Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0, Avaya Aura® Session Manager R6.1 and Acme Packet SBC to support Telephonica BTNG (Business Trunking Next Generation) SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Telefonica BTNG SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Telefonica 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 Telephonica BTNG 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 Telefonica BTNG 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 Avaya Aura® Session Manager and Avaya Aura® Communication Manager. The enterprise site was configured to use the SIP Trunk Service provided by Telefonica.

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 Telefonica. Incoming PSTN calls were made to H.323, SIP and analog telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via Telefonica to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP 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 protocol.
- 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") was enabled during this test.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Telefonica requiring an Avaya response and SIP OPTIONS sent by Avaya requiring a Telefonica response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Telefonica BTNG 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 operates using the G.711 or G.729 Codecs for transporting data to the tested version of Communication Manager over the Telefonica BTNG SIP Trunking service.
- All tests were completed using H.323, SIP 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 911) was not tested.

2.3. Support

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

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Telefonica BTNG SIP Trunk Service. Located at the enterprise site is an Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Endpoints are Avaya 9600 series IP telephones (with H.323 firmware), 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.

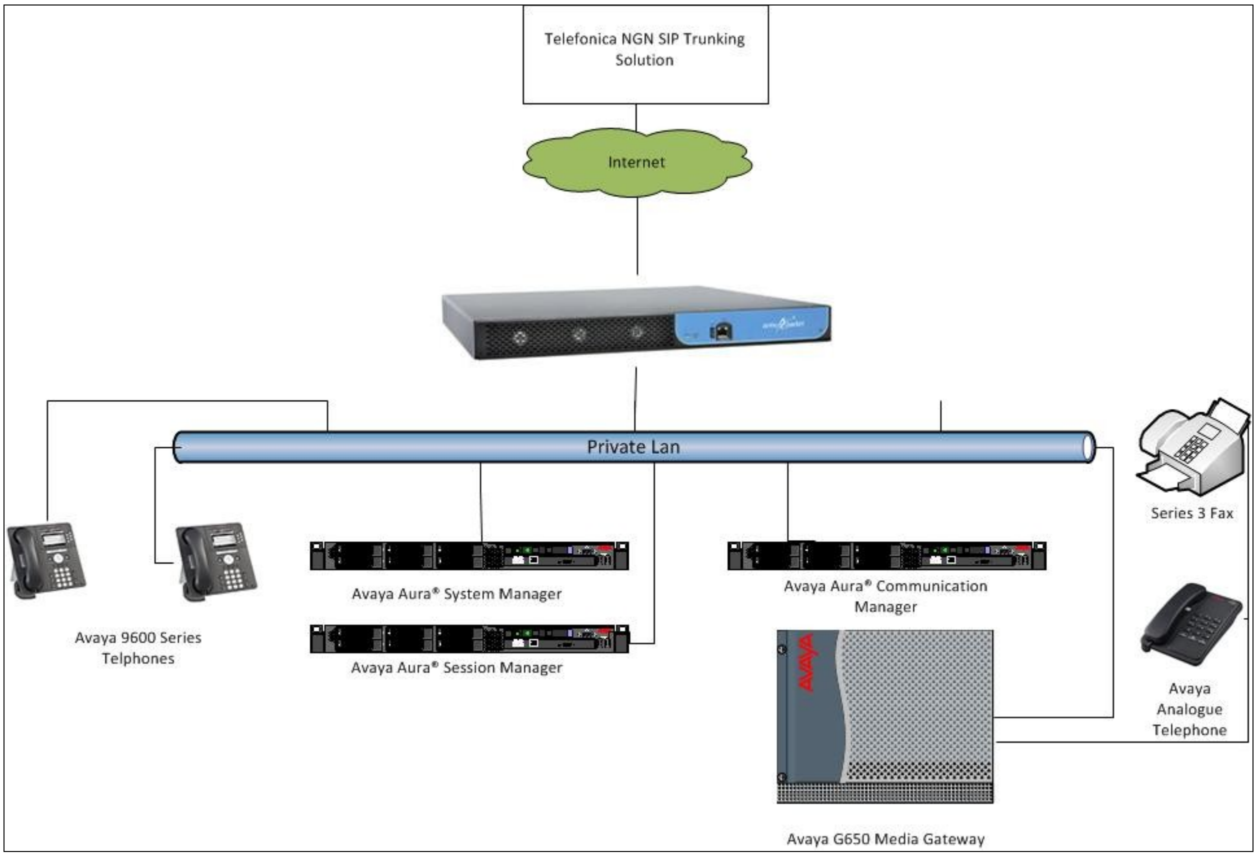


Figure 1: Telefonica BTNG SIP Solution Topology

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	 HW31 FW093
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
Analog Phone	N/A
Telefonica BTNG SIP Trunk Service with Acme Packet 3800 series SBC and Core NGN ICS	BTNG 1.2 SBC 6.1 M7 P4 NGN 5.0
Acme Packet Net-Net 3800	SCX 6.1.0 MR-2 Patch 5 (Build 471)

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 Telefonica BTNG SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from Telefonica 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 Avaya Aura® Session Manager directs the outbound SIP messages to the Telefonica 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 G650 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 Telefonica 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, **asm01** and **10.10.25.21** 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 its SIP signaling interface to Session Manager.

```
display node-names ip
                                  IP NODE NAMES
    Name              IP Address
 procr              10.10.25.133
 asm01              10.10.25.21
 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 **bstk.telefonica.net**.
- 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: bstk.telefonica.net
    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 Telefonica were configured, namely G.711A, G.729 and G.711MU. In this configuration the **Frames Per Packet** is set to **3**.

```
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          3        30
 2: G.729            n          3        30
 3: G.711MU          n          3        30
```

Telephonica BTNG 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 Telefonica BTNG 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 Communication Manager 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 a**sm01**), 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** as network region **1** for calls using this signaling group**.**
- 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: asm01
 Near-end Listen Port: 5060              Far-end Listen Port: 5060
                                       Far-end Network Region: 1
Far-end Domain:

                                             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? y             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: asm01                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 upon with Telefonica 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.**

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

                     Numbering Format: public
                                                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. In this configuration the **Support Request History** must be set to **n.**

```
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? n
             Telephone Event Payload Type:
```

5.7. Administer Calling Party Number Information

5.7.1. Set Public Unknown Numbering

Use the **change public-unknown-numbering** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **4-digit** extension beginning with **3** will send the calling party number **911111111** to Telefonica BTNG 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 public-unknown-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  3           1          911111111        9     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 Telefonica BTNG SIP Trunk Service. In the sample configuration, the single digit 0 is used as the ARS access code. Avaya telephone users will dial 0 to reach an outside line. Use the **change feature-access-codes** command to configure 0 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: 0     Access Code 2: 9
                 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 0. 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        pubu         n
    00                   11    15    1        pubu         n
    9                    9     9     1        pubu         n
    6                    9     9     1        pubu         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.

```
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                                          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 Telefonica 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 Telefonica correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers 900003895-900003899 to a 4 digit extension by deleting **5** of the incoming digits which leaves the administered 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    9   9             5
```

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 Avaya Aura® Session Manager. The Avaya Aura® Session Manager is configured via the Avaya Aura® System Manager. The procedures include the following areas:

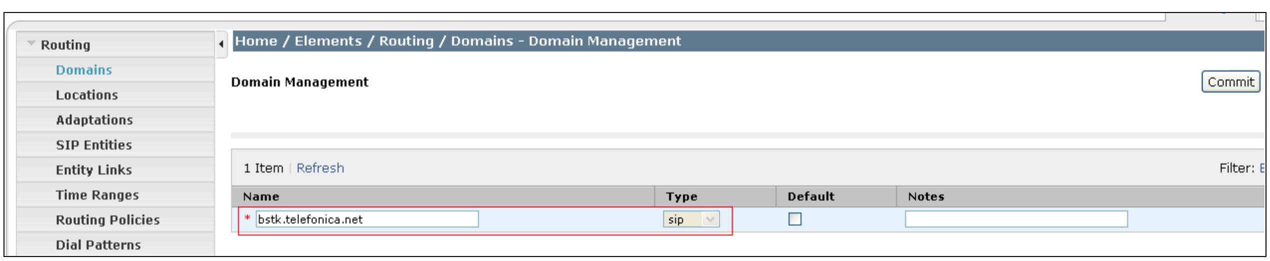
- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Communication Manager as Managed Element
- Administer Application for Avaya Aura® Communication Manager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

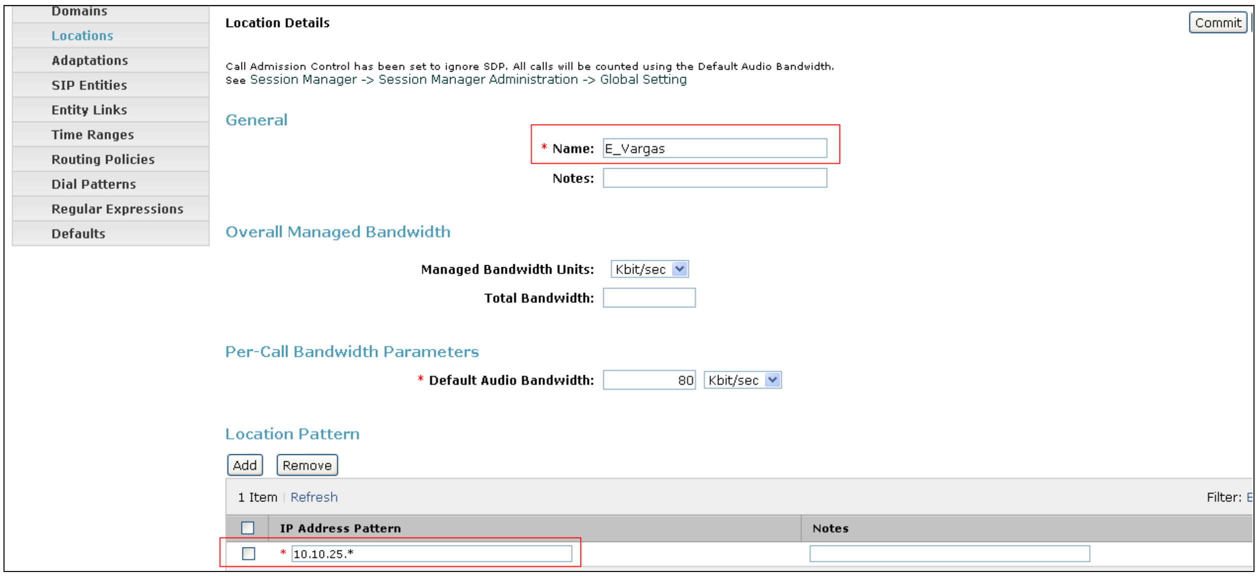
6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu (not shown) and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **bstk.telefonica.net** and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes (not shown).



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.



6.4. Administer SIP Entities

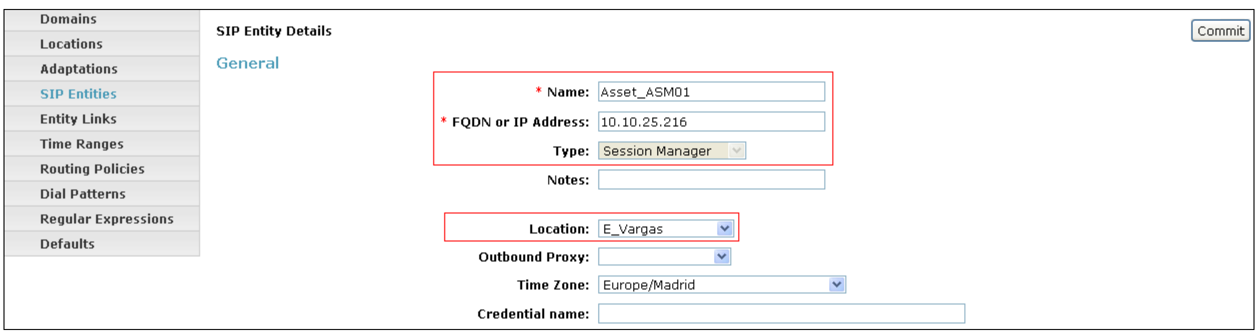
A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity. Under **General:**

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field either enter the IP address of Session Manager (when adding the Session Manager SIP entity) or the signaling interface of 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.

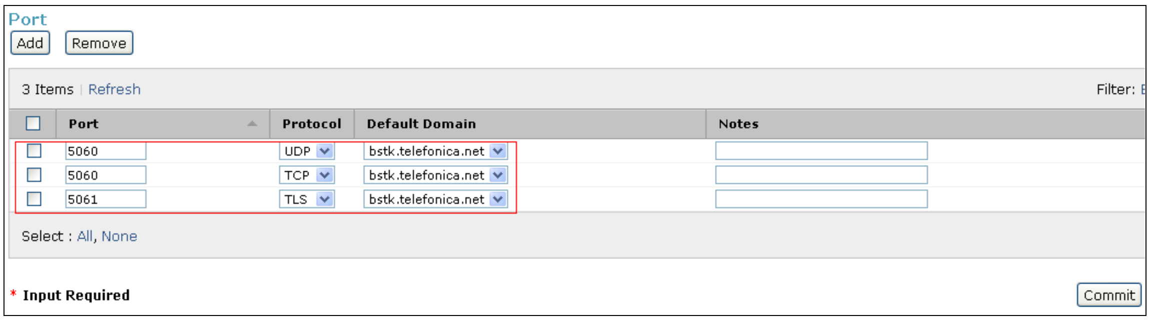
- Session Manager SIP Entity
- Communication Manager SIP Entity
- Acme Packet SBC SIP Entity

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.



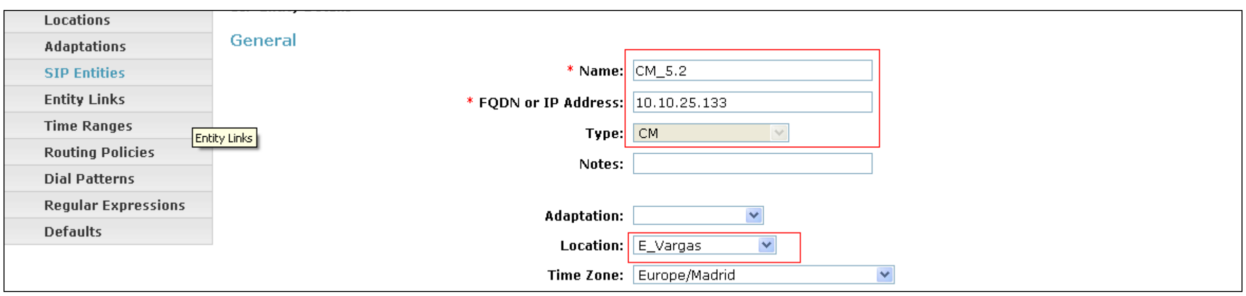
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row.

- 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 **bstk.telefonica.net** as the default domain.



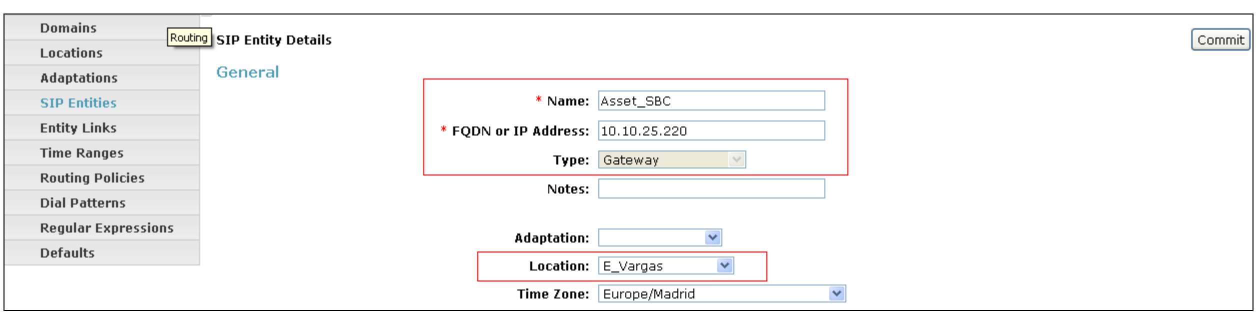
6.4.1. Avaya Aura® Communication Manager SIP Entity

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 on Communication Manager.



6.4.2. Acme Packet SBC SIP Entities

Each SBC used by Telefonica 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 present in the enterprise configuration.

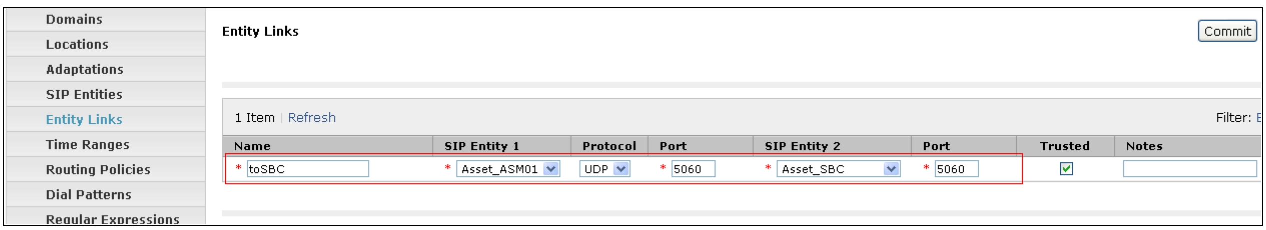


6.5. Administer Entity Links

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 the Session Manager entity**.**
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4.**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select the **Trusted** tick box to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.

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



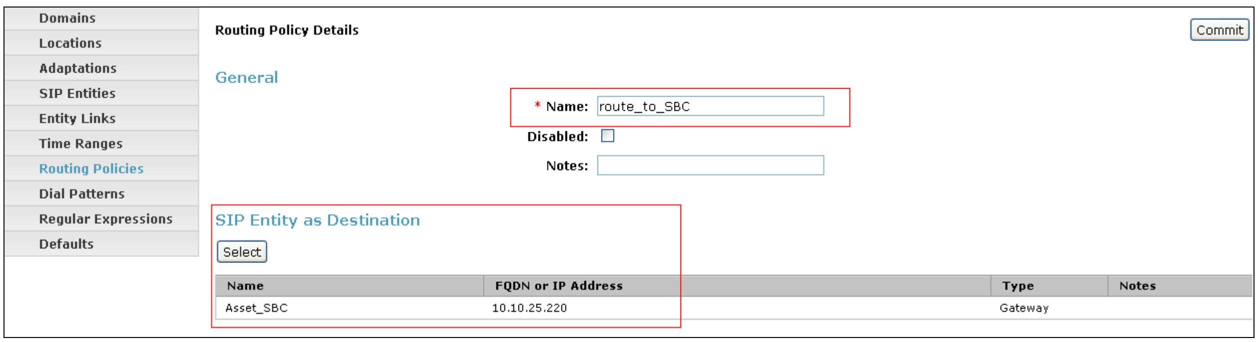
6.6. Administer Routing Policies

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 the Acme Packet SBC.



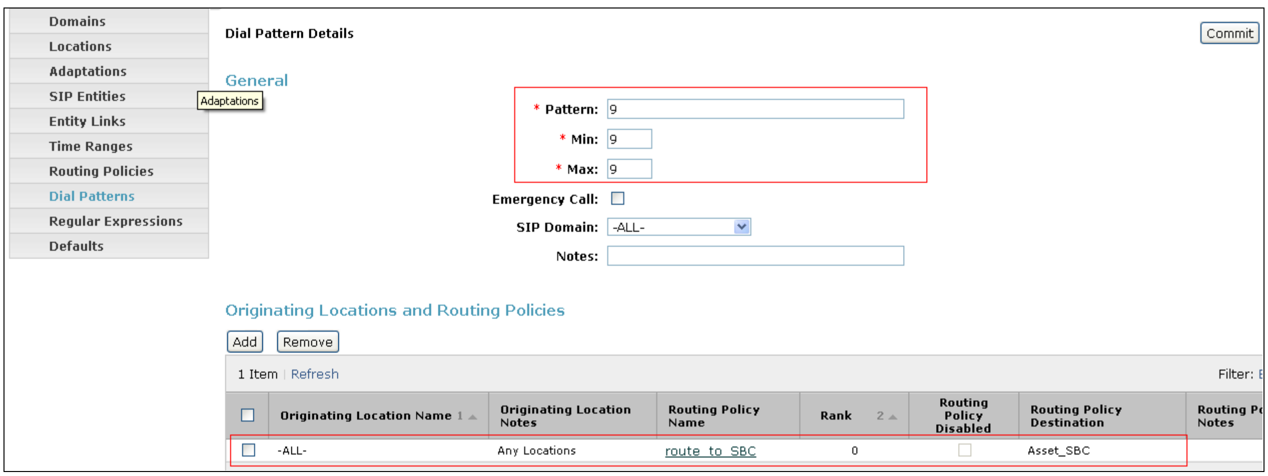
6.7. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

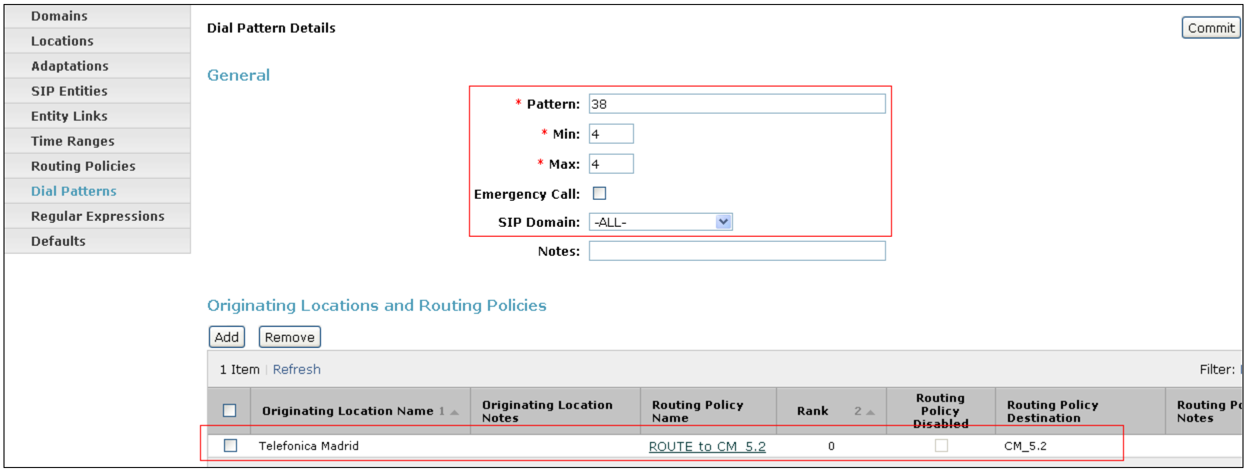
Under **General:**

- In the **Pattern** field enter a dialed number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialed number.
- In the **Max** field enter the maximum length of the dialed number.
- In the **SIP Domain** field select **-ALL-.**

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 6.6.** Click the **Select** button to save (not shown). The following screen shows an example dial pattern configured for Telefonica BTNG SIP Trunk Service.



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



7. Configure Acme Packet 3800 Net-Net Session Director

This section describes the configuration of the Acme Packet Net-Net 3800 SBC. The Acme Packet Session Director was configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet Session Director. This section does not cover the Acme Packet configuration in its entirety, only the fields directly related to the compliance test will be covered. For completeness the running configuration used during the compliance testing is displayed in **Appendix A.**

7.1. Accessing Acme Packet 3800 Net-Net Session Director

Connect to the Acme Packet session director and login with the appropriate username and password. At the prompt enter the **enable** command and then the superuser password. Once in superuser mode enter the command **configure terminal** to enter configuration mode.

7.2. System Configuration

The system configuration defines system-wide parameters for the Acme Packet Session Director. Access the **system-config** element and set the following element parameters:

- **default-gateway**: The IP address of the default gateway for the Acme Packet Session Director. In this case, the default gateway is **10.10.25.129**.
- **source-routing**: Should be set to **enabled.**

