



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager Access Element, Avaya Aura® Session Manager and Acme Packet 4500 Net-Net Session Director to support British Telecom SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the British Telecom (BT) SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Acme Packet 4500 Net-Net Session Director, Avaya Aura® Session Manager and Avaya Aura® Communication Manager. British Telecom 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 British Telecom SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Acme Packet 4500 Net-Net Session Director, Avaya Aura® Session Manager and Avaya Aura® Communication Manager Access Element. Customers using this Avaya SIP-enabled enterprise solution with British Telecom 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 Communication Manager, Session Manager and Acme Packet 4500 Net-Net Session Director. The enterprise site was configured to use the SIP Trunk Service provided by BT.

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 BT. Incoming PSTN calls were terminated on H.323 and analog telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via BT to PSTN destinations. Outgoing calls from the enterprise to the PSTN were made from H.323 and analog telephones.
- Calls were made using G.729A, and G.711A codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode.
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as “shuffling”) with H.323 telephones.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by BT requiring Avaya response and sent by Avaya requiring BT response.

2.2. Test Results

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

- The Caller-ID set at the enterprise is overridden by BT with a pre-configured number, if the number is withheld at the enterprise no number is presented to the called party.
- All tests were completed using H.323 or analogue telephone types. No soft clients, SIP stations or digital handsets were used throughout the testing.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Routing to emergency numbers (such as 999) was not tested.
- G729 annex b (silence suppression) is not supported by BT SIP Trunk Service and thus was not tested.
- G711mu is not supported by BT SIP Trunk Service and thus was not tested.

2.3. Support

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

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the BT SIP Trunk Service. Located at the enterprise site are an Acme Packet 4500 Net-Net Session Director, Session Manager and Communication Manager. The endpoints are Avaya 9600 series IP telephones, Avaya 4600 series IP telephones (with H.323 firmware), an Analog Telephone and a 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. Instead, public IP addresses have been replaced with private addresses and all phone numbers have been replaced with arbitrary numbers that bear no relevance to the test configuration.

