



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura[®] Communication Manager Access Element and Avaya Aura[®] Session Manager to support UPC Business SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the UPC Business SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager and Avaya Aura[®] Communication Manager. UPC is a member of the DevConnect Service Provider program.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between UPC Business SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager and Avaya Aura[®] Communication Manager Access Element. Customers using this Avaya SIP-enabled enterprise solution with the UPC Business SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

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 Session Manager and Communication Manager. The enterprise site was configured to use the SIP Trunk Service provided by UPC.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by UPC. Incoming PSTN calls were made to H.323, SIP, Digital and analog telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via UPC to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and analog telephones.
- Calls using G.729, G.711A and G.711Mu codec's.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode.
- DTMF transmission using RFC 2833 with successful 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 was turned off during this test.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by UPC requiring Avaya response and sent by Avaya requiring UPC response.

2.2. Test Results

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

- The Calling Line Identity (CLI) set at the enterprise and is hidden if the number is withheld at the enterprise in this case no number is presented to the called party.
- T38 Fax only operates using the G.711 Codec for transporting data to Communication Manager over the UPC Business SIP Trunking service.
- All tests were completed using H.323, SIP, Digital and analogue phone types. The Avaya one-X Communicator was used to test Soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Routing to emergency numbers (such as 999) was not tested.

2.3. Support

For technical support on UPC products please contact an authorized UPC representative.

Email: iotest@upc.nl

Phone: +31-88-1212000 (Request contact to Product Manager for VoIP services)

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the UPC Business SIP Trunk Service. Located at the enterprise site is a Session Manager and Communication Manager. Endpoints are Avaya 9600 series IP telephones, Avaya 4600 series IP telephones (with H.323 firmware), Avaya 2400 series Digital telephone, an Analog Telephone and fax machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

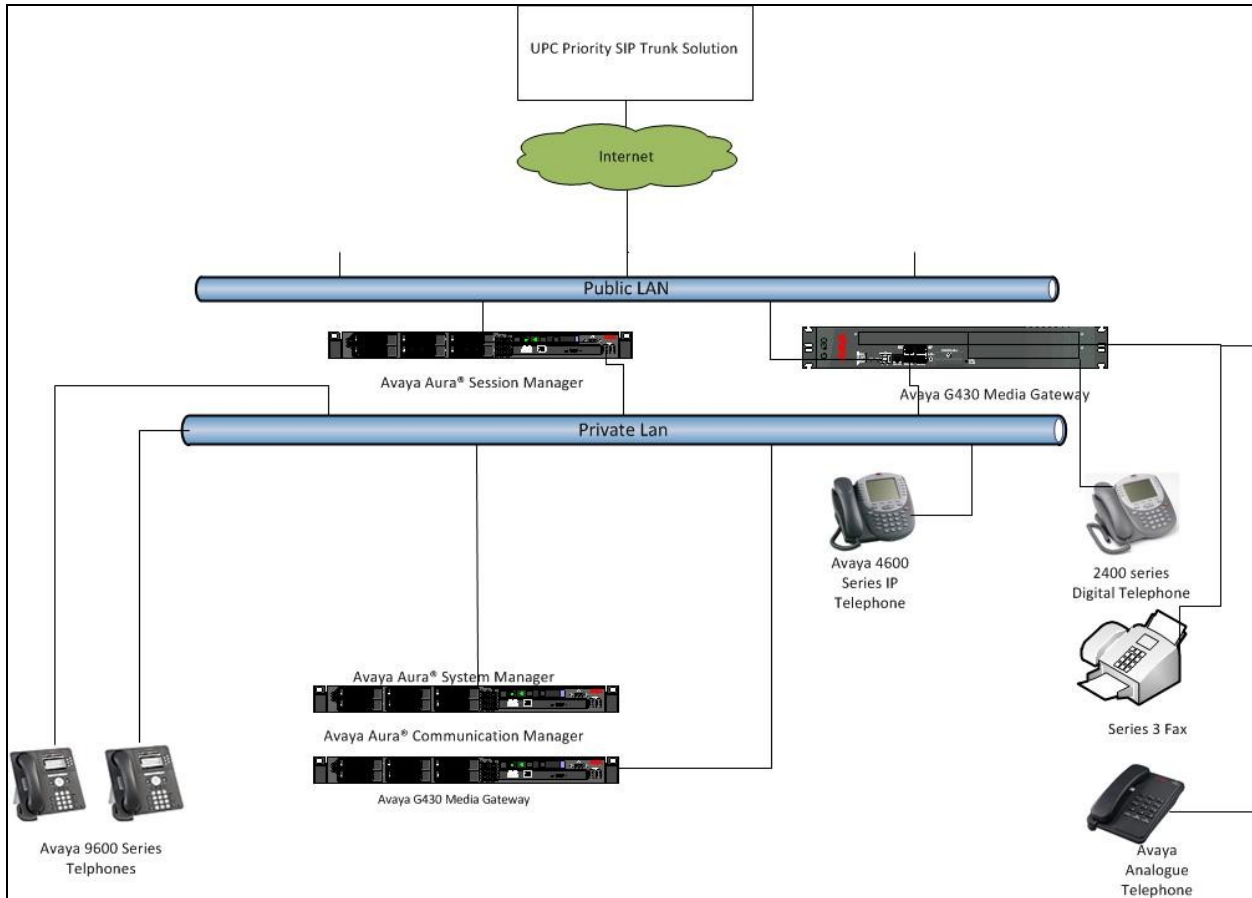


Figure 1: UPC Business SIP Solution Topology

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Media Server	Avaya Aura® Communication Manager R6.0.1 (R016x.00.1.510.1-18860)
Avaya G430 Media Gateway MM711 Analogue MM712 Digital	HW31 FW093 HW07 FW009
Avaya S8800 Media Server	Avaya Aura® Session Manager R6.1 (6.1.0.0.610023)
Avaya S8800 Media Server	Avaya Aura® System Manager R6.1 (6.1.0.4.5072-6.1.4.113)
Avaya 9620 Phone (H.323)	3.11
Avaya 9620 Phone (SIP)	2.6.4.0
Avaya 4621 Phone (H.323)	2.9.1
Avaya 2420 Digital Phone	N/A
Analog Phone	N/A
UPC SIP Trunk Service	UPC Voipconnect platform version 2.0 SBC: Genband S3 Release version V5.2.2

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signaling associated with UPC Business SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from UPC 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 UPC 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 S8730 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 UPC network, and any other SIP trunks used.

```
display system-parameters customer-options                               Page 2 of 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 0
      Maximum Concurrently Registered IP Stations: 18000 3
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 18000 0
      Maximum Video Capable IP Softphones: 18000 0
      Maximum Administered SIP Trunks: 24000 30
```

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? n                                         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? n
    IP Trunks? y

IP Attendant Consoles? y
(NOTE: You must logoff & login to effect the permission changes.)
```

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, **smpub** and **192.168.1.18** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** name as this is the 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        10.10.7.52
  smpub        192.168.1.18
  default       0.0.0.0
```

5.3. Administer IP Network Region

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

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **Avaya.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is set to yes to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. In this configuration this must be set to **no**.
- 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** will be used.

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
Region: 1
Location: 1          Authoritative Domain: Avaya.com
Name: Default NR
MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: no
                          Codec Set: 1          Inter-region IP-IP Direct Audio: no
                          UDP Port Min: 2048          IP Audio Hairpinning? n
                          UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5          AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS          RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
```

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 UPC were configured, namely G.711A, G.711MU and G.729.

```
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.711A      n           2          20
2: G.729      n           2          20
3: G.711MU    n           2          20
```


UPC Business SIP Trunk Service supports the T.38 fax protocol. Configure the T.38 fax protocol by setting the **Fax Mode** to **t.38-standard** on **Page 2** of the codec set form as shown below.

```
change ip-codec-set 1 Page 2 of 2
```

IP Codec Set

Allow Direct-IP Multimedia? n

	Mode	Redundancy
FAX	t.38-standard	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

5.5. Administer SIP Signaling Groups

This signaling group (and trunk group) will be used for inbound and outbound PSTN calls to UPC Business SIP Trunk Service and will be configured using UDP (User Datagram Protocol) and the default udp port of 5060. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set the **Group Type** field to **sip**.
- The **Transport Method** field is set to **udp** (User Datagram Protocol).
- 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 **smpub**), also shown in **Section 5.2**.
- Ensure that the recommended UDP port value of **5060** 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 6.2**. This field logically establishes the **far-end** for calls using this signaling group as network region **1**.
- Set the **Far-end Domain** field to the domain of the enterprise i.e. **avaya.com**
- 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 1
                                SIGNALING GROUP

Group Number: 1                Group Type: sip
                                Transport Method: udp

IMS Enabled? n

Near-end Node Name: procr      Far-end Node Name: smpub
Near-end Listen Port: 5060     Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate
                                Bypass If IP Threshold Exceeded? n
                                RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3
                                IP Audio Hairpinning? n
                                Enable Layer 3 Test? n
                                Direct IP-IP Early 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, i.e. **135**.
- 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 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                                     Group Type: sip           CDR Reports: y
  Group Name: smpub                                COR: 1                   TN: 1           TAC: 135
  Direction: two-way                               Outgoing Display? n
Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                                  Auth Code? n
                                               Signaling Group: 1
                                               Number of Members: 30
```

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 UPC to prevent unnecessary SIP messages during call setup.

```
add trunk-group 1                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                               Redirect On OPTIM Failure: 8000
  SCCAN? n                                         Digital Loss Group: 18
                                               Preferred Minimum Session Refresh Interval(sec): 1800
```

On **Page 3**, set the **Numbering Format** field to **unk-pvt**. As a legal requirement in the Netherlands, it is required that a calling number is sent from the enterprise when a call is forwarded. This is achieved by setting **Modify Tandem Calling Number** to **tandem-cpn-form** (this form is administered in **Section 5.7.2**).

```

add trunk-group 1                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                               Measured: none
                                                Maintenance Tests? y

  Numbering Format: unk-pvt
  UUI Treatment: service-provider

  Replace Restricted Numbers? n
  Replace Unavailable Numbers? N

  Modify Tandem Calling Number: tandem-cpn-form

```

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 **Send Transferring Party Information** to **y**, to allow trunk to trunk transfers. Set **Telephone Event Payload Type** to **101** the value preferred by UPC.

```

add trunk-group 1                                     Page 4 of 21
                                                PROTOCOL VARIATIONS

  Mark Users as Phone? y
  Prepend '+' to Calling Number? n
  Send Transferring Party Information? y
  Network Call Redirection? n
  Send Diversion Header? n
  Support Request History? y
  Telephone Event Payload Type: 101

```

5.7. Administer Calling Party Number Information

5.7.1. Set Private Unknown Numbering

Use the **change private-unknown-numbering** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **4-digit** extension beginning with **13** will send the calling party number **0207111111** to UPC Business SIP Trunk Service. This calling party number will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones.

```

change private-unknown-numbering 0                   Page 1 of 2
  NUMBERING - PUBLIC/UNKNOWN FORMAT
  Total
Ext  Ext      Trk   CPN      Total
Len  Code     Grp(s)  Prefix   CPN
  4   13       1       3110111111  10
Total Administered: 1
Maximum Entries: 240

```

5.7.2. Set Tandem Calling Party Numbering

To allow a CLI to be sent from the enterprise when a call forward off net is in place use the change **tandem-calling-party-num** so that diverted incoming calls from certain **CPN Prefix** numbers are converted to send 3110111111 in this example. The **Number Format** is set to **unk-unk**

```
ch tandem-calling-party-num                               Page 1 of 8
                CALLING PARTY NUMBER CONVERSION
                FOR TANDEM CALLS
```

CPN	Trk	Number
Len Prefix	Grp(s)	Format
7 3	1	unk-unk
10 0	1	unk-unk
12 3	1	unk-unk

```
                Delete  Insert
                3110111111  3110111111  3110111111
```

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 UPC 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**.

```
change feature-access-codes                               Page 1 of 9
                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: *37
                Answer Back Access Code: *12
                Attendant Access Code:
                Auto Alternate Routing (AAR) Access Code: 7
                Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2: *99
                Automatic Callback Activation:      Deactivation:
                Call Forwarding Activation Busy/DA: *87      All: *88      Deactivation: #88
                Call Forwarding Enhanced Status:      Act:      Deactivation:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are 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 0 or 00. Calls are sent to **Route Pattern 1**, which contains the previously configured SIP Trunk Group.

```
change ars analysis 02
```

Page 1 of 2

ARS DIGIT ANALYSIS TABLE						
Location: all					Percent Full: 1	
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
0	10	11	1	lpvt		n
00	11	15	1	lpvt		n

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern 1 is used to route calls to trunk group 1. Set the **Numbering Format** to **unk-unk** for the first route selected to allow CLI to be sent without a + to the UPC network

```
display route-pattern 1
```

Page 1 of 3

Pattern Number: 1 Pattern Name: tosm100									
SCCAN? n Secure SIP? n									
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Digits	DCS/ QSIG	IXC Intw
1: 1	0							n	user
2:								n	user
3:								n	user
4:								n	user
5:								n	user
6:								n	user

BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	No. Dgts	Numbering Format	LAR
0	1	2	M	4	W	Request				
1:	y	y	y	y	y	n	n	rest	unk-unk	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 UPC 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 UPC correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers 3110111111 and 3110222222 to a 4 digit extension by deleting all of the incoming digits and inserting an extension.

```
change inc-call-handling-trmt trunk-group 1                               Page 1 of 3
                                INCOMING CALL HANDLING TREATMENT
Service/      Number   Number   Del Insert
Feature       Len     Digits
public-ntwrk  12    3110111111  all  1306
public-ntwrk  12    3110111111  all  1307
```

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

6. Configuring Avaya Aura® Session Manager

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

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer 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.

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 **SIP 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 screenshot displays the Avaya Aura System Manager interface. On the left, a navigation menu is visible under the 'Routing' section, with 'Domains' highlighted. The main content area is titled 'Domain Management' and includes a breadcrumb trail: 'Home / Elements / Routing / Domains - Domain Management'. Below the title, there are action buttons: 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. A table below shows one domain entry:

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

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

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 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. 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

The screenshot displays the configuration page for a location. On the left is a sidebar with a menu including 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main area is titled 'Location Details' and contains a 'Commit' button in the top right. A message at the top states: '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'. The 'General' section includes a 'Name' field with the value 'SPLab7' and an empty 'Notes' field. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Kbit/sec' and an empty 'Total Bandwidth' field. The 'Per-Call Bandwidth Parameters' section shows 'Default Audio Bandwidth' as '80 Kbit/sec'. The 'Location Pattern' section has 'Add' and 'Remove' buttons and a table with one row: 'IP Address Pattern' with the value '*10.10.7.*' and an empty 'Notes' field.

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 will need to be entered for each SIP Entity. Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the 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 SBC 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.

The screenshot shows the configuration page for a SIP entity. The left sidebar contains a menu with options: Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'General' and contains several fields: 'Name' (ASM61), 'FQDN or IP Address' (10.10.7.61), 'Type' (Session Manager), 'Notes' (empty), 'Location' (SPLab7), 'Outbound Proxy' (empty), 'Time Zone' (Etc/GMT), 'Credential name' (empty), and 'SIP Link Monitoring' (Use Session Manager Configuration). A 'Commit' button is in the top right corner.

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.

The screenshot shows the 'Port' configuration section. It includes an 'Add' button and a 'Remove' button. Below is a table with 3 items and a 'Refresh' button. The table has columns: Port, Protocol, Default Domain, and Notes. The rows are: 5060 UDP avaya.com, 5060 TCP avaya.com, and 5061 TLS avaya.com. There is a 'Select: All, None' option and a '* Input Required' label at the bottom left. A 'Commit' button is at the bottom right.

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

6.4.2. Avaya Aura® Communication Manager SIP Entity

The following screens show the SIP entity for Communication Manager which is configured as an Access Element. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling.

The screenshot shows the 'SIP Entity Details' configuration page for a SIP entity named 'CMEVO'. The page is titled 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. A left-hand navigation menu includes 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'SIP Entity Details' section is currently set to 'General'. A 'Commit' button is visible in the top right corner. The configuration fields are as follows:

- Name:** CMEVO
- FQDN or IP Address:** 10.10.7.52
- Type:** CM
- Notes:** (empty)
- Adaptation:** (dropdown menu)
- Location:** SPLab7
- Time Zone:** Etc/GMT
- Override Port & Transport with DNS SRV:**
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none

6.4.3. UPC Business SIP Trunk Service SIP Entities

Each SBC used by UPC for the SIP trunk provision must be added to Session Manager as a SIP entity. The **FQDN or IP Address** field is set to the IP address of the SBC provided by UPC.

The screenshot shows the 'SIP Entity Details' configuration page for a SIP entity named 'UPCSBC'. The page is titled 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. A left-hand navigation menu includes 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'SIP Entity Details' section is currently set to 'General'. A 'Commit' button is visible in the top right corner. The configuration fields are as follows:

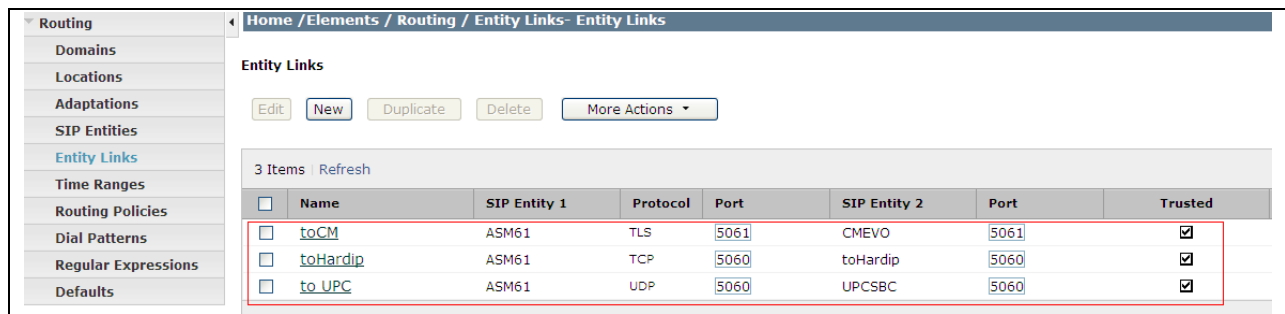
- Name:** UPCSBC
- FQDN or IP Address:** 192.168.0.2
- Type:** Gateway
- Notes:** (empty)
- Adaptation:** (dropdown menu)
- Location:** SPLab7
- Time Zone:** Europe/Amsterdam
- Override Port & Transport with DNS SRV:**
- SIP Timer B/F (in seconds):** 4

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

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



<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	toCM	ASM61	TLS	5061	CMEVO	5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	toHardip	ASM61	TCP	5060	toHardip	5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	to_UPC	ASM61	UDP	5060	UPCSBC	5060	<input checked="" type="checkbox"/>

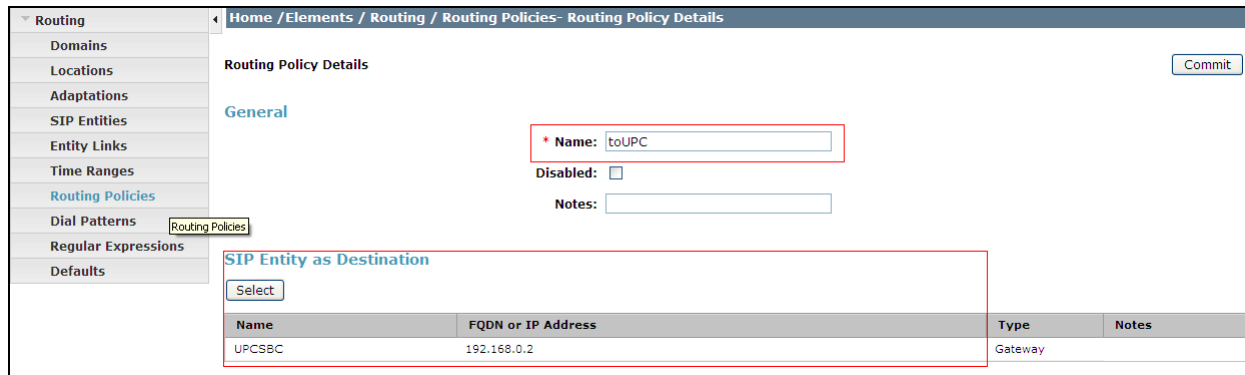
6.6. Administer Routing Policies

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.

The following screen shows the routing policy for Communication Manager



Routing Policy Details

Commit

General

* Name:

Disabled:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
UPCSBC	192.168.0.2	Gateway	

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 the domain configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save (not shown). The following screen shows an example dial pattern configured for UPC Business SIP Trunk Service.

The screenshot displays the configuration interface for a SIP Dial Pattern. The left sidebar contains a menu with options: SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled 'General' and includes the following fields:

- * Pattern:** 311
- * Min:** 10
- * Max:** 15
- Emergency Call:**
- SIP Domain:** -ALL- (dropdown menu)
- Notes:** (empty text field)

Below the 'General' section is the 'Originating Locations and Routing Policies' section, which includes 'Add' and 'Remove' buttons and a '1 Item Refresh' link. A table lists the configured items:

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	SPLab7		toUPC	0	<input type="checkbox"/>	UPCSBC

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

Dial Pattern Details Commit

General

* Pattern:

* Min:

* Max:

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

2 Items Refresh Filter:

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SPLab7		TO_CMEVO	0	<input type="checkbox"/>	CMEVO	

7. UPC Configuration

The configuration required by UPC to allow the tests to be carried is not covered in this document and any further information required shown be obtained through the local UPC representative.

8. Verification Steps

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

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

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CMEVO

Summary View

1 Item Refresh Filter: E

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	ASM61	10.10.7.52	5061	TLS	Up	200 OK	Up

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

```

status trunk 1

                                TRUNK GROUP STATUS

Member   Port      Service State   Mtce Connected Ports
                                Busy
0001/001 T00001   in-service/idle no
0001/002 T00007   in-service/idle no
0001/003 T00008   in-service/idle no
0001/004 T00009   in-service/idle no
0001/005 T00010   in-service/idle no

```

- 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 Access Element and Avaya Aura® Session Manager to UPC Business SIP Trunk Service. UPC Business SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>

©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.