```
system-config
        hostname
        description
        location

      < text removed for brevity >

       call-trace                     disabled
      internal-trace                  disabled
      log-filter                      all
      default-gateway                 10.10.25.129
      restart                         enabled
      exceptions
      telnet-timeout                  0
      console-timeout                 0
      remote-control                  enabled
      cli-audit-trail                 enabled
      link-redundancy-state           disabled
      source-routing                  enabled
      cli-more                        disabled
      terminal-height                 24
      < text removed for brevity >
```

7.3. Physical Interfaces

During the compliance test, the Ethernet interface slot 0 / port 0 of the Acme Packet Session Director was connected to the outside, untrusted network. Ethernet slot 1 / port 1 was connected to the inside, enterprise network. A network interface was defined for each physical interface to assign it a routable IP address. Access the **phy-interface** element and set the following element parameters:

- **name**: A descriptive string used to reference the Ethernet interface.
- **operation-type**: Set to **Media** to indicate both signalling and media packets are sent on this interface.
- **slot / port**: The identifier of the specific Ethernet interface used.

```
phy-interface
        name                            s0p0
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-by                admin@console
        last-modified-date              2009-11-18 07:58:36
phy-interface
        name                            s1p1
        operation-type                  Media
        port                            1
        slot                            1
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode
        speed
        last-modified-by                admin@192.168.0.2
        last-modified-date              2010-09-30 06:30:39
```

7.4. Network Interfaces

Access the **network-interface** element and set the following element parameters:

- **name**: The name of the physical interface defined in **Section 7.3.**
- **ip-address**: The IPv4 address assigned to this interface.
- **netmask**: Subnet mask for the IP subnet.
- **gateway**: The subnet gateway address.
- **hip-ip-list**: The virtual IP address assigned to the Acme Packet Session Director on this interface.
- **icmp-address**: The list of IP addresses which the Acme Packet Session Director will answer ICMP requests on this interface.

The settings for the inside, enterprise side network interface are shown below

```
network-interface
        name                            s1p1
        sub-port-id                     0
        description                     packet-trace
        hostname
        ip-address                      10.10.25.220
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         10.10.25.129
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list                     10.10.25.220
        ftp-address
         icmp-address                    10.10.25.220
        snmp-address
        telnet-address
        last-modified-by                admin@192.168.0.2
        last-modified-date              2010-09-30 06:32:29
```

The settings for the outside, untrusted network interface are shown below.

```
network-interface
        name                            s0p0
        sub-port-id                     0
        description                     SIPTrunkSide
        hostname
        ip-address                      10.10.25.21
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         10.10.25.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list                     10.10.25.21
        ftp-address                     10.10.25.21
         icmp-address                    10.10.25.21
        snmp-address
        telnet-address                  10.10.25.21
        last-modified-by                admin@192.168.0.2
        last-modified-date              2009-11-18 09:59:57
```

7.5. Realm

A realm represents a group of related Acme Packet Session Director components. Two realms were defined for the compliance test. The **access-noas** realm was defined for the external untrusted network and the **core-noas** realm was defined for the internal enterprise network. Access the **realm-config** element and set the following element parameters:

- **identifier**: A descriptive string used to reference the realm.
- **network interfaces**: The network interfaces located in this realm.

```
realm-config
       identifier                      INSIDE
       description                     AvayaSide
       addr-prefix                     0.0.0.0
       network-interfaces
                                       s1p1:0
       mm-in-realm                     enabled
       mm-in-network                   enabled

< text removed for brevity >

realm-config
       identifier                      OUTSIDE
       description                     SIPTrunk
       addr-prefix                     0.0.0.0
       network-interfaces
                                       s0p0:0
       mm-in-realm                     enabled
       mm-in-network                   enabled

< text removed for brevity >
```

7.6. SIP Interface

The SIP interface defines the ip address and port upon which the Acme Packet Session Director receives and sends SIP messages. Two SIP interfaces were defined; one for each realm. Access the **sip-interface** element and set the following element parameters:

- **realm-id**: The name of the realm to which this interface is assigned.
- **sip port:**
  - **address**: The IP address assigned to this sip-interface.
  - **port**: The port assigned to this sip-interface.
  - **transport-protocol**: The transport method used for this interface.
  - **allow-anonymous:** Defines from whom SIP requests will be allowed. The value of **agents-only** means SIP requests will only be accepted on this interface from session agents defined in **Section 7.8**.
- **trans-expire:** The time to live in seconds for SIP transactions, this setting controls timers B, F, H and TEE specified in RFC 3261. A value of **0** indicates the timers in the **sip-config (Section 7.6)** will be used.
- **invite expire:** The time to live in seconds for SIP transactions that have received a provisional response. A value of **0** indicates the timers in the **sip-config** section will be used.

```
sip-interface
       state                        enabled
       realm-id                     INSIDE
       description
       sip-port
              address                      10.10.25.220
              port                         5060
              transport-protocol           UDP
              tls-profile
              allow-anonymous              agents-only
              ims-aka-profile
       carriers
       trans-expire                 0
       invite-expire                0

< text removed for brevity >

sip-interface
       state                        enabled
       realm-id                     OUTSIDE
       description
       sip-port
              address                      10.10.25.21
              port                         5060
              transport-protocol           UDP
              tls-profile
              allow-anonymous              agents-only
              ims-aka-profile
       carriers
       trans-expire                 0
       invite-expire                0

< text removed for brevity >
```

7.7. Session Agent

A session agent defines the characteristics of a signalling peer to the Acme Packet Session Director such as Session Manager. Access the **session-agent** element and set the following element parameters:

- **hostname**: Fully qualified domain name or IP address of the SIP peer.
- **ip-address**: IP address of the SIP peer.
- **port**: The port used by the peer for SIP traffic.
- **app-protocol**: Is set to **SIP.**
- **transport-method**: The transport method used for this session agent.
- **realm-id**: The realm id where the peer resides.
- **description**: A descriptive name for the peer.
- **ping-method**: This setting enables SIP OPTIONS to be sent to the peer to verify that the SIP connection is functional and sets the value that will be used in the SIP Max-Forward field. As an example, an entry of **OPTIONS;hops=66** would generate OPTIONS messages with a Max Forwards value of 66.
- **ping-interval**: Specifies the interval (in seconds) between each ping attempt.
- **ping-in-service-response-codes:** A list of response codes that the session agent will accept in response to ping requests in order for the session agent to remain in service.
- **in-manipulationid:** The name of the SIP header manipulation to apply to inbound SIP packets.
- **out-manipulationid:** The name of the SIP header manipulation to apply to outbound SIP packets.

The settings for the session agent on the private enterprise side are shown below.

```
session-agent
       hostname                         10.10.25.216
       ip-address                       10.10.25.216
       port                             5060
       state                            enabled
       app-protocol                     SIP
       app-type
       transport-method                 UDP
       realm-id                         INSIDE
       egress-realm-id
       description                      AvayaAsset
< text removed for brevity >

        response-map
       ping-method
       ping-interval                    0
       ping-send-mode                   keep-alive
       ping-in-service-response-codes
< text removed for brevity >

         li-trust-me                     disabled
       in-manipulationid
       out-manipulationid
       trunk-group
< text removed for brevity >
```

The settings for the session agent relating to Telefonica NGN are shown below.

```
session-agent
       hostname                         10.10.5.23
       ip-address                       10.10.5.23
       port                             5060
       state                            enabled
       app-protocol                     SIP
       app-type
       transport-method                 UDP
       realm-id                         OUTSIDE
       egress-realm-id
       description                      SIPTrunk1
       carriers

< text removed for brevity >
        response-map
       ping-method                      OPTIONS;hops=0
       ping-interval                    10
       ping-send-mode                   keep-alive
       ping-in-service-response-codes 483

< text removed for brevity >
        in-manipulationid
       out-manipulationid               manip-out
       manipulation-string

< text removed for brevity >
```

The settings for the session agent relating to Telefonica NGN2 are shown below.

```
session-agent
       hostname                          10.10.5.123
       ip-address                        10.10.5.123
       port                              5060
       state                             enabled
       app-protocol                      SIP
       app-type
       transport-method                  UDP
       realm-id                          OUTSIDE
       egress-realm-id
       description                       SIPTrunk2
       carriers
< text removed for brevity >

        response-map
       ping-method                       OPTIONS;hops=0
       ping-interval                     10
       ping-send-mode                    keep-alive
       ping-in-service-response-codes 483
< text removed for brevity >

        li-trust-me                       disabled
       in-manipulationid
       out-manipulationid                manip-out
       manipulation-string
< text removed for brevity >
```

7.8. Session Agent Group

Where multiple session agents exist, a session group is used to define a list of session agents and the hunting order for the defined session agents. Access the **session-group** element and set the following element parameters:

- **group-name:** A descriptive string used to reference the Session Agent Group (SAG).
- **app-protocol:** Set to **SIP.**
- **strategy:** Defines the method for hunting through the defined session agents, the default value is **Hunt.**
- **dest:** a list of the session agents available to the session agent group in priority order.

```
session-group
        group-name                      OUTSIDE-SAG
        description                     SIPTrunk
        state                           enabled
        app-protocol                    SIP
        strategy                        Hunt
        dest
                                        10.10.5.23
                                        10.10.5.123
        trunk-group
        sag-recursion                   disabled
        stop-sag-recurse                401,407
        last-modified-by                admin@192.168.0.2
        last-modified-date              2009-11-20 09:29:13
session-group
        group-name                      INSIDE-SAG
        description                     AvayaAsset
        state                           enabled
        app-protocol                    SIP
        strategy                        Hunt
        dest
                                        10.10.25.216
                                        10.10.25.217
        trunk-group
        sag-recursion                   disabled
        stop-sag-recurse                401,407
        last-modified-by                admin@192.168.0.2
        last-modified-date              2010-09-30 05:30:04
```

7.9. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages. During the compliance test two sip manipulations were used; these were assigned to session agents in **Section 7.7**. Multiple header rules can exist for each sip manipulation. Only the first sip manipulation and first header rule within that sip manipulation will be discussed in this section, the additional header rules and additional sip manipulations can be observed in **Appendix A.**

Access the **sip-manipulation** element and set the following element parameters:

- **name**: A descriptive string used to reference the sip manipulation.
- **header-rule**:
  - **name**: The name of this individual header rule.
  - **header-name**: The SIP header to be modified.
  - **action**: The action to be performed on the header.
  - **comparison-type**: The type of comparison performed when determining a match.
  - **msg-type**: The type of message to which this rule applies.
  - **element-rule**:
    - **name:** The name of this individual element rule.
    - **type:** Defines the particular element in the header to be modified.
    - **action:** The action to be performed on the element.
    - **match-val-type**: The type of value to be matched. If the default value of **any** is used then the sip message is compared with the **match value** field.
    - **comparison-type**: The type of comparison performed when determining a match.
    - **match-value**: The value to be matched
    - **new-value**: The new value to be used .

In the example below the sip manipulation **manip-out** is shown , the first header rule called **manipFrom** specifies the from header in sip request messages will be manipulated based on the element rule defined. The element rule called **From** specifies that the host part of the URI in the from header should be replaced with the Value **$LOCAL_IP**. The Value **$LOCAL_IP** is the IP address of the SIP interface that the SIP message is being sent from.

```
sip-manipulation
        name                                manip-out
        description
        header-rule
                name                                manipFrom
                header-name                         From
                action                              manipulate
                comparison-type                     case-sensitive
                match-value
                msg-type                            request
                new-value
                methods
                element-rule
                        name                                FROM
                        parameter-name
                        type                                uri-host
                        action                              replace
```

```
                     match-val-type                  any
                     comparison-type                 case-sensitive
                     match-value
                     new-value                       $LOCAL_IP
< text removed for brevity >
```

7.10. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools are defined; one for each realm. Access the **steering-pool** element and set the following element parameters:

- **ip-address:** The address of the interface on the Acme Packet Session Director.
- **start-port:** The port number that begins the range.
- **end-port:** The port number that ends the range.
- **realm-id:** The realm to which this steering pool is assigned.

```
steering-pool
        ip-address                      10.10.25.220
        start-port                      20000
        end-port                        29999
        realm-id                        INSIDE
        network-interface               s1p1:0
        last-modified-by                admin@192.168.0.2
        last-modified-date              2010-09-30 06:33:30
steering-pool
        ip-address                      10.10.25.21
        start-port                      30000
        end-port                        39999
        realm-id                        OUTSIDE
        network-interface               s0p0:0
        last-modified-by                admin@console
        last-modified-date              2009-11-18 08:19:41
```

7.11. Local Policy

Local policy controls the routing of SIP calls from one realm to another. Access the **local-policy** element and set the following element parameters:

- **from-address**: The originating IP address to which this policy applies. An asterisk * indicates any IP address.
- **to-address**: The destination IP address to which this policy applies. An asterisk * indicates any IP address.
- **source-realm**: The realm from which traffic is received.
- **policy-attribute**:
    - **next-hop**: The session agent or session agent group where the message should be sent when the policy rules match.
    - **realm**: The egress realm associated with the next-hop.

The settings for the first local-policy are shown below. The first policy indicates that messages originating from the **INSIDE** realm are to be sent to the **OUTSIDE** realm using the SAG defined in **Section 7.8.**

```
local-policy
       from-address
                                 *
       to-address
                                 *
       source-realm
                                 INSIDE
       description
       activate-time             N/A
       deactivate-time           N/A
       state                     enabled
       policy-priority           none
       last-modified-by          admin@192.168.0.2
       last-modified-date        2009-11-18 10:09:18
       policy-attribute
              next-hop                 SAG:OUTSIDE-SAG
              realm                    OUTSIDE
              action                   none
              terminate-recursion      disabled
              carrier
              start-time               0000
              end-time                 2400
              days-of-week             U-S
              cost                     0
              app-protocol             SIP
              state                    enabled
              methods
              media-profiles
```

The settings for the second **local-policy** are shown below. This policy indicates that messages originating from the **OUTSIDE** realm are to be sent to the **INSIDE** realm using the SAG created in **Section 7.8**.

```
local-policy
        from-address
                                      *
        to-address
                                      *
        source-realm
                                      OUTSIDE
        description
        activate-time                 N/A
        deactivate-time               N/A
        state                         enabled
        policy-priority               none
        last-modified-by              admin@192.168.0.2
        last-modified-date            2010-09-30 05:32:31
        policy-attribute
                next-hop                      SAG:INSIDE-SAG
                realm                         INSIDE
                action                        none
                terminate-recursion           disabled
                carrier
                start-time                    0000
                end-time                      2400
                days-of-week                  U-S
                cost                          0
                app-protocol                  SIP
                state                         enabled
                methods
                media-profiles
```

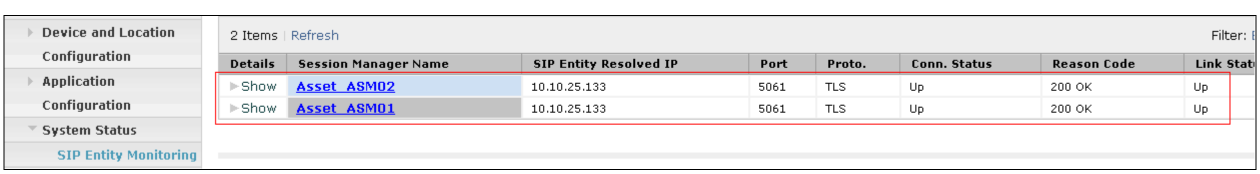
8. Telefonica Configuration

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

9. Verification Steps

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

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



Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Stat
Show	Asset_ASM02	10.10.25.133	5061	TLS	Up	200 OK	Up
Show	Asset_ASM01	10.10.25.133	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.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager Access Element and Avaya Aura® Session Manager to Telefonica BTNG SIP Trunk Service. Telefonica BTNG SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. 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.

[5] *Installing and Upgrading Avaya Aura® System ManagerRelease6.1*, 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/

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.

Appendix A: Acme Packet Session Director Configuration File

Included below is the Acme Packet Session Director configuration file used during the compliance testing. The contents of the configuration can be shown by using the **show running-config** command.

show run
local-policy
    from-address
        *
    to-address
        *
    source-realm
        INSIDE
    description
    activate-time N/A
    deactivate-time N/A
    state enabled
    policy-priority none
    last-modified-by admin@192.168.0.2
    last-modified-date 2009-11-18 10:09:18
    policy-attribute
        next-hop SAG:OUTSIDE-SAG
        realm OUTSIDE
        action none
        terminate-recursion disabled
        carrier
        start-time 0000
        end-time 2400
        days-of-week U-S
        cost 0
        app-protocol SIP
        state enabled
        methods
        media-profiles
local-policy
    from-address
        *
    to-address
        *
    source-realm
        OUTSIDE
    description
    activate-time N/A
    deactivate-time N/A

```
        state                     enabled
        policy-priority           none
        last-modified-by          admin@192.168.0.2
        last-modified-date        2010-09-30 05:32:31
        policy-attribute
                next-hop                  SAG:INSIDE-SAG
                realm                     INSIDE
                action                    none
                terminate-recursion       disabled
                carrier
                start-time                0000
                end-time                  2400
                days-of-week              U-S
                cost                      0
                app-protocol              SIP
                state                     enabled
                methods
                media-profiles
media-manager
        state                     enabled
        latching                  enabled
        flow-time-limit           86400
        initial-guard-timer       300
        subsq-guard-timer         300
        tcp-flow-time-limit       86400
        tcp-initial-guard-timer   300
        tcp-subsq-guard-timer     300
        tcp-number-of-ports-per-flow   2
        hnt-rtcp                  disabled
        algd-log-level            NOTICE
        mbcd-log-level            NOTICE
        red-flow-port             1985
        red-mgcp-port             1986
        red-max-trans             10000
        red-sync-start-time       5000
        red-sync-comp-time        1000
        media-policing            enabled
        max-signaling-bandwidth   775880
        max-untrusted-signaling   5
        min-untrusted-signaling   4
        app-signaling-bandwidth   0
        tolerance-window          30
        rtcp-rate-limit           0
        min-media-allocation      32000
        min-trusted-allocation    1000
        deny-allocation           1000
```

```
        anonymous-sdp                disabled
        arp-msg-bandwidth            32000
        fragment-msg-bandwidth       0
        rfc2833-timestamp            disabled
        default-2833-duration        100
        rfc2833-end-pkts-only-for-non-sig enabled
        translate-non-rfc2833-event  disabled
        dnsalg-server-failover       disabled
        last-modified-by             admin@console
        last-modified-date           2009-11-18 07:58:07
network-interface
        name                         s0p0
        sub-port-id                  0
        description                  SIPTrunkSide
        hostname
        ip-address                   10.10.25.21
        pri-utility-addr
        sec-utility-addr
        netmask                      255.255.255.128
        gateway                      10.10.25.1
        sec-gateway
        gw-heartbeat
                state                disabled
                heartbeat            0
                retry-count          0
                retry-timeout        1
                health-score         0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                  11
      hip-ip-list                    10.10.25.21
        ftp-address                  10.10.25.21
      icmp-address                   10.10.25.21
        snmp-address
        telnet-address               10.10.25.21
        last-modified-by             admin@192.168.0.2
        last-modified-date           2009-11-18 09:59:57
network-interface
        name                         s1p1
        sub-port-id                  0
        description                  packet-trace
        hostname
        ip-address                   10.10.25.220
        pri-utility-addr
```

sec-utility-addr
netmask 255.255.255.128
gateway 10.10.25.129
sec-gateway
gw-heartbeat
state disabled
heartbeat 0
retry-count 0
retry-timeout 1
health-score 0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list 10.10.25.220
ftp-address
icmp-address 10.10.25.220
snmp-address
telnet-address
last-modified-by admin@192.168.0.2
last-modified-date 2010-09-30 06:32:29
phy-interface
name s0p0
operation-type Media
port 0
slot 0
virtual-mac
admin-state enabled
auto-negotiation enabled
duplex-mode FULL
speed 100
last-modified-by admin@console
last-modified-date 2009-11-18 07:58:36
phy-interface
name s1p1
operation-type Media
port 1
slot 1
virtual-mac
admin-state enabled
auto-negotiation enabled
duplex-mode
speed
last-modified-by admin@192.168.0.2
last-modified-date 2010-09-30 06:30:39

realm-config

identifier **INSIDE**
description AvayaSide
addr-prefix 0.0.0.0
network-interfaces
s1p1:0
mm-in-realm enabled
mm-in-network enabled
mm-same-ip enabled
mm-in-system disabled
bw-cac-non-mm disabled
msm-release disabled
qos-enable disabled
generate-UDP-checksum disabled
max-bandwidth 0
fallback-bandwidth 0
max-priority-bandwidth 0
max-latency 0
max-jitter 0
max-packet-loss 0
observ-window-size 0
parent-realm
dns-realm
media-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
class-profile
average-rate-limit 0
access-control-trust-level none
invalid-signal-threshold 0
maximum-signal-threshold 0
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period 30
ext-policy-svr
symmetric-latching disabled
pai-strip disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching none
restriction-mask 32

```
        accounting-enable             enabled
        user-cac-mode                 none
        user-cac-bandwidth            0
        user-cac-sessions             0
        icmp-detect-multiplier        0
        icmp-advertisement-interval   0
        icmp-target-ip
        monthly-minutes               0
        net-management-control        disabled
        delay-media-update            disabled
        refer-call-transfer           disabled
        codec-policy
        codec-manip-in-realm          disabled
        constraint-name
        call-recording-server-id
        stun-enable                   disabled
        stun-server-ip                0.0.0.0
        stun-server-port              3478
        stun-changed-ip               0.0.0.0
        stun-changed-port             3479
        match-media-profiles
        qos-constraint
        last-modified-by              admin@192.168.0.2
        last-modified-date            2010-09-30 06:33:16
realm-config
        identifier                    OUTSIDE
        description                   SIPTrunk
        addr-prefix                   0.0.0.0
        network-interfaces
                                      s0p0:0
        mm-in-realm                   enabled
        mm-in-network                 enabled
        mm-same-ip                    enabled
        mm-in-system                  disabled
        bw-cac-non-mm                 disabled
        msm-release                   disabled
        qos-enable                    disabled
        generate-UDP-checksum         disabled
        max-bandwidth                 0
        fallback-bandwidth            0
        max-priority-bandwidth        0
        max-latency                   0
        max-jitter                    0
        max-packet-loss               0
        observ-window-size            0
        parent-realm
```

```
dns-realm
media-policy
in-translationid              rules-in
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
class-profile
average-rate-limit            0
access-control-trust-level    none
invalid-signal-threshold      0
maximum-signal-threshold      0
untrusted-signal-threshold    0
nat-trust-threshold           0
deny-period                   30
ext-policy-svr
symmetric-latching            disabled
pai-strip                     disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching           none
restriction-mask              32
accounting-enable             enabled
user-cac-mode                 none
user-cac-bandwidth            0
user-cac-sessions             0
icmp-detect-multiplier        0
icmp-advertisement-interval   0
icmp-target-ip
monthly-minutes               0
net-management-control        disabled
delay-media-update            disabled
refer-call-transfer           disabled
codec-policy
codec-manip-in-realm          disabled
constraint-name
call-recording-server-id
stun-enable                   disabled
stun-server-ip                0.0.0.0
stun-server-port              3478
stun-changed-ip               0.0.0.0
stun-changed-port             3479
match-media-profiles
qos-constraint
```

last-modified-by admin@10.10.25.141
last-modified-date 2009-11-25 12:15:32
session-agent
hostname 10.10.5.23
ip-address 10.10.5.23
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id OUTSIDE
egress-realm-id
description SIPTrunk1
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing enabled
send-media-session enabled
response-map
ping-method OPTIONS;hops=0
ping-interval 10
ping-send-mode keep-alive
ping-in-service-response-codes 483
out-service-response-codes
media-profiles
in-translationid
out-translationid

```
        trust-me                    disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                 disabled
        in-manipulationid
        out-manipulationid          manip-out
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate   0
        early-media-allow
        invalidate-registrations    disabled
        rfc2833-mode                none
        rfc2833-payload             0
        codec-policy
        enforcement-profile
        refer-call-transfer         disabled
        reuse-connections           NONE
        tcp-keepalive               none
        tcp-reconn-interval         0
        max-register-burst-rate     0
        register-burst-window       0
        last-modified-by            admin@192.168.0.2
        last-modified-date          2009-11-20 11:46:45
session-agent
        hostname                    10.10.25.216
        ip-address                  10.10.25.216
        port                        5060
        state                       enabled
        app-protocol                SIP
        app-type
        transport-method            UDP
        realm-id                    INSIDE
        egress-realm-id
        description                 AvayaAsset
        carriers
        allow-next-hop-lp           enabled
        constraints                 disabled
        max-sessions                0
        max-inbound-sessions        0
        max-outbound-sessions       0
        max-burst-rate              0
        max-inbound-burst-rate      0
```

```
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method
ping-interval                  0
ping-send-mode                 keep-alive
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                       disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                    disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
```

tcp-keepalive none
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
last-modified-by admin@192.168.0.2
last-modified-date 2010-09-30 05:26:16

session-agent

hostname 10.10.5.123
ip-address 10.10.5.123
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id OUTSIDE
egress-realm-id
description SIPTrunk2
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing enabled
send-media-session enabled
response-map
ping-method OPTIONS;hops=0
ping-interval 10
ping-send-mode keep-alive
ping-in-service-response-codes 483

```
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                      disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                   disabled
        in-manipulationid
        out-manipulationid            manip-out
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate     0
        early-media-allow
        invalidate-registrations      disabled
        rfc2833-mode                  none
        rfc2833-payload               0
        codec-policy
        enforcement-profile
        refer-call-transfer           disabled
        reuse-connections             NONE
        tcp-keepalive                 none
        tcp-reconn-interval           0
        max-register-burst-rate       0
        register-burst-window         0
        last-modified-by              admin@192.168.0.2
        last-modified-date            2009-11-20 11:47:02
session-agent
        hostname                      10.10.25.217
        ip-address                    10.10.25.217
        port                          5060
        state                         enabled
        app-protocol                  SIP
        app-type
        transport-method              UDP
        realm-id                      INSIDE
        egress-realm-id
        description                   AvayaAsset2
        carriers
        allow-next-hop-lp             enabled
        constraints                   disabled
        max-sessions                  0
```

```
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method
ping-interval                  0
ping-send-mode                 keep-alive
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                       disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                    disabled
in-manipulationid
out-manipulationid
manipulation-string
p-asserted-id
trunk-group
max-register-sustain-rate      0
early-media-allow
invalidate-registrations       disabled
rfc2833-mode                   none
rfc2833-payload                0
```

codec-policy
enforcement-profile
refer-call-transfer disabled
reuse-connections NONE
tcp-keepalive none
tcp-reconn-interval 0
max-register-burst-rate 0
register-burst-window 0
last-modified-by admin@192.168.0.2
last-modified-date 2010-09-30 05:27:07

session-group
group-name **OUTSIDE-SAG**
description SIPTrunk
state enabled
app-protocol SIP
strategy Hunt
dest
10.10.5.23
10.10.5.123
trunk-group
sag-recursion disabled
stop-sag-recurse 401,407
last-modified-by admin@192.168.0.2
last-modified-date 2009-11-20 09:29:13

session-group
group-name **INSIDE-SAG**
description AvayaAsset
state enabled
app-protocol SIP
strategy Hunt
dest
10.10.25.216
10.10.25.217
trunk-group
sag-recursion disabled
stop-sag-recurse 401,407
last-modified-by admin@192.168.0.2
last-modified-date 2010-09-30 05:30:04

session-translation
id rules-in
rules-calling deleteplus34
rules-called deleteplus34
last-modified-by admin@192.168.0.2
last-modified-date 2009-11-20 11:24:38

translation-rules
id deleteplus34

```
        type                    delete
        add-string
        add-index               0
        delete-string           +34
        delete-index            0
        last-modified-by        admin@192.168.0.2
        last-modified-date      2009-11-20 11:25:14
sip-config
        state                   enabled
        operation-mode          dialog
        dialog-transparency     enabled
        home-realm-id
        egress-realm-id
        nat-mode                None
        registrar-domain
        registrar-host
        registrar-port          0
        register-service-route  always
        init-timer              500
        max-timer               4000
        trans-expire            32
        invite-expire           180
        inactive-dynamic-conn   32
        enforcement-profile
        pac-method
        pac-interval            10
        pac-strategy            PropDist
        pac-load-weight         1
        pac-session-weight      1
        pac-route-weight        1
        pac-callid-lifetime     600
        pac-user-lifetime       3600
        red-sip-port            1988
        red-max-trans           10000
        red-sync-start-time     5000
        red-sync-comp-time      1000
        add-reason-header       disabled
        sip-message-len         4096
        enum-sag-match          disabled
        extra-method-stats      disabled
        registration-cache-limit 0
        register-use-to-for-lp  disabled
        options                 max-udp-length=0
        add-ucid-header         disabled
        last-modified-by        admin@console
        last-modified-date      2009-11-18 08:11:42
```

```
sip-interface
        state                       enabled
        realm-id                    INSIDE
        description
        sip-port
                address                     10.10.25.220
                port                        5060
                transport-protocol          UDP
                tls-profile
                allow-anonymous             agents-only
                ims-aka-profile
        carriers
        trans-expire                0
        invite-expire               0
        max-redirect-contacts       0
        proxy-mode
        redirect-action
        contact-mode                none
        nat-traversal               none
        nat-interval                30
        tcp-nat-interval            90
        registration-caching        disabled
        min-reg-expire              300
        registration-interval       3600
        route-to-registrar          disabled
        secured-network             disabled
        teluri-scheme               disabled
        uri-fqdn-domain             bstk.telefonica.net
        trust-mode                  all
        max-nat-interval            3600
        nat-int-increment           10
        nat-test-increment          30
        sip-dynamic-hnt             disabled
        stop-recurse                401,407
        port-map-start              0
        port-map-end                0
        in-manipulationid           manip-in
        out-manipulationid
        manipulation-string
        sip-ims-feature             disabled
        operator-identifier
        anonymous-priority          none
        max-incoming-conns          0
        per-src-ip-max-incoming-conns 0
        inactive-conn-timeout       0
        untrusted-conn-timeout      0
```

```
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode          pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                none
        implicit-service-route        disabled
        rfc2833-payload               101
        rfc2833-mode                  transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature               disabled
        enforcement-profile
        refer-call-transfer           disabled
        route-unauthorized-calls
        tcp-keepalive                 none
        add-sdp-invite                disabled
        add-sdp-profiles
        last-modified-by              admin@192.168.0.2
        last-modified-date            2010-09-30 05:16:28
sip-interface
        state                         enabled
        realm-id                      OUTSIDE
        description
        sip-port
                address                       10.10.25.21
                port                          5060
                transport-protocol            UDP
                tls-profile
                allow-anonymous               agents-only
                ims-aka-profile
        carriers
        trans-expire                  0
        invite-expire                 0
        max-redirect-contacts         0
        proxy-mode
        redirect-action
        contact-mode                  none
        nat-traversal                 none
        nat-interval                  30
        tcp-nat-interval              90
        registration-caching          disabled
        min-reg-expire                300
```

```
registration-interval          3600
route-to-registrar             disabled
secured-network                disabled
teluri-scheme                  disabled
uri-fqdn-domain
trust-mode                     all
max-nat-interval               3600
nat-int-increment              10
nat-test-increment             30
sip-dynamic-hnt                disabled
stop-recurse                   401,407
port-map-start                 0
port-map-end                   0
in-manipulationid
out-manipulationid
manipulation-string
sip-ims-feature                disabled
operator-identifier
anonymous-priority             none
max-incoming-conns             0
per-src-ip-max-incoming-conns  0
inactive-conn-timeout          0
untrusted-conn-timeout         0
network-id
ext-policy-server
default-location-string
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
term-tgrp-mode                 none
implicit-service-route         disabled
rfc2833-payload                101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
ims-aka-feature                disabled
enforcement-profile
refer-call-transfer            disabled
route-unauthorized-calls
tcp-keepalive                  none
add-sdp-invite                 disabled
add-sdp-profiles
last-modified-by               admin@192.168.0.2
last-modified-date             2010-09-30 06:15:38
```

sip-manipulation
name **manip-out**
description
header-rule
name **manipFrom**
header-name **From**
action **manipulate**
comparison-type case-sensitive
match-value
msg-type request
new-value
methods
element-rule
name **FROM**
parameter-name
type **uri-host**
action **replace**
match-val-type **any**
comparison-type **case-sensitive**
match-value
new-value **$LOCAL_IP**
header-rule
name **manipTo**
header-name To
action manipulate
comparison-type case-sensitive
match-value
msg-type request
new-value
methods
element-rule
name **TO**
parameter-name
type **uri-host**
action **replace**
match-val-type **any**
comparison-type **case-sensitive**
match-value
new-value **$REMOTE_IP**
last-modified-by admin@192.168.0.2
last-modified-date 2009-11-20 11:52:14
sip-manipulation
name manip-in
description
header-rule
name delHistory-Info

```
            header-name             History-Info
            action                  delete
            comparison-type         case-sensitive
            match-value
            msg-type                request
            new-value
            methods
        header-rule
            name                    delAlert-Info
            header-name             Alert-Info
            action                  delete
            comparison-type         case-sensitive
            match-value
            msg-type                request
            new-value
            methods
        header-rule
            name                    delPAI
            header-name             P-Asserted-Identity
            action                  delete
            comparison-type         case-sensitive
            match-value
            msg-type                request
            new-value
            methods
        header-rule
            name                    delPCV
            header-name             P-Charging-Vector
            action                  delete
            comparison-type         case-sensitive
            match-value
            msg-type                request
            new-value
            methods
        header-rule
            name                    manipMF
            header-name             Max-Forwards
            action                  manipulate
            comparison-type         case-sensitive
            match-value
            msg-type                request
            new-value               70
            methods
        last-modified-by        admin@10.10.25.141
        last-modified-date      2009-11-23 15:58:02
sip-manipulation
```

```
        name                  manip-in2
        description
        header-rule
                name                  convertPAI
                header-name              P-Asserted-Identity
                action                manipulate
                comparison-type            pattern-rule
                match-value
                msg-type               request
                new-value
                methods
                element-rule
                        name                  isTel
                        parameter-name
                        type                 header-value
                        action                store
                        match-val-type             any
                        comparison-type            pattern-rule
                        match-value               ^<tel:(.*)>$
                        new-value
                element-rule
                        name                  changeTelToSipURI
                        parameter-name
                        type                 header-value
                        action                replace
                        match-val-type             any
                        comparison-type            boolean
                        match-value               $convertPAI.$isTel
                        new-value
<sip:+$convertPAI.$isTel.$1+@bstk.telefonica.net>
        last-modified-by          admin@192.168.0.2
        last-modified-date         2010-09-30 06:15:38
steering-pool
        ip-address              10.10.25.220
        start-port             20000
        end-port               29999
        realm-id               INSIDE
        network-interface           s1p1:0
        last-modified-by          admin@192.168.0.2
        last-modified-date         2010-09-30 06:33:30
steering-pool
        ip-address              10.10.25.21
        start-port             30000
        end-port               39999
        realm-id               OUTSIDE
        network-interface           s0p0:0
```

```
        last-modified-by              admin@console
        last-modified-date            2009-11-18 08:19:41
system-config
        hostname
        description
        location                      Emilio Vargas 4
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                  enabled
        enable-snmp-auth-traps        disabled
        enable-snmp-syslog-notify     disabled
        enable-snmp-monitor-traps     disabled
        enable-env-monitor-traps      disabled
        snmp-syslog-his-table-length  1
        snmp-syslog-level             WARNING
        system-log-level              WARNING
        process-log-level             NOTICE
        process-log-ip-address        0.0.0.0
        process-log-port              0
        collect
                sample-interval               5
                push-interval                 15
                boot-state                    disabled
                start-time                    now
                end-time                      never
                red-collect-state             disabled
                red-max-trans                 1000
                red-sync-start-time           5000
                red-sync-comp-time            1000
                push-success-trap-state       disabled
        call-trace                    disabled
        internal-trace                disabled
        log-filter                    all
        default-gateway               10.10.25.129
        restart                       enabled
        exceptions
        telnet-timeout                0
        console-timeout               0
        remote-control                enabled
        cli-audit-trail               enabled
        link-redundancy-state         disabled
        source-routing                disabled
        cli-more                      disabled
        terminal-height               24
        debug-timeout                 0
```

```
    trap-event-lifetime        0
    last-modified-by           admin@192.168.0.2
    last-modified-date         2009-11-18 10:09:50
capture-receiver
    state                      disabled
    address                    1.1.1.1
    network-interface          s1p0:0
    last-modified-by           admin@192.168.0.2
    last-modified-date         2010-09-30 06:34:43
```