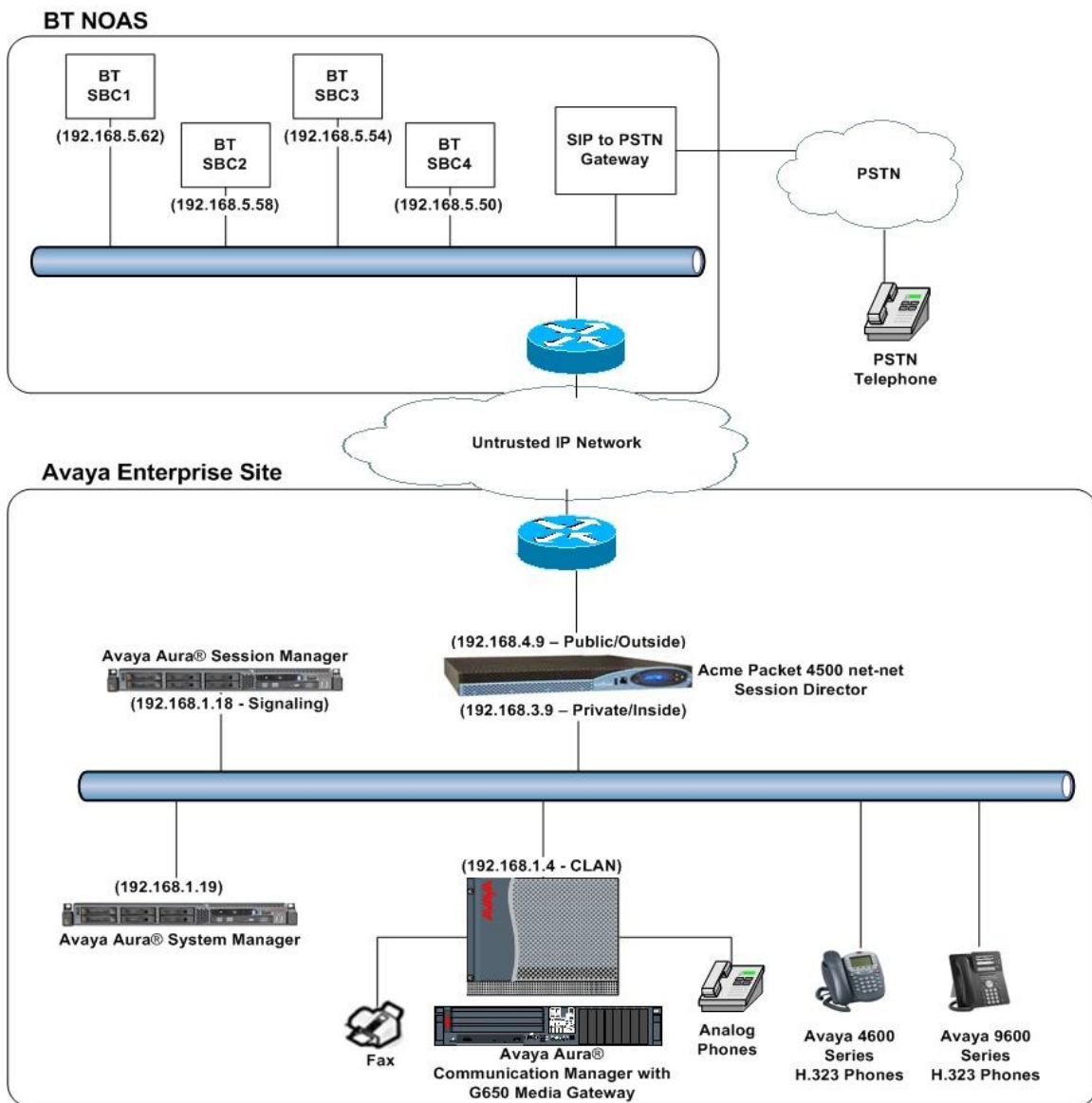


Figure 1: BT Sample Configuration

4. Equipment and Software Validated

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

| Equipment | Software |
|---|---|
| Avaya S8730 Server with G650 Media Gateway | Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4) Service Pack 18475 |
| Avaya G650 Media Gateway TN799DP CLAN TN2602AP MedPro | HW01 FW015 HW08 FW031 |
| Avaya S8800 Server | Avaya Aura® Session Manager 6.1 (6.1.0.0.610023) |
| Avaya S8800 Server | Avaya Aura® System Manager 6.1 |
| Acme Packet 4500 Net-Net Session Director | Acme Packet 4500 Net-Net Session Director 6.4. |
| Avaya 9620 Phone (H.323) | 3.11 |
| Avaya 4621 Phone (H.323) | 2.9.1 |
| Analog Phone | N/A |
| BT SIP Trunk Service | 2.1.0.8 |

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 BT SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the SBC and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the SBC; the SBC then sends the SIP messages to the BT 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 BT 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 20
      Maximum Concurrently Registered IP Stations: 18000 8
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 2 0
      Max Concur Registered Unauthenticated H.323 Stations: 0 0
      Maximum Video Capable H.323 Stations: 0 0
      Maximum Video Capable IP Softphones: 0 0
      Maximum Administered SIP Trunks: 420 98
      Maximum Administered Ad-hoc Video Conferencing Ports: 0 0
```

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

```
display system-parameters customer-options                               Page 4 of 11
                                OPTIONAL FEATURES

Emergency Access to Attendant? y                                     IP Stations? y
  Enable 'dadmin' Login? y
  Enhanced Conferencing? y                                         ISDN Feature Plus? y
    Enhanced EC500? y                                             ISDN/SIP Network Call Redirection? y
Enterprise Survivable Server? n                                     ISDN-BRI Trunks? y
  Enterprise Wide Licensing? n                                     ISDN-PRI? y
    ESS Administration? 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, **romsm6sm100** and **192.168.1.18** are the **Name** and **IP Address** for the Session Manager. Also note the **cm5clan2** name as this is the he C-LAN interface that Communication Manager will use as the SIP signaling interface to Session Manager.

```
change node-names ip                                               IP NODE NAMES

Name      IP Address
cm5clan2  192.168.1.4
romsm6sm100 192.168.1.18
default  0.0.0.0
```

5.3. Administer IP Network Region

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

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager (**Section 6.2**). In this configuration, the domain name is **rom2.bt.com**.
- By default, **IP-IP Direct Audio** (both **Intra-** and **Inter-Region**) is enabled to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources. When a PSTN call is shuffled the enterprise end point will talk directly to the inside interface of the Session Border Controller.
- 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 (**Section 5.4**).

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
Region: 1
Location: 1          Authoritative Domain: rom2.bt.com
Name: Default 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 BT were configured, namely G711A and G729. During compliance testing, other codec set configurations were also verified.

```
change ip-codec-set 1                                       Page 1 of 2
                                                           IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    Size(ms)
1: G.711A      n            2          20
2: G.729      n            2          20
3: G.711MU    n            2          20
```


BT 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 BT SIP Trunk Service and will be configured using TCP (Transport control Protocol) and the default tcp port of **5060**. Configure the **Signaling Group** using the **add signaling-group n** command as follows:

- Set the **Group Type** field to **sip**.
- The **Transport Method** field is set to **tcp** (Transport Control Protocol).
- Set the **Near-end Node Name** to the CLAN interface (node name **cm5clan2**). 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 **romsm6sm100**), shown in **Section 5.2**.
- Ensure that the recommended TCP port value of **5060** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 5.3**. This field logically establishes the far-end network-region for calls using this signaling group as network region 1.
- Set the **Far-end Domain** field to the domain of the enterprise.
- 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 **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

```
add signaling-group 35
                                SIGNALING GROUP

Group Number: 35                Group Type: sip
                                Transport Method: tcp

IMS Enabled? n

Near-end Node Name: cm5clan2    Far-end Node Name: romsm6sm100
Near-end Listen Port: 5060      Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: rom2.bt.com

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

5.6. Administer SIP Trunk Group

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

- Set the **Group Type** field to **sip**.
- Choose any descriptive **Group Name**.
- Specify a trunk access code (**TAC**) consistent with the dial plan.
- The **Direction** is set to **two-way** to allow incoming and outgoing calls.
- Set the **Service Type** field to **tie**.
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as configured in **Section 5.5**.
- Specify the **Number of Members** supported by this SIP trunk group.

```
add trunk-group 35                                     Page 1 of 21
                                                    TRUNK GROUP
Group Number: 35                                     Group Type: sip           CDR Reports: y
  Group Name: asm6-sm100                             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: 35
                                                    Number of Members: 4
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with BT to prevent unnecessary SIP messages during call setup.

```
add trunk-group 35                                     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 35                                     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
```

On **Page 4** set the **Mark Users as Phone** to **y**; this field inserts a parameter to SIP requests indicating to any receiving SIP entity that the user part of the request URI should be treated as a telephone number. Set **Send Transferring Party Information** to **y**, to allow trunk to trunk transfers. Set **Telephone Event Payload Type** to **101** the value preferred by BT.

```

add trunk-group 35
                                     Page 4 of 21
                                     PROTOCOL VARIATIONS
                                     Mark Users as Phone? y
                                     Prepend '+' to Calling Number? n
                                     Send Transferring Party Information? y
                                     Network Call Redirection? n
                                     Send Diversion Header? n
                                     Support Request History? y
                                     Telephone Event Payload Type: 101

```

5.7. Administer Calling Party Number Information

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 **38** will send the calling party number **02071111111** to BT 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      Total
Len Code    Grp(s)   Prefix  CPN
                                     Len
                                     Total Administered: 1
4  38        35        02071111111  11      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 BT SIP Trunk Service. In the sample configuration, the single digit **9** is used as the ARS access code. Avaya telephone users will dial **9** to reach an outside line. Use the **change feature-access-codes** command to configure or observe **9** as the **Auto Route Selection (ARS) - Access Code 1**.

```

change feature-access-codes
                                     Page 1 of 9
                                     FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code: *37
Answer Back Access Code: *12
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 7
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2: *99
Automatic Callback Activation:      Deactivation:
Call Forwarding Activation Busy/DA: *87      All: *88      Deactivation: #88
Call Forwarding Enhanced Status:      Act:      Deactivation:

```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. A small sample of dial patterns is illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning **0207** or **0208**. Calls are sent to Route Pattern 35.

```

change ars analysis 02                                     Page 1 of 2
                ARS DIGIT ANALYSIS TABLE
                Location: all                            Percent Full: 1

```

| Dialed String | Total | | Route Pattern | Call Type | Node Num | ANI Reqd |
|---------------|-------|-----|---------------|-----------|----------|----------|
| | Min | Max | | | | |
| 0207 | 4 | 11 | 35 | pubu | | n |
| 0208 | 4 | 11 | 35 | 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 **35** is used to route calls to trunk group **35**.

```

change route-pattern 35                                   Page 1 of 3
                Pattern Number: 35  Pattern Name: asm6-sm100
                SCCAN? n          Secure SIP? n

```

| Grp No | FRL | NPA | Pfx | Hop | Toll | No. | Inserted | DCS/ | IXC |
|--------|-----|-----|-----|-----|------|-----|----------|------|------|
| | | | Mrk | Lmt | List | Del | Digits | QSIG | |
| | | | | | | | Dgts | Intw | |
| 1: | 35 | 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 BT 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 BT correlate to the internal extensions assigned within Communication Manager. The entries displayed below translates incoming DID numbers 0207111111 and 0208111111 to a 4 digit extension by deleting all of the incoming digits and inserting an extension.

```
change inc-call-handling-trmt trunk-group 1                               Page 1 of 3
                                INCOMING CALL HANDLING TREATMENT
Service/      Number   Number   Del Insert
Feature       Len      Digits
public-ntwrk  12      0207111111  all 3802
public-ntwrk  12      0208111111  all 3803
```

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

6. Configuring Avaya Aura® Session Manager

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

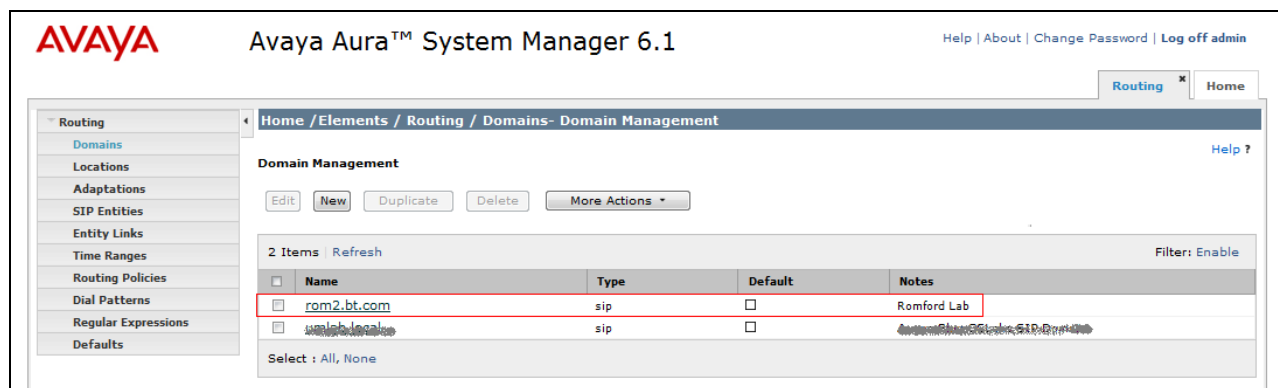
- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns

6.1. Log in to Avaya Aura® System Manager

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

6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu (not shown) and in the resulting tab select **SIP Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **rom2.bt.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** (not shown) to save changes.



The screenshot displays the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the AVAYA logo, the title "Avaya Aura™ System Manager 6.1", and links for "Help | About | Change Password | Log off admin". The main content area is titled "Domain Management" and shows a table of SIP domains. The table has columns for Name, Type, Default, and Notes. Two domains are listed: "rom2.bt.com" and "rom2.bt.com". The "rom2.bt.com" entry is highlighted with a red box, and its "Notes" field contains "Romford Lab".

| Name | Type | Default | Notes |
|--------------------------------------|------|--------------------------|-------------|
| <input type="checkbox"/> rom2.bt.com | sip | <input type="checkbox"/> | Romford Lab |
| <input type="checkbox"/> rom2.bt.com | sip | <input type="checkbox"/> | |

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. Two locations are added for the sample configuration, one for the SBC and another for the remaining enterprise SIP entities. Under 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 SBC.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is set to 'Routing' > 'Locations'. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Help ?' link. The 'General' section has a 'Name' field containing 'NOAS SIP Service' and an empty 'Notes' field. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Mbit/sec' and 'Total Bandwidth' as '1000'. The 'Per-Call Bandwidth Parameters' section shows 'Default Audio Bandwidth' as '80 Kbit/sec'. The 'Location Pattern' section has an 'Add' button and a table with one item. The table has columns for 'IP Address Pattern' and 'Notes'. The first row contains '*192.168.3.9' and 'Romford Acme SBC'. There are 'Select: All, None' options at the bottom.

Below is the location configuration used for the simulated Enterprise

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane is set to 'Routing' > 'Locations'. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Help ?' link. The 'General' section has a 'Name' field containing 'Romford Avaya Lab' and an empty 'Notes' field. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Mbit/sec' and 'Total Bandwidth' as '1000'. The 'Per-Call Bandwidth Parameters' section shows 'Default Audio Bandwidth' as '80 Kbit/sec'. The 'Location Pattern' section has an 'Add' button and a table with one item. The table has columns for 'IP Address Pattern' and 'Notes'. The first row contains '*192.168.1.*' and 'Romford Avaya Lab'. There are 'Select: All, None' options at the bottom.

6.4. Administer Adaptations

In order to ensure that the E.164 numbering format is used between the enterprise and BT SIP Trunk Service, an adaptation module is used to perform some digit manipulation. This adaptation is applied to the Communication Manager SIP entity. To add an adaptation, under the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown).

Under **General**:

- In the **Adaptation Name** field enter any informative name.
- In the **Module Name** field select <click to add module> from the drop down list and enter **DigitConversionAdapter** in the resulting **New Module Name** field.

AVAYA Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Adaptations- Adaptation Details

Adaptation Details

General

* Adaptation name: Romford CM i/c and o/g PSTN

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes: For calls into and out of the Romf

Under **Digit Conversion for Incoming Calls to SM**, click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the **Matching Pattern** field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so **destination** has been selected.

This will ensure any destination numbers received from Communication Manager are converted to the E.164 numbering format before being processed by Session Manager

Digit Conversion for Incoming Calls to SM

Add Remove

5 Items Refresh Filter: Enable

| <input type="checkbox"/> | Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Notes |
|--------------------------|------------------|-----|-----|---------------|---------------|---------------|-------------------|--------------------------------|
| <input type="checkbox"/> | *0207 | *4 | *36 | | *1 | +44 | destination | converts 0207 to +44207 for N |
| <input type="checkbox"/> | *0208 | *4 | *36 | | *1 | +44 | destination | converts 0208 to +44208 for N |
| <input type="checkbox"/> | *07 | *2 | *13 | | *1 | +44 | destination | converts 07 numbers to +447 fo |

Select : All, None

Under **Digit Conversion for Outgoing Calls from SM** click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the **Matching Pattern** field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so **destination** has been selected.

This will ensure any destination numbers will have the + symbol and international dialing code removed before being presented to Communication Manager.

| Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Notes |
|------------------|-----|-----|---------------|---------------|---------------|-------------------|--------------------------------|
| *+44207 | *6 | *36 | | *3 | 0 | destination | converts +44207 to 0207 for Cj |
| *+44208 | *6 | *36 | | *3 | 0 | destination | converts +44208 to 0208 for Cj |

6.5. Administer SIP Entities

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

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity and **Gateway** for the SBC SIP entity.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are three SIP Entities.

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

6.5.1. Avaya Aura[®] Session Manager SIP Entity

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

The screenshot shows the Avaya Aura System Manager 6.1 interface. The breadcrumb trail is Home / Elements / Routing / SIP Entities - SIP Entity Details. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. The configuration fields are as follows:

- Name:** Romford SM 6.1
- FQDN or IP Address:** 192.168.1.18
- Type:** Session Manager
- Notes:** (empty)
- Location:** Romford Avaya Lab
- Outbound Proxy:** (empty)
- Time Zone:** Europe/London
- Credential name:** (empty)
- SIP Link Monitoring:** Use Session Manager Configuration

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

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests. In this sample configuration TCP was used to connect to Communication Manager and UDP was used to connect to the Acme Packet SBC.
- In the **Default Domain** field, from the drop down menu select **rom2.bt.com** as the default domain.

The screenshot shows the 'Port' configuration section. It includes 'Add' and 'Remove' buttons. Below is a table with 3 items and a 'Refresh' button. The table has columns for 'Port', 'Protocol', 'Default Domain', and 'Notes'. The 'Filter' is set to 'Enable'. The table contains three rows, each with a checkbox, a port number, a protocol, a default domain, and a notes field.

| | Port | Protocol | Default Domain | Notes |
|--------------------------|------|----------|----------------|-------|
| <input type="checkbox"/> | 5060 | TCP | rom2.bt.com | |
| <input type="checkbox"/> | 5060 | UDP | rom2.bt.com | |
| <input type="checkbox"/> | 5061 | TLS | rom2.bt.com | |

Select : All, None

6.5.2. Avaya Aura® Communication Manager SIP Entities

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 CLAN that will be providing SIP signaling. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 6.4**.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The breadcrumb navigation shows 'Home / Elements / Routing / SIP Entities - SIP Entity Details'. The left sidebar contains a menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. Two red boxes highlight specific configuration fields: the first box encloses the 'Name' (Romford CM5.2), 'FQDN or IP Address' (192.168.1.4), and 'Type' (CM) fields; the second box encloses the 'Adaptation' (Romford CM i/c and o/g PSTN), 'Location' (Romford Avaya Lab), and 'Time Zone' (Europe/London) dropdown menus. Other visible fields include 'Notes' (CLAN address), 'Override Port & Transport with DNS SRV' (unchecked), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), 'Call Detail Recording' (none), and 'SIP Link Monitoring' (Use Session Manager Configuration).

6.5.3. Acme Packet 4500 Net-Net Session Director SIP Entity

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

The screenshot displays the Avaya Aura System Manager 6.1 interface for configuring a SIP Entity. The breadcrumb trail is Home / Elements / Routing / SIP Entities - SIP Entity Details. The left-hand navigation menu includes Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and is currently on the 'General' tab. A red rectangular box highlights the 'Name' field (Romford SBC Acme 4500 net-ne) and the 'FQDN or IP Address' field (192.168.3.9). The 'Type' is set to 'Other' and the 'Notes' field contains 'virtual address of AcmePacket'. Below this, the 'Adaptation' field is empty, while 'Location' is set to 'NOAS SIP Service' and 'Time Zone' is 'Europe/London'. There is an unchecked checkbox for 'Override Port & Transport with DNS SRV'. The 'SIP Timer B/F (in seconds)' is set to 8. The 'Credential name' field is empty, and 'Call Detail Recording' is set to 'none'. At the bottom, 'SIP Link Monitoring' is set to 'Use Session Manager Configuration'. Buttons for 'Commit' and 'Cancel' are visible in the top right corner.

6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **SessionManager**.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select the **Trusted** tick box to make the other system trusted.

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

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options like Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table of 25 items. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. Three rows are highlighted with a red box:

| <input type="checkbox"/> | Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Trusted | Notes |
|--------------------------|--|----------------|----------|------|-------------------------------|------|-------------------------------------|-------|
| <input type="checkbox"/> | Romford SM 6.1 to Romford Acme SBC | Romford SM 6.1 | UDP | 5060 | Romford SBC Acme 4500 net-net | 5060 | <input checked="" type="checkbox"/> | |
| <input type="checkbox"/> | Romford SM6.1 to Romford CM5.2 | Romford SM 6.1 | TCP | 5060 | Romford CM5.2 | 5060 | <input checked="" type="checkbox"/> | |
| <input type="checkbox"/> | Romford SM 6.1 to Romford CM 6.1 | Romford SM 6.1 | TLS | 5061 | Romford CM6.1 | 5061 | <input checked="" type="checkbox"/> | |

6.7. Administer Routing Policies

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

- Under **General** enter an informative name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select**, and in the resulting window (not shown) select the appropriate SIP entity to which this routing policy applies.
- Under **Time of Day**, click **Add**, and then select the time range.

The following screen shows the routing policy for Communication Manager

The screenshot displays the Avaya Aura System Manager 6.1 interface. The left sidebar shows a navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and is divided into three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' field is populated with 'NOAS Calls to Rom CM5.2'. The 'SIP Entity as Destination' section shows a 'Select' button and a table with one entry: 'Romford CM5.2' with EQDN or IP Address '192.168.1.4' and Type 'CM'. The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, a '1 Item Refresh' button, and a table with one entry: '24/7' with a ranking of '0' and a time range of '00:00' to '23:59'.

| Name | EQDN or IP Address | Type | Notes |
|---------------|--------------------|------|--------------|
| Romford CM5.2 | 192.168.1.4 | CM | CLAN address |

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

The following screen shows the routing policy for Acme Packet 4500 Net-Net Session Director.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The breadcrumb trail is 'Home / Elements / Routing / Routing Policies - Routing Policy Details'. The page title is 'Routing Policy Details' with 'Commit' and 'Cancel' buttons. The 'General' section shows the policy name as 'SIP Calls to Romford Acme SBC'. Below this, there is a 'SIP Entity as Destination' section with a 'Select' button. A table lists the destination entity:

| Name | FQDN or IP Address | Type | Notes |
|-------------------------------|--------------------|-------|-------------------------------|
| Romford SBC Acme 4500 net-net | 192.168.3.9 | Other | virtual address of AcmePacket |

The 'Time of Day' section includes 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below is a table with one item:

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

At the bottom, there is a 'Select : All, None' option.

6.8. Administer Dial Patterns

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

Under **General**:

- In the **Pattern** field enter a dialed number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialed number.
- In the **Max** field enter the maximum length of the dialed number.
- In the **SIP Domain** field select the domain configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**, click **Add**. In the resulting screen (not shown), under **Originating Location** select **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save. The following screen shows an example dial pattern configured for the Acme Packet 4500 Net-Net Session Director.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The left sidebar shows a navigation menu with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and is divided into two sections: 'General' and 'Originating Locations and Routing Policies'.

General Section:

- Pattern:** +44208
- Min:** 6
- Max:** 36
- Emergency Call:**
- SIP Domain:** rom2.bt.com
- Notes:** (empty field)

Originating Locations and Routing Policies Section:

Buttons: Add, Remove

1 Item Refresh Filter: Enable

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|-------------------------------|------|--------------------------|-------------------------------|----------------------|
| <input type="checkbox"/> | -ALL- | Any Locations | SIP Calls to Romford Acme SBC | 0 | <input type="checkbox"/> | Romford SBC Acme 4500 net-net | |

Select : All, None

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

The screenshot displays the Avaya Aura System Manager 6.1 interface. The breadcrumb navigation is Home / Elements / Routing / Dial Patterns - Dial Pