Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.1, Avaya Aura® Session Border Controller to support BT Wholesale/HIPCOM SIP Trunk Service – Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between BT Wholesale (BTW)/HIPCOM's SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Aura® Communication Manager. BT 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 BTW/HIPCOM's SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager and an Avaya Aura® Session Border Controller (AASBC). Customers using this Avaya SIP-enabled enterprise solution with BTW/HIPCOM's 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 BTW/HIPCOM.

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 BTW/HIPCOM. 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 BTW/HIPCOM to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and analog telephones.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, and local directory assistance.
- 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.
- Response to incomplete call attempts and trunk errors
- SIP trunk serviceability was tested by taking the trunk out of service
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

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

- 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.

2.3. Support

For technical support on BTW/HIPCOM products please contact the following website: http://www.hipcom.co.uk

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to BTW/HIPCOM's SIP Trunk Service. Located at the enterprise site is a Session Manager, Communication Manager, and Session Border Controller. 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.

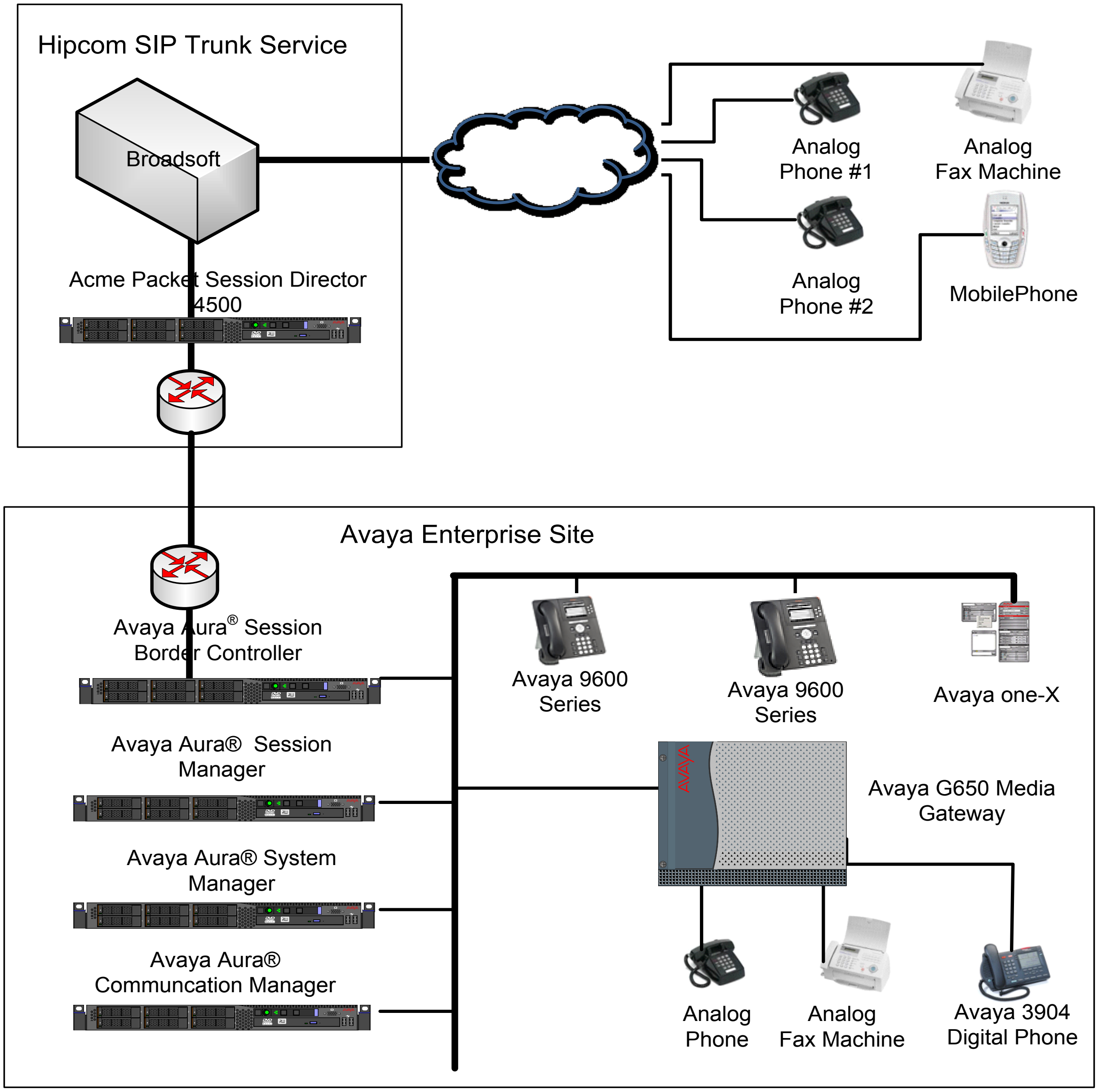


Figure 1: BTW/HIPCOM SIP Solution Topology

4. Equipment and Software Validated

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

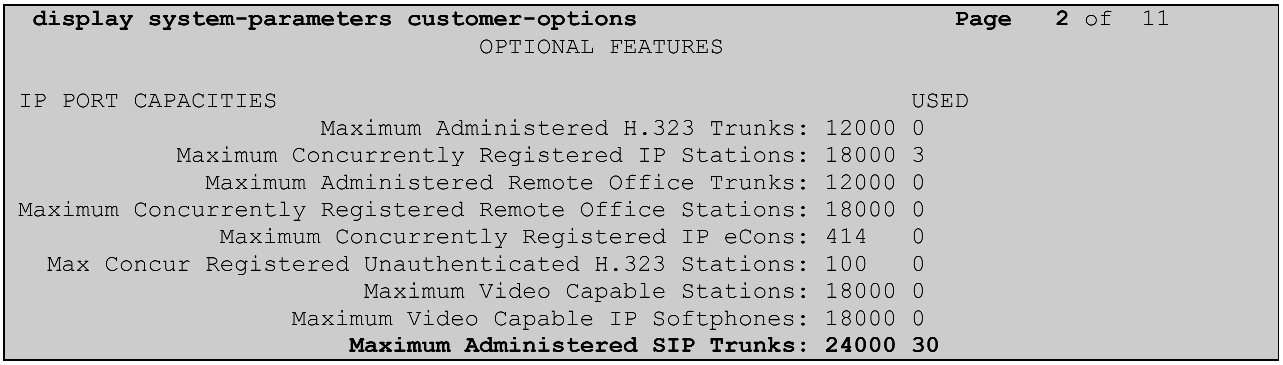
Equipment	Software
Avaya S8800 Media Server	Avaya Aura® Communication Manager R6.0.1 (R016x.00.1.510.1-19009) Service Pack 3
Avaya G650 Media Gateway MM711 Analogue MM712 Digital	 HW31 FW093 HW07 FW009
Avaya S8800 Media Server	Avaya Aura® Session Manager R6.1 (6.1.3.0.613006) Service Pack 3
Avaya S8800 Media Server	Avaya Aura® System Manager R6.1 (6.1.0.0.7345 – 6.1.5.112) Service Pack 3
Avaya Media S8800 server	Avaya Aura® Session Border Controller version E362P4
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
BTW/HIPCOM SIP Trunk Service	Acme Packet 4500 Net-Net SBC ver SCX6.1.0 Broadsoft - ver 14 Service Pack 9 Configuration version - A1B149G1

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 BTW/HIPCOM Business SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from BTW/HIPCOM 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 BTW/HIPCOM 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 S8800 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 BTW/HIPCOM 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.
- 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: Defualt 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
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 BTW/HIPCOM 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
```

BTW/HIPCOM 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 BTW/HIPCOM Business SIP Trunk Service and will be configured using TCP (Transport Control Protocol) and the default tcp 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 **tcp** (Transport Control 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 TCP 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 5.3** 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: tcp
  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

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  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:

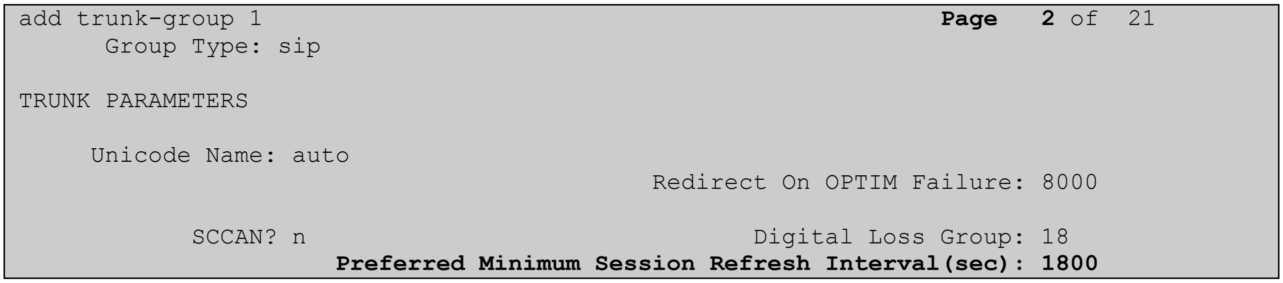
- Set the **Group Type** field to **sip**.
- Choose a descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan, i.e. **135**.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **tie**.
- Specify 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 BTW/HIPCOM to prevent unnecessary SIP messages during call setup.



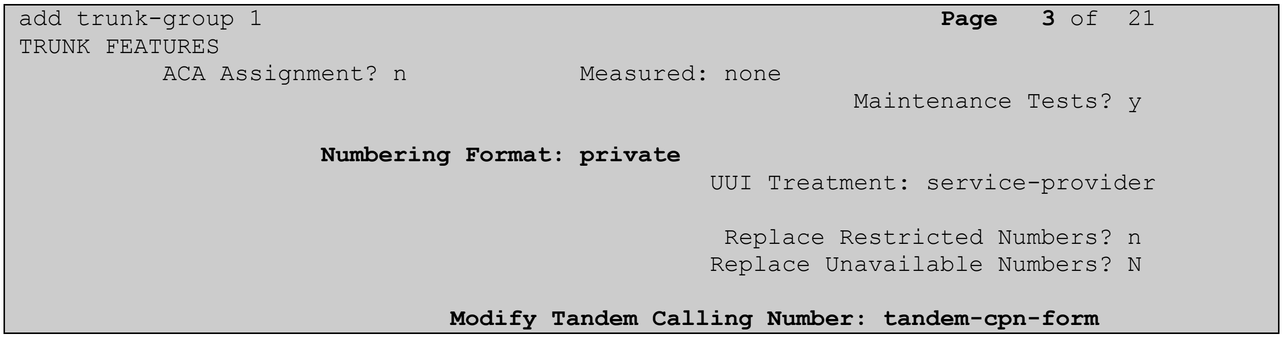
```
add trunk-group 1                                               Page   2 of  21
      Group Type: sip

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 **public.** This is achieved by setting **Modify Tandem Calling Number** to **tandem-cpn-form** (this form is administered in **Section 5.7.1.**



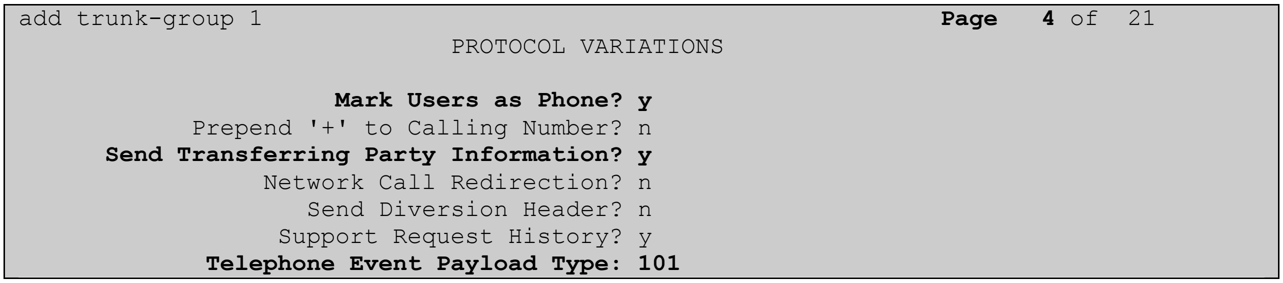
```
add trunk-group 1                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y

                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? N

                              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 BTW/HIPCOM.



```
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-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 **442031122333** to BTW/HIPCOM 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-numbering 0                                  Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 1
 4  13           1          442031122333     12    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 BTW/HIPCOM 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           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   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 BTW/HIPCOM network

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

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                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 BTW/HIPCOM 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 BTW/HIPCOM correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers **44203xxxx1** and **44203xxxx2** 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
 tie             12  44203xxxxxx1     all  1306
 tie             12  44203xxxxxx2     all  1307
```

5.10. Save Transalations

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:

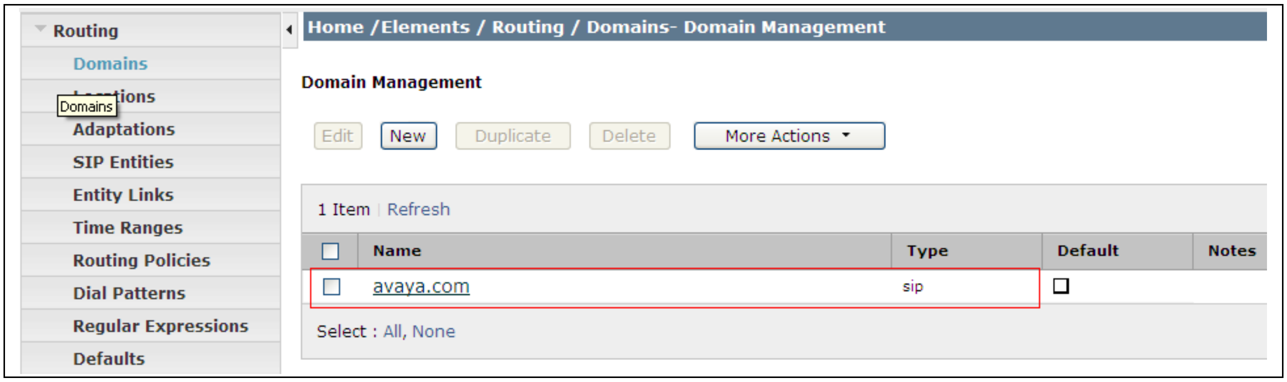
- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns

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).

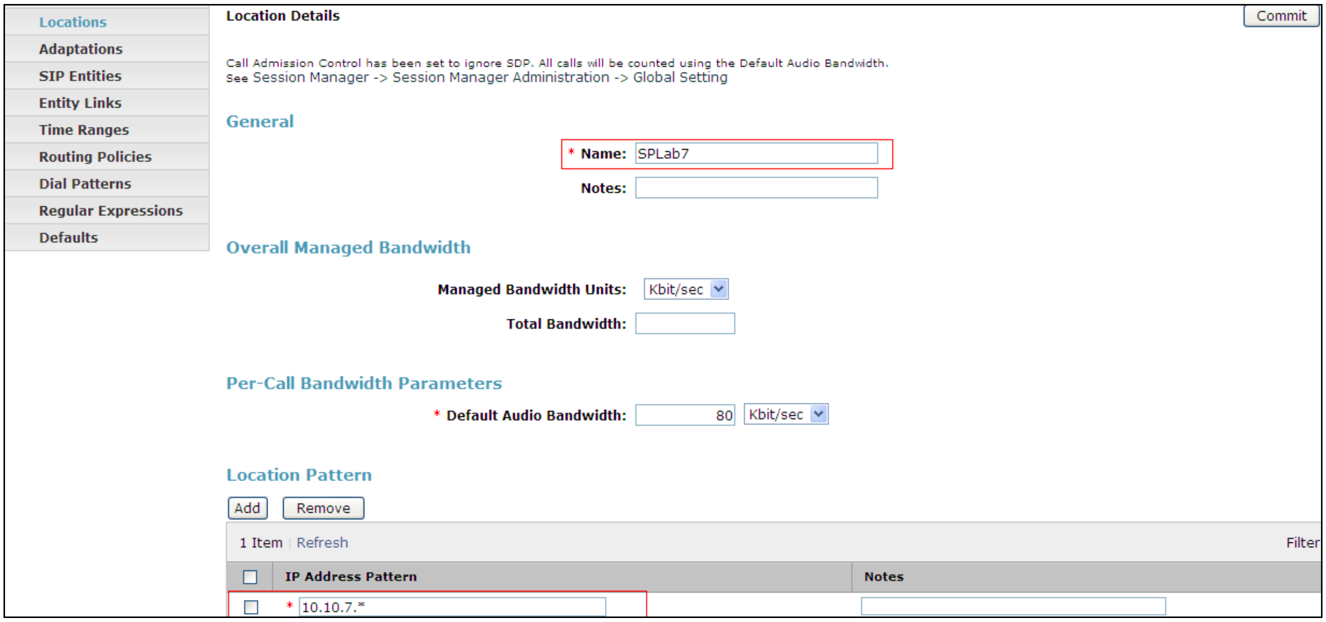


Domain Management

□	Name	Type	Default	Notes
□	avaya.com	sip	□	

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One locations 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



Location Details

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: SPLab7

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

1 Item

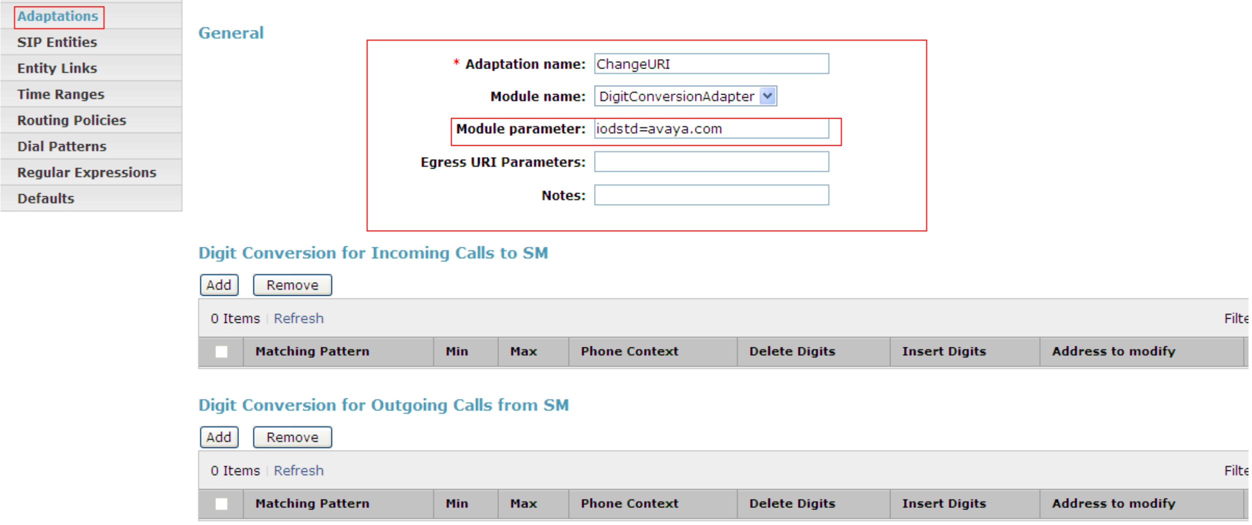
□	IP Address Pattern	Notes
□	* 10.10.7.*	

6.4. Configure Adaptation Module

Session Manager is installed with a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as host names in the Request-URI (Uniform Resource Identifier). In this configuration the adaptation is used by the AASBC to ensure ingress messages have the hostname **avaya.com** when they are sent to the Session Manager and to the CS1K. To add an adaptation, select **Adaptations** on the left panel menu and then click on the **New** button (not shown). Under **General:**

- **Adaptation Name:** Enter an informative name
- **Module Name:** **<click to add module>** from the drop down list and enter "DigitConversionAdapter" in the resulting **New Module Name** field
- **Module Parameter:** Enter the modification parameters to be used. In this configuration the modification parameters used was **"iodstd=avaya.com"**.

iodstd (or **ingressOverrideDestinationDomain**) replaces the domain in a Request-URI and Notify/message-summary body with the given value for ingress only. The reason why this was added was that incoming calls to the enterprise had BTW/HIPCOM's domain name in the SIP messages. The domain on the enterprise is avaya.com so this Adaption Module changed incoming SIP messages destined for the enterprise to a recognised domain.



General

* Adaptation name: ChangeURI

Module name: DigitConversionAdapter

Module parameter: iodstd=avaya.com

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify

Digit Conversion for Outgoing Calls from SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General:**

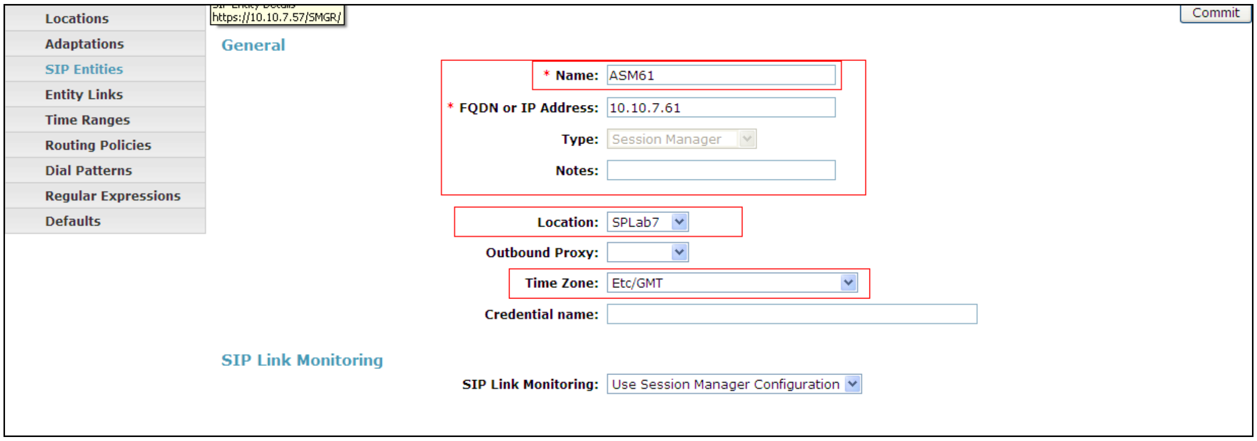
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP 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

6.5.1. Avaya Aura® Session Manager SIP Entity

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



General

* Name: ASM61

* FQDN or IP Address: 10.10.7.61

Type: Session Manager

Notes:

Location: SPLab7

Outbound Proxy:

Time Zone: Etc/GMT

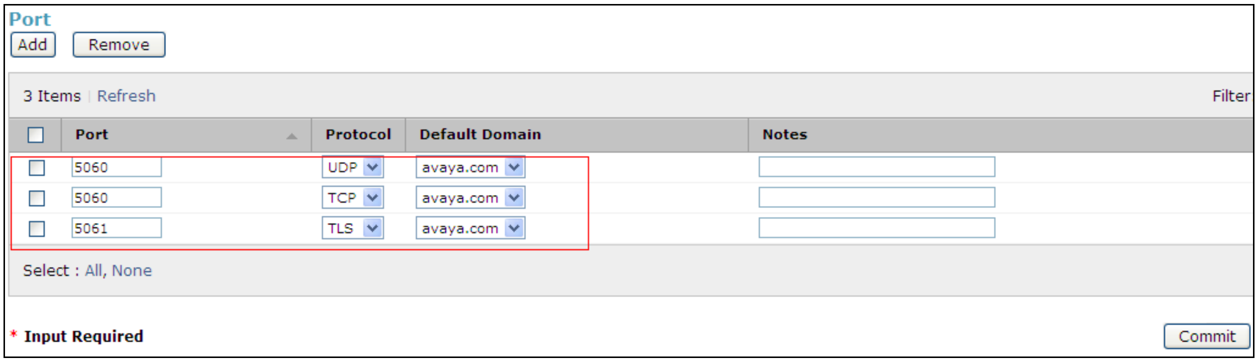
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

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

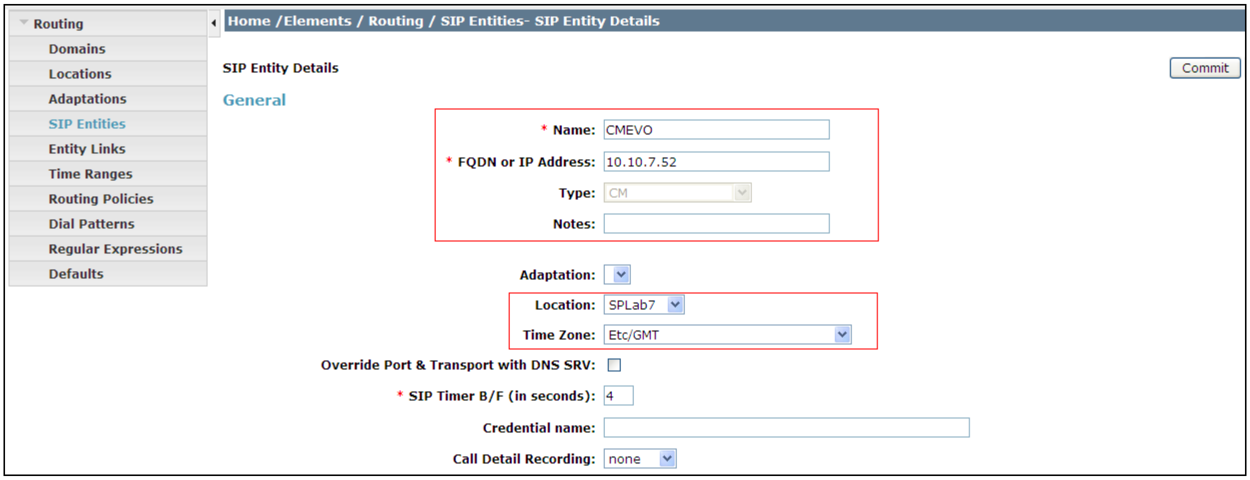


□	Port	Protocol	Default Domain	Notes
□	5060	UDP	avaya.com	
□	5060	TCP	avaya.com	
□	5061	TLS	avaya.com	

* Input Required

6.5.2. 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.



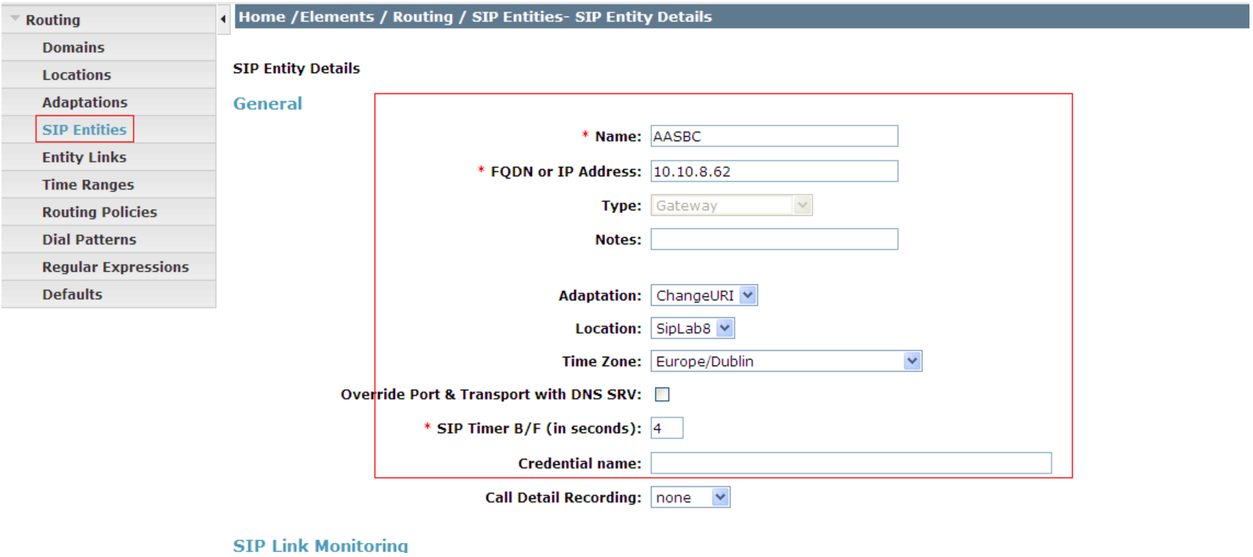
SIP Entity Details

General

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

6.5.3. Avaya Aura® Session Border Controller SIP Entity

The following screens show the SIP entity for AASBC which is configured as a Gateway element. The **FQDN or IP Address** field is set to the IP address of the Interface that will be providing SIP signaling. The following screenshot shows the SIP Entity defined for AASBC in the sample configuration, note the adaption created in **Section 6.4** is associated with this entity link.



SIP Entity Details

General

* Name:	AASBC
* FQDN or IP Address:	10.10.8.62
Type:	Gateway
Notes:	
Adaptation:	ChangeURI
Location:	SipLab8
Time Zone:	Europe/Dublin
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

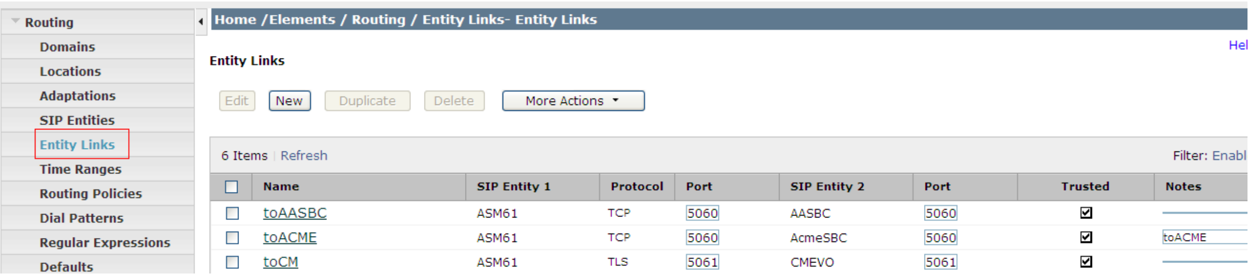
SIP Link Monitoring

6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button . 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 6.5.2 and 6.5.3**
- 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.



Entity Links

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
□	toAASBC	ASM61	TCP	5060	AASBC	5060	☑	
□	toACME	ASM61	TCP	5060	AcmeSBC	5060	☑	toACME
□	toCM	ASM61	TLS	5061	CMEVO	5061	☑	

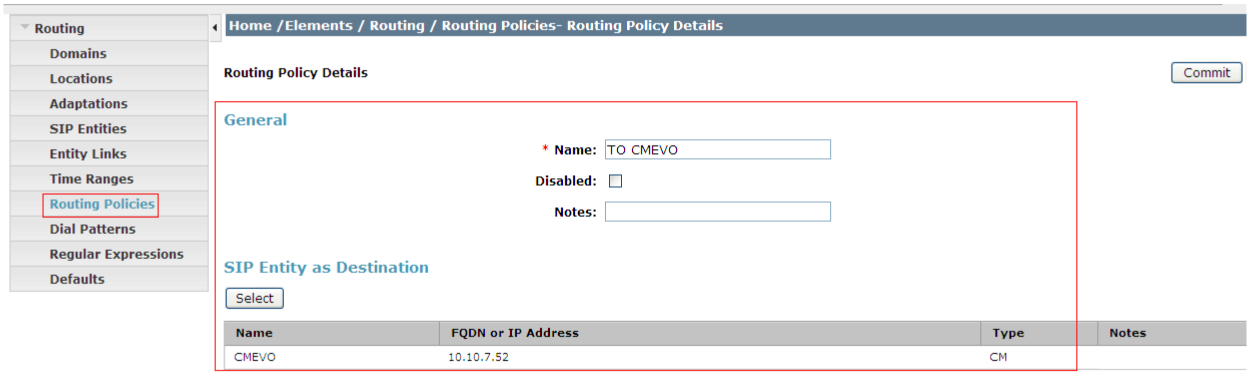
6.7. Administer Routing Policies

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

Under **General:**

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

The following screen shows the routing policy for Communication Manager



Routing Policy Details

General

* Name: TO CMEVO

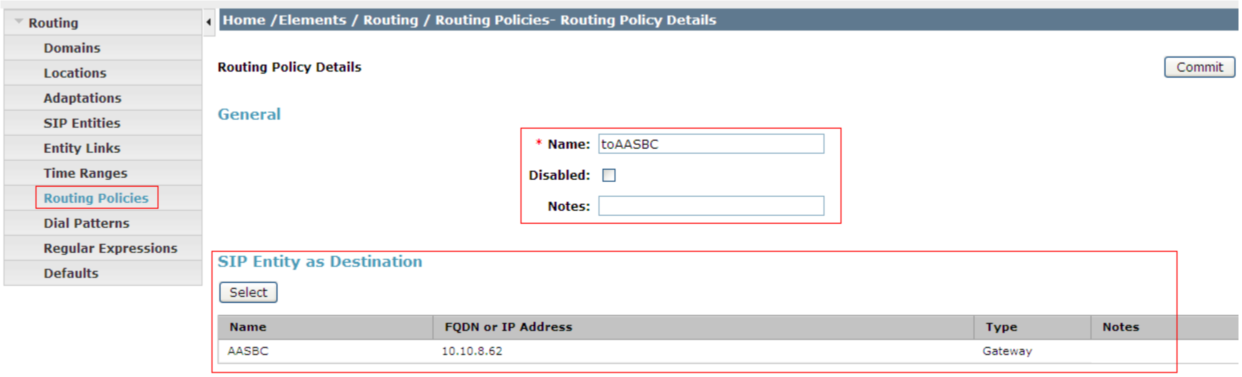
Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CMEVO	10.10.7.52	CM	

For routing policy to the AASBC – BTW/HIPCOM SIP Trunk, select the SIP Entity associated with AASBC defined in **Section 6.5.3** and click **Select.** The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition. The following screenshot shows the Routing Policy for AASBC – BTW/HIPCOM SIP Trunk.



Routing Policy Details

General

* Name: toAASBC

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
AASBC	10.10.8.62	Gateway	

6.8. Administer Dial Patterns

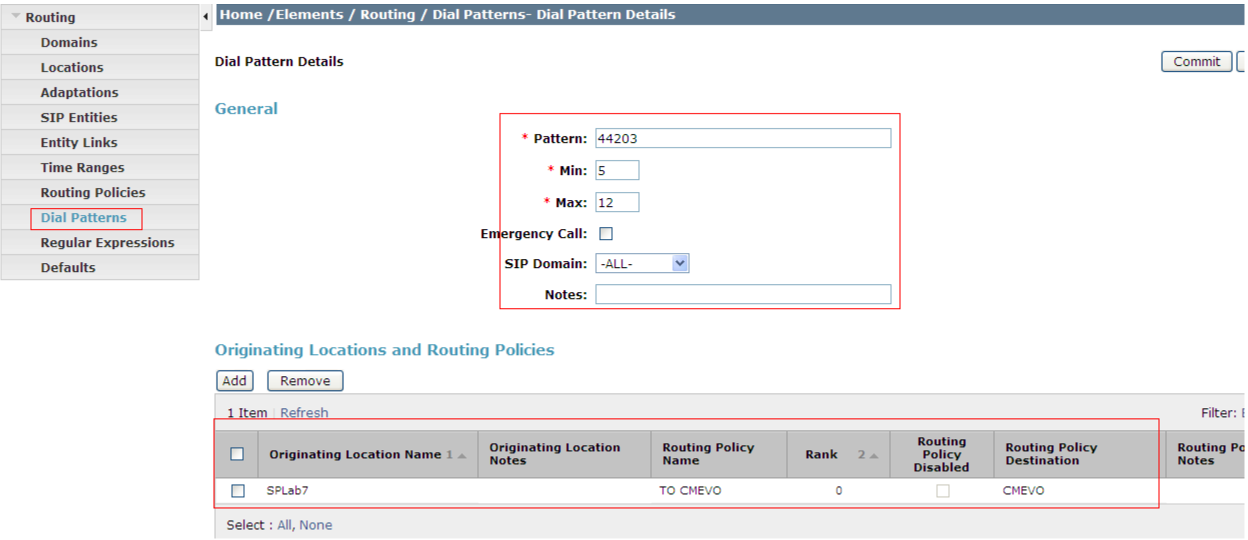
Dial patterns are used to route calls to appropriate SIP Entities. In the sample configuration, since the DDI range given for the testing all numbers that start with **44203** will be routed to the Communication Manager for terminating to test sets. Alternately calls that are originated on the Communication Manager that start with digits **00353** will be routed to the AASBC and then on to BTW/HIPCOM's SIP network, there is a dialing pattern added for this as well. To define a dial pattern, expand **Elements → Routing** and select **Dial Patterns** (not shown). Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Communication Manager
- **Min:** Enter the minimum number digits that must to be dialed
- **Max:** Enter the maximum number digits that may be dialed
- **SIP Domain:** Select the SIP Domain from drop-down menu or select **All** if Session Manager should accept incoming calls from all SIP domains
- **Notes:** Enter a brief description.[Optional]

In the **Originating Locations and Routing Policies** section, click **Add.** The **Originating Locations and Routing Policy List** page opens (not shown).

- **Originating Locations** Select **All**
- **Routing Policies** Select the Routing Policy defined for Communication Manager in **Section 6.7**

Click **Select** to save these changes and return to **Dial Pattern Details** page. Click **Commit** to save. The following screen shows the Dial Pattern defined for sample configuration. The following screenshot shows the Routing Policy for Communication Manager.



Dial Pattern Details

General

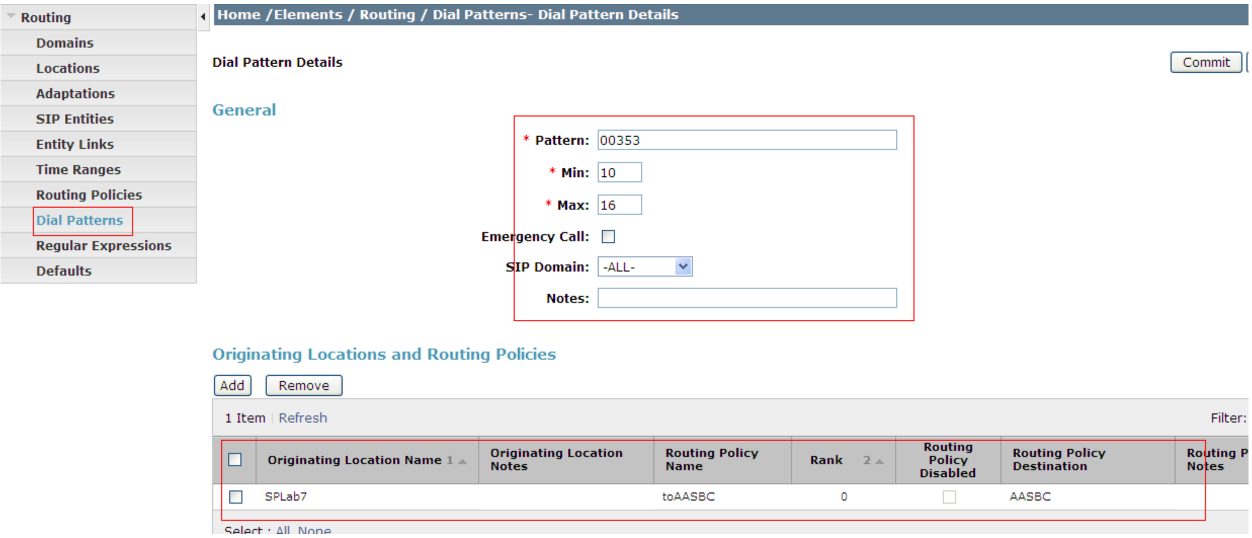
* Pattern: 44203
* Min: 5
* Max: 12
Emergency Call: □
SIP Domain: -ALL-
Notes:

Originating Locations and Routing Policies

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Po Notes
□	SPLab7		TO CMEVO	0	□	CMEVO	

Select : All, None

Repeat the above steps to add the dial Pattern to the AASBC, select the routing policy defined for the AASBC in **Section 6.7**. The following screenshot shows the Routing Policy for AASBC – BTW/HIPCOM's SIP network.



Dial Pattern Details

General

* Pattern:	00353
* Min:	10
* Max:	16
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

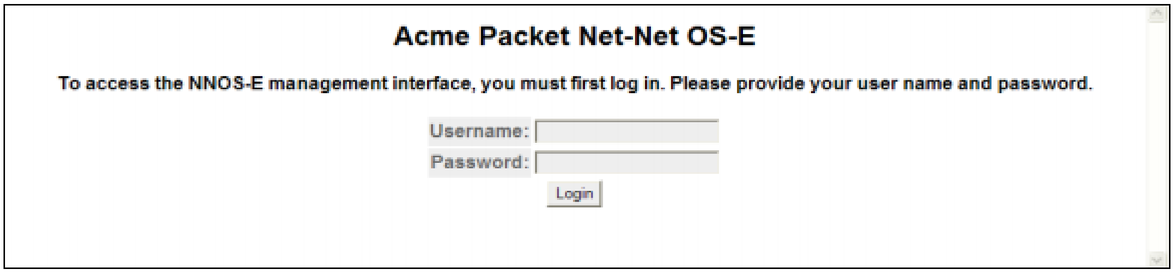
□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing P Notes
□	SPLab7		toAASBC	0	□	AASBC	

7. Configure Avaya Aura® Session Border Controller

This section provides the procedures for configuring AASBC to receive and route calls over the SIP trunk between CS1K and BTW/HIPCOM SIP Trunks. These instructions assume other administration activities have already been completed such as the default configuration. This section will cover the configuration that was put in place specifically for BTW/HIPCOM.

7.1. Access Avaya Aura Session Border Controller

Access the Avaya Aura® SBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured.



Acme Packet Net-Net OS-E

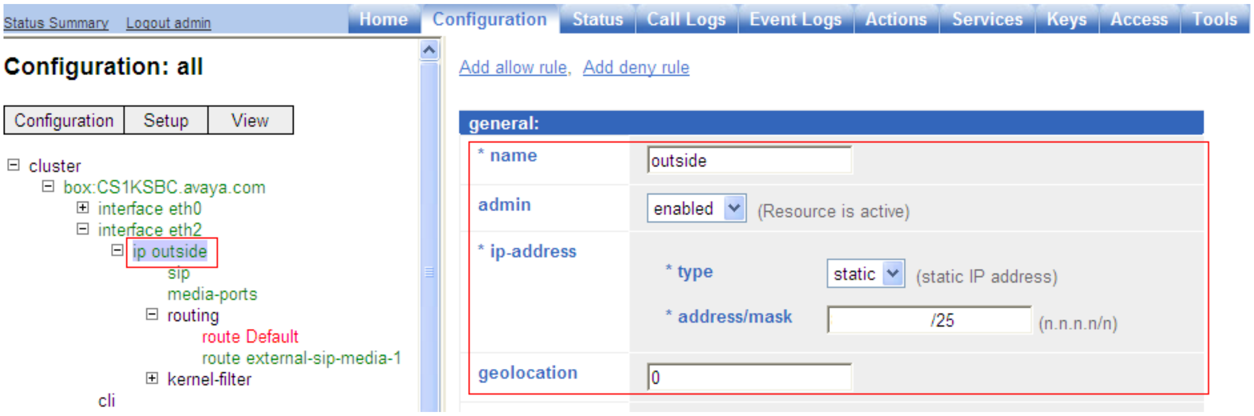
To access the NNOS-E management interface, you must first log in. Please provide your user name and password.

Username:

Password:

7.2. Configuring Outside Interface

An ip address was given to the outside interface that is on the public internet. The ip address is blanked out in the screenshot below for security purposes. Click on the **Configuration** tab and browse to **cluster → interface eth2 → ip outside.**



Configuration: all

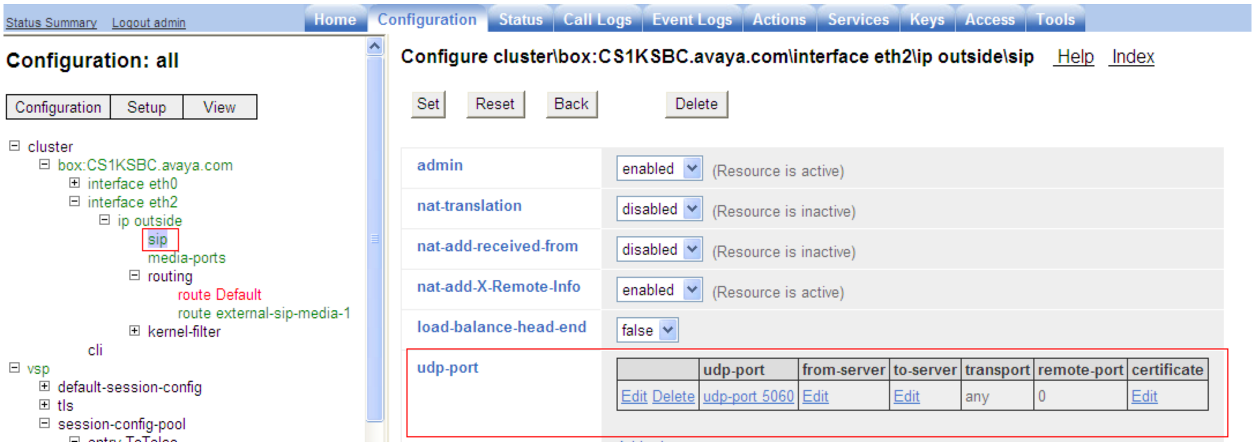
- cluster
  - box:CS1KSBC.avaya.com
    - interface eth0
    - interface eth2
      - ip outside
        - sip
        - media-ports
        - routing
          - route Default
          - route external-sip-media-1
        - kernel-filter
  - cli

general:

* name	outside
admin	enabled (Resource is active)
* ip-address	* type: static (static IP address) * address/mask: /25 (n.n.n.n/n)
geolocation	0

7.2.1. Configure SIP

For the outside interface a transport protocol needs to be configured. In the compliance testing we used UDP for the SIP messaging. Click on the **Configuration** tab and browse to **cluster → interface eth2 → ip outside → sip.**



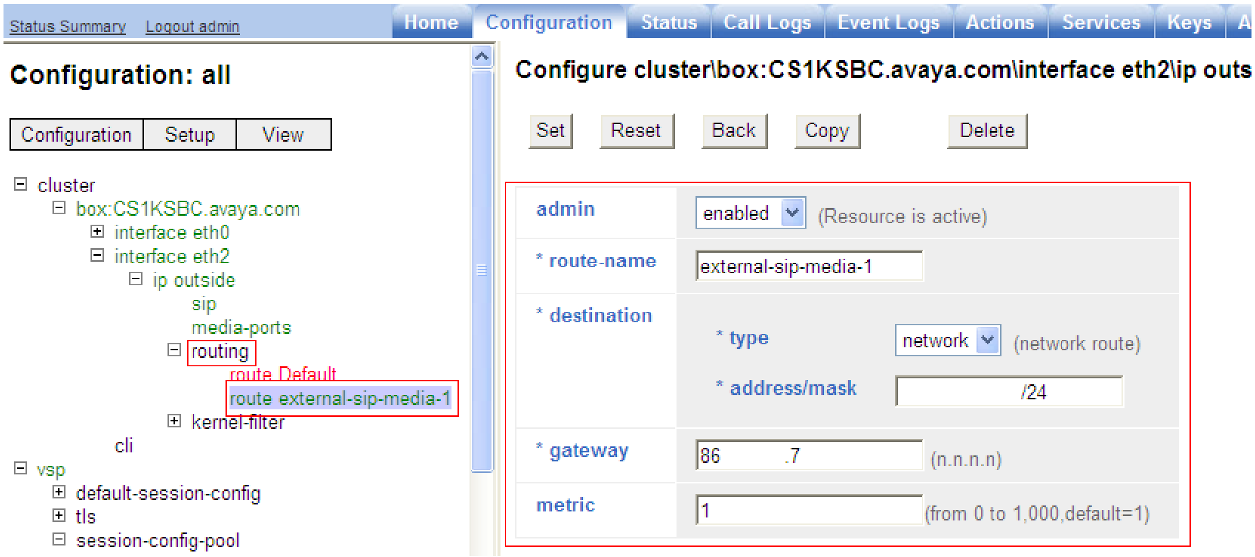
Configure cluster\box:CS1KSBC.avaya.com\interface eth2\ip outside\sip

admin	enabled (Resource is active)
nat-translation	disabled (Resource is inactive)
nat-add-received-from	disabled (Resource is inactive)
nat-add-X-Remote-Info	enabled (Resource is active)
load-balance-head-end	false
udp-port	

	udp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	udp-port 5060	Edit	Edit	any	0	Edit

7.2.2. Configure Routing

For the outside interface routing needs to be configured to advise the SIP traffic how to route out to BTW/HIPCOM's network from the outside interface of the AASBC. The ip address is blanked out in the screenshot below for security purposes. Click on the **Configuration** tab and browse to **cluster → interface eth2 → ip outside → routing → add route.**



Configure cluster\box:CS1KSBC.avaya.com\interface eth2\ip outs

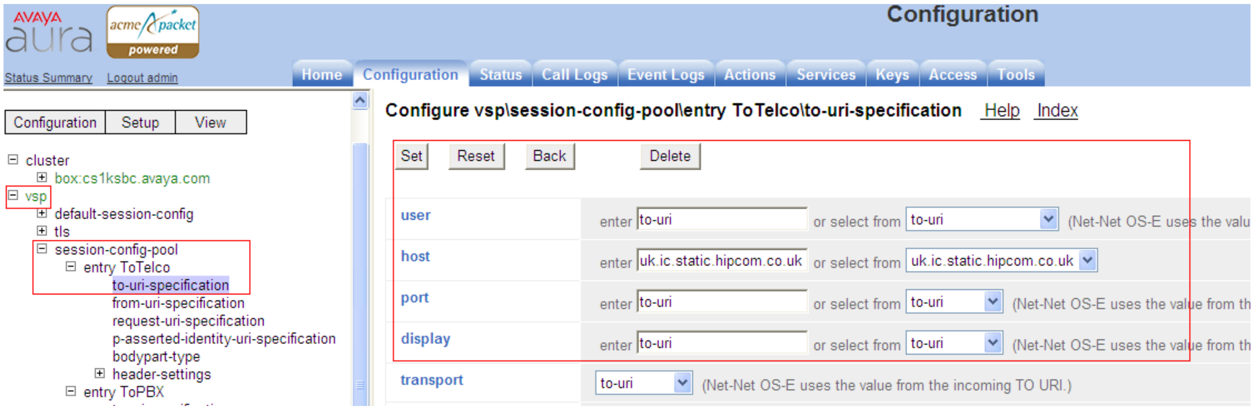
admin	enabled (Resource is active)
* route-name	external-sip-media-1
* destination	* type: network (network route) * address/mask: /24
* gateway	86 .7 (n.n.n.n)
metric	1 (from 0 to 1,000,default=1)

7.3. Configuring VSP

7.3.1. Configure Session-Config-Pool Entry ToTelco

In the **to-uri-specification** a valid host was added for BTW/HIPCOM. Expand **vsp → session-config pool → entry ToTelco → to-uri-specification**. For our testing we used **uk.ic.static.hipcom.co.uk** as shown below.

Please note the domain name used by BTW/HIPCOM will change depending on access method, please consult BTW/HIPCOM to confirm what this will be.



Configure vsp\session-config-pool\entry ToTelco\to-uri-specification

user: enter to-uri or select from to-uri (Net-Net OS-E uses the valu

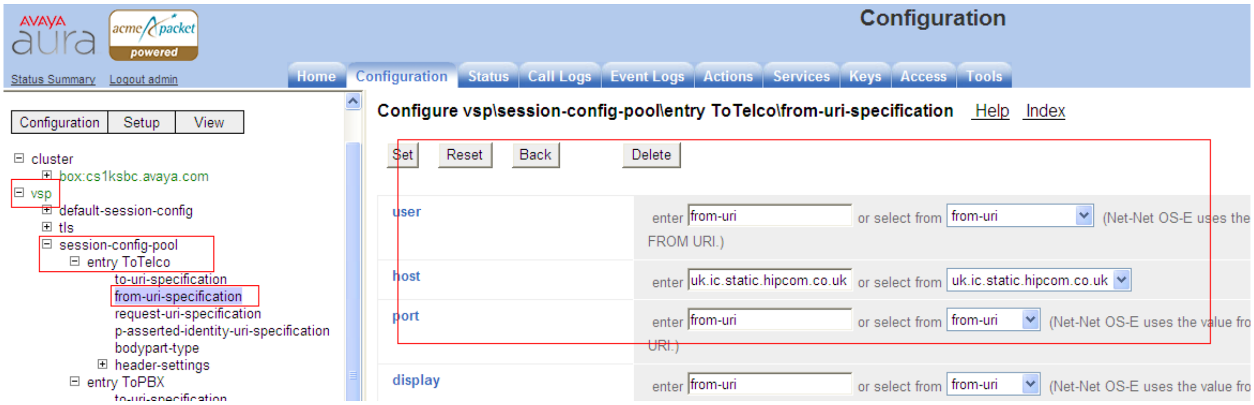
host: enter uk.ic.static.hipcom.co.uk or select from uk.ic.static.hipcom.co.uk

port: enter to-uri or select from to-uri (Net-Net OS-E uses the value from th

display: enter to-uri or select from to-uri (Net-Net OS-E uses the value from th

transport: to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

In the **from-uri-specification** a valid host was added for BTW/HIPCOM. Expand **vsp → session-config pool → entry ToTelco → to-from-specification**. For our testing we used **uk.ic.static.hipcom.co.uk** as seen below:



Configure vsp\session-config-pool\entry ToTelco\from-uri-specification

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

host: enter uk.ic.static.hipcom.co.uk or select from uk.ic.static.hipcom.co.uk

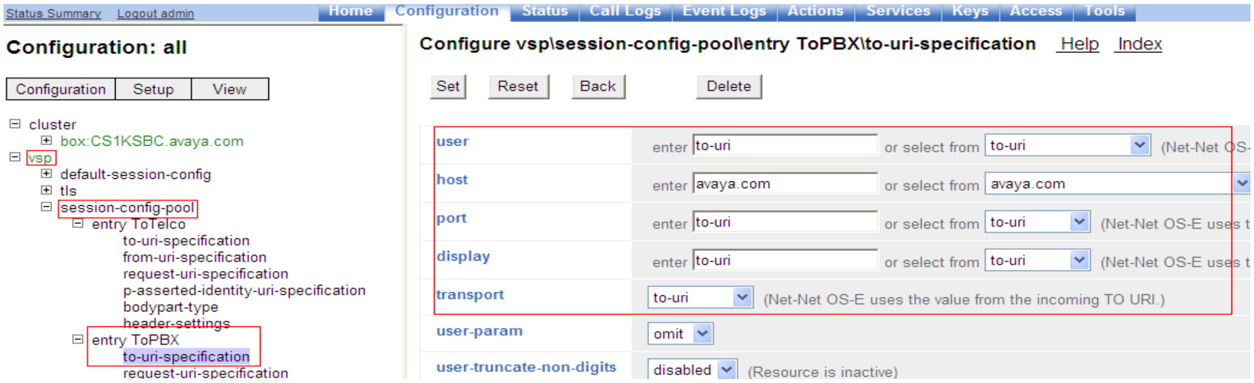
port: enter from-uri or select from from-uri (Net-Net OS-E uses the value fro URI.)

display: enter from-uri or select from from-uri (Net-Net OS-E uses the value fro

Repeat the same process to the change the host value in the request and p-asserted-identity headers to **uk.ic.static.hipcom.co.uk**, this is not shown**.**

7.3.2. Configure Session-Config-Pool Entry ToPBX

In the **to-uri-specification** a new host was added **avaya.com**, this is the SIP domain used in the enterprise and is configured in **Section 6.1**. Expand **vsp → session-config pool → entry ToPBX → to-uri-specification**.

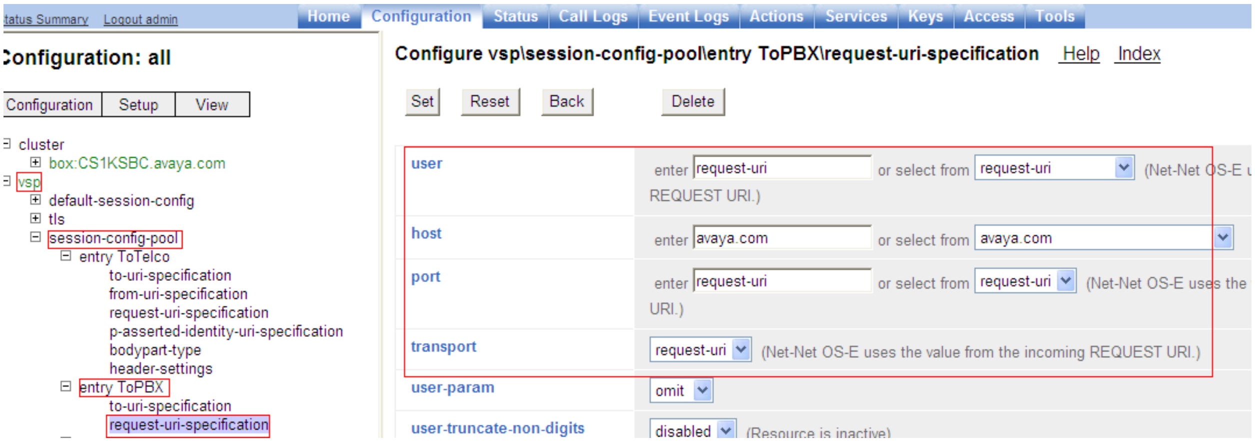


Configure vsp\session-config-pool\entry ToPBX\to-uri-specification

```
cluster
  box:CS1KSBC.avaya.com
vsp
  default-session-config
  tls
  session-config-pool
    entry ToTelco
      to-uri-specification
      from-uri-specification
      request-uri-specification
      p-asserted-identity-uri-specification
      bodypart-type
      header-settings
    entry ToPBX
      to-uri-specification
      request-uri-specification
```

user	enter to-uri or select from to-uri (Net-Net OS-
host	enter avaya.com or select from avaya.com
port	enter to-uri or select from to-uri (Net-Net OS-E uses t
display	enter to-uri or select from to-uri (Net-Net OS-E uses t
transport	to-uri (Net-Net OS-E uses the value from the incoming TO URI.)
user-param	omit
user-truncate-non-digits	disabled (Resource is inactive)

In the **request-uri-specification** a new host was added **avaya.com**, this is the SIP domain used in the enterprise and is configured in **Section 6.1**. Expand **vsp → session-config pool → entry ToPBX → request-uri-specification**.



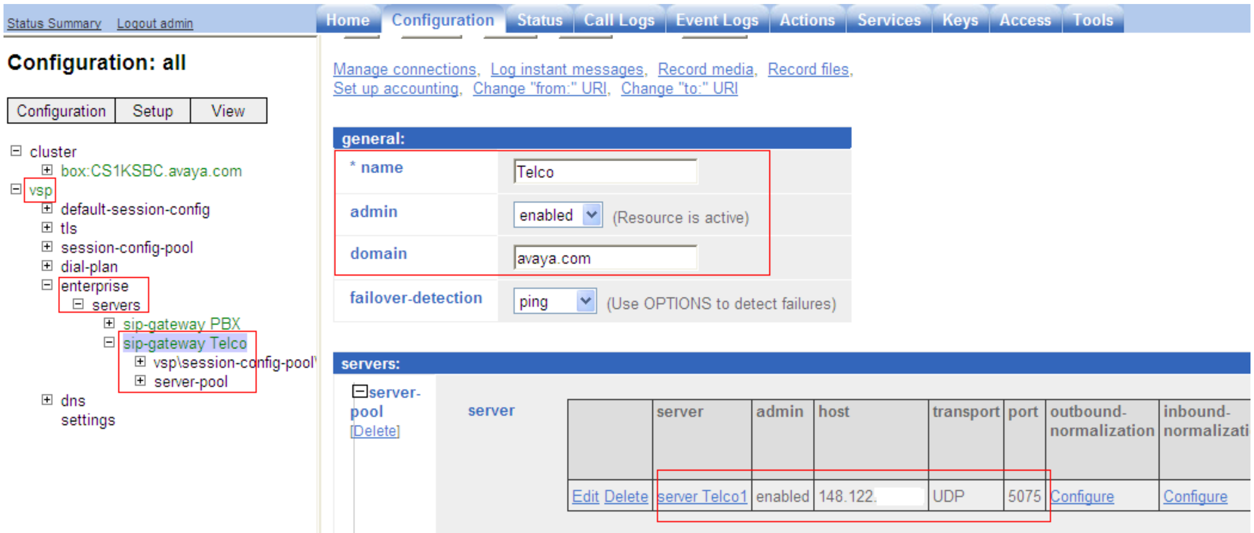
Configure vsp\session-config-pool\entry ToPBX\request-uri-specification

```
cluster
  box:CS1KSBC.avaya.com
vsp
  default-session-config
  tls
  session-config-pool
    entry ToTelco
      to-uri-specification
      from-uri-specification
      request-uri-specification
      p-asserted-identity-uri-specification
      bodypart-type
      header-settings
    entry ToPBX
      to-uri-specification
      request-uri-specification
```

user	enter request-uri or select from request-uri (Net-Net OS-E u REQUEST URI.)
host	enter avaya.com or select from avaya.com
port	enter request-uri or select from request-uri (Net-Net OS-E uses the URI.)
transport	request-uri (Net-Net OS-E uses the value from the incoming REQUEST URI.)
user-param	omit
user-truncate-non-digits	disabled (Resource is inactive)

7.3.3. Configuring Enterprise

In the **sip-gateway-Telco** the domain name used is **avaya.com**. A newly added server was created for BTW/HIPCOM's SBC; information needed here is the ip address, port and transport protocol. Click on the **Configuration** tab and browse to **vsp → enterprise → servers → sip-gateway Telco → server-pool.** Click the **Add server** link**.** The ip address of the SBC has been partially hidden.



general:

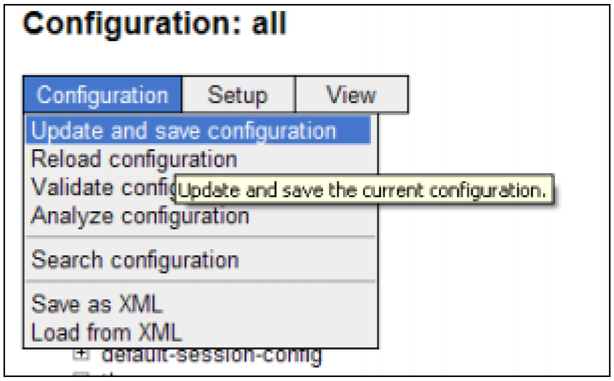
* name	Telco
admin	enabled (Resource is active)
domain	avaya.com
failover-detection	ping (Use OPTIONS to detect failures)

servers:

server	admin	host	transport	port	outbound-normalization	inbound-normalizati
server Telco1	enabled	148.122.	UDP	5075	Configure	Configure

7.4. Save the Configuration

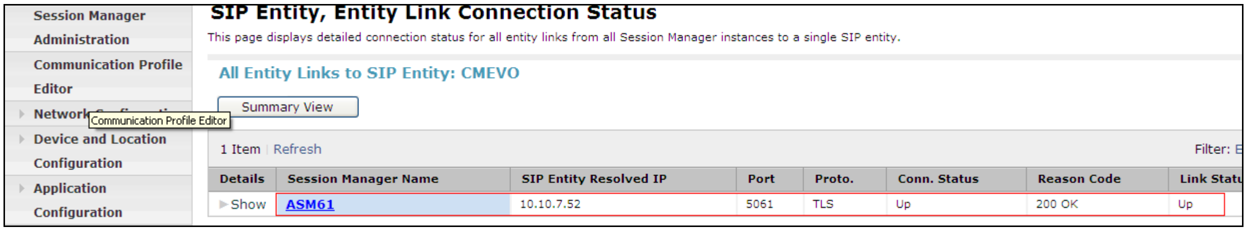
To save the configuration, click on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.



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.**



Session Manager Administration
Communication Profile Editor
Network Configuration
Communication Profile Editor
Device and Location Configuration
Application Configuration
Summary View
1 Item | Refresh
Filter: E

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

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

2. 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
```

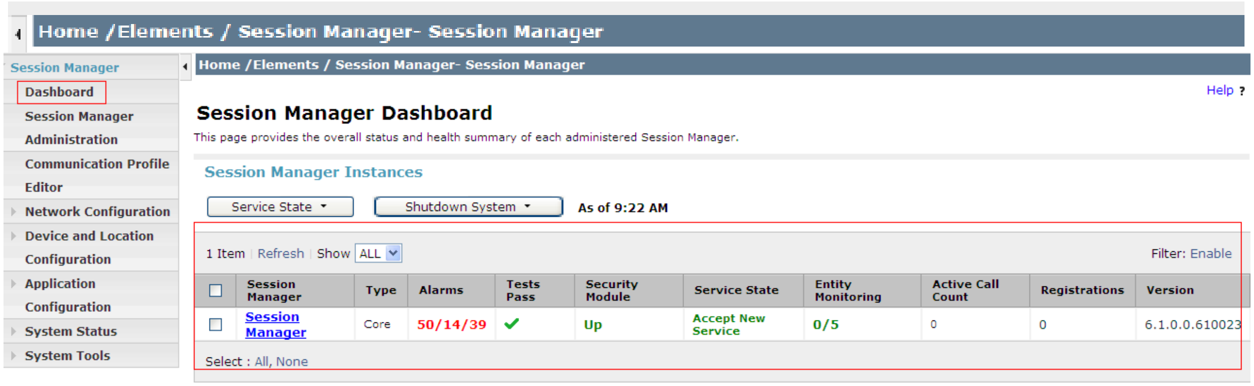
3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
5. Verify that the user on the PSTN can end an active call by hanging up.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

8.1. Verify Avaya Aura® Session Manager Operational Status

8.1.1. Verify Avaya Aura® Session Manager is Operational

Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager. Specifically, verify the status of the following fields as shown below.

- Tests Pass ✓
- Security Module Up
- Service State Accept New Service


Home /Elements / Session Manager- Session Manager
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Help ?

Home /Elements / Session Manager- Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State ▾
Shutdown System ▾

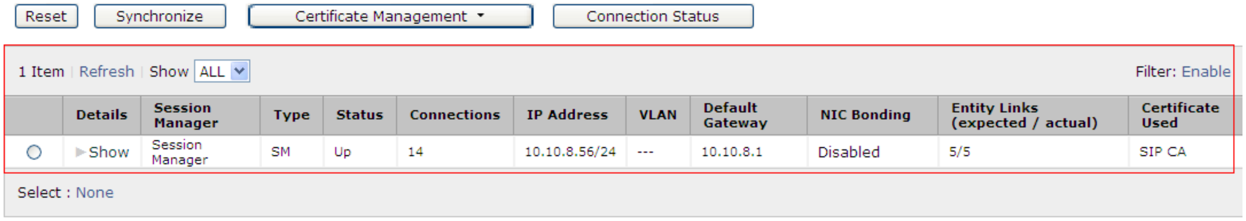
As of 9:22 AM

1 Item | Refresh | Show ALL | Filter: Enable

□	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
□	Session Manager	Core	50/14/39	✓	Up	Accept New Service	0/5	0	0	6.1.0.0.610023

Select : All, None

Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.



1 Item | Refresh | Show ALL | Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
○	▸Show	Session Manager	SM	Up	14	10.10.8.56/24	---	10.10.8.1	Disabled	5/5	SIP CA

Select : None

9. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Manager, Avaya Aura® Session Manager and an Avaya Aura® Session Border Controller to BTW/HIPCOM's SIP Service. The 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 6.0.3, February 2011.

[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.

[3] *Administering Avaya Aura® Communication Manager*, Release 6.0.1, April 2011.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* August 2010, 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*, April 2011, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager,* May 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/

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.