resulting screen select the **operation OR** from the drop down menu and click the **Add-to-uri-condition** link under the **to-uri-condition** section.

The screenshot shows the Avaya Aura Configuration interface for the 'condition-list' configuration. The left sidebar shows the tree view with 'vsp' > 'dial-plan' > 'source-route FromPBXmobile' > 'condition-list' selected. The main area is titled 'Configure vsp\dial-plan\source-route FromPBXmobile\condition-list'. It has buttons for 'Set', 'Reset', 'Back', and 'Delete'. The configuration fields are as follows:

operation	OR
mode	evaluate (The Net-Net OS-E runs the conditions to determine whether to apply session configuration settings.)
sip-message-condition	Add sip-message-condition
from-uri-condition	Add from-uri-condition
to-uri-condition	Add to-uri-condition
request-uri-condition	Add request-uri-condition

In the resulting screen define the dial patterns that the condition list should match by updating the fields as shown below:

- For **attribute** select **user** from the drop down menu. This means that the condition will try to match the user part of the uri.
- For **match** select **contains** from the drop down menu. This means that the condition list will match anything that contains the entry in the value field.
- In the **value** field enter the digits to match using regular expression.

Click **Create** to save the condition.

Configuration: all

Configuration Setup View

cluster

box:AASBC01Vlan6.avaya.com

vsp

default-session-config

tls

session-config-pool

dial-plan

route Default

source-route FromTelcofixed

source-route FromPBXmobile

Create vspldial-plan|source-route FromPBXmobile|condition-list|to-uri-condition - Step 1 of 1: Edit to-uri-condition Help

Please provide some basic information for to-uri-condition. Then press "Create".

\* attribute user (particular resource located at host)

\* match contains (allow values which contain the specified expression)

\* value ^00316 (regular expression)

Create Reset Cancel

The AASBC can be used to create the regular expression for the **value** field. Click the **(regular expression)** link next to the **value** field as seen in the previous screen. The following pop up box is displayed. Enter the digits to be matched and select the appropriate radio button for the type of match. The example below will match any digits beginning with 210, this will produce a regular expression of **^210**.

(regular expression)

You can set the match option so that the system matches the entire string, the beginning or end of the string, or any part of the string.

Enter String Pattern 210

Match option

☐ Exact Match ☒ Match Beginning ☐ Match End ☐ Match Any

OK Cancel



The following screen shows the to-uri-conditions used during the compliance test.

**Configuration**

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

**Configuration: all**

Configuration Setup View

- cluster
  - box:AASBC01Vlan6.avaya.com
- vsp
  - default-session-config
  - tls
  - session-config-pool
  - dial-plan
    - route Default
      - source-route FromTelcofixed
      - source-route FromPBXmobile
      - source-route FromTelcomobile
      - source-route FromPBXfixed
  - enterprise
  - dns
  - settings

**Configure vspldial-plan|source-route FromPBXmobile|condition-list** Help Index

Set Reset Back Delete

Press "Set" to keep these values.

**operation** OR

**mode** evaluate (The Net-Net OS-E runs the conditions to determine whether to apply session configuration settings.)

**sip-message-condition** Add sip-message-condition

**from-uri-condition** Add from-uri-condition

**to-uri-condition**

		attribute
▼	Edit Delete	user contains *00316
▲▼	Edit Delete	user contains *210
▲▼	Edit Delete	user contains *06
▲	Edit Delete	user contains ^+316

Add to-uri-condition

## 7.7. Save the Configuration

To save the configuration, click on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.

**Configuration: all**

Configuration Setup View

- Update and save configuration
- Reload configuration
- Validate configuration
- Analyze configuration
- Search configuration
- Save as XML
- Load from XML

default-session-config

## 8. Verification Steps

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

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

```
status trunk 2
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00001	in-service/idle	no
0002/002	T00007	in-service/idle	no
0002/003	T00008	in-service/idle	no
0002/004	T00009	in-service/idle	no
0002/005	T00010	in-service/idle	no

2. From System Manager **Home** Tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The left sidebar contains a navigation menu with options like Session Manager, Dashboard, Session Manager, Administration, Communication Profile, Editor, Network Configuration, Device and Location, Configuration, Application, and Configuration. The main content area is titled 'SIP Entity, Entity Link Connection Status' and includes a sub-header 'All Entity Links to SIP Entity: AASBC01'. Below this, there is a table with columns: Details, Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. A single row is visible, showing 'sesmgr02' as the Session Manager Name, '10.10.6.38' as the SIP Entity Resolved IP, '5060' as the Port, 'TCP' as the Protocol, 'Up' as the Connection Status, '200 OK' as the Reason Code, and 'Up' as the Link Status. The table is filtered to show 1 item.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	sesmgr02	10.10.6.38	5060	TCP	Up	200 OK	Up

- From the AASBC **Actions** tab it is possible to send a SIP OPTIONS message to a specified IP address to confirm the correct response. Select **sip** from the left hand menu and select **ping** from the drop down menu in the **type** field. Enter the required IP address in the **server** field and specify the appropriate **transport** type and **port**. Click **Invoke** and the result of the test are shown towards the top of the page.

The screenshot shows the Avaya Aura web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions' (selected), 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar lists various actions, with 'sip' selected. The main content area is titled 'sip' and 'Actions for SIP transport connections'. It displays a 'Success' message with the following details: 'Sending OPTIONS to 62.140.143.75:5060 UDP', 'Success! Received OPTIONS Response 200:', 'From: sip:62.140.151.115', 'To: sip:62.140.143.75', and 'Contact: <sip:62.140.143.75>'. Below the message is a form for configuring the test. The form fields are: '\* action' (empty), '\* type' (set to 'ping' with a dropdown arrow and a hint '(Query a SIP endpoint with SIP option)'), '\* server' (set to '62.140.143.75'), 'transport' (set to 'UDP' with a dropdown arrow and a hint '(User Datagram Protocol)'), and 'port' (set to '5060' with a hint '(at minimum 1,default=5060)'). An 'Invoke' button is located at the bottom right of the form.

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

## 9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to Vodafone Netherlands SIP Trunk Solution comprising of Vodafone Office Voice and Vodafone OneVoice Corporate. Vodafone Netherlands SIP Trunk Solution is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Vodafone Vodafone Netherlands SIP Trunk Solution comprising of Vodafone Office Voice and Vodafone OneVoice Corporate passed compliance testing. Please refer to **Section 2.2** for any observations or workarounds relating the testing covered by these Application Notes.

## 10. 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, June 2010.
- [2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [3] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, May 2009, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager Release 6.1*, November 2010.
- [6] *Installing and Configuring Avaya Aura® Session Manager*, January 2011, Document Number 03-603473
- [7] *Administering Avaya Aura® Session Manager*, March 2011, Document Number 03-603324.
- [8] *Avaya Aura® Session Border Controller System Administration*, September 2010
- [9] *Installing and Configuring Avaya Aura Session Border Controller*, May 2011
- [8] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>

Additional Vodafone product documentation is available at [http://www.vodafone.nl/zakelijk/totaal\\_oplossingen/vast\\_en\\_mobiel/](http://www.vodafone.nl/zakelijk/totaal_oplossingen/vast_en_mobiel/)

---

**©2011 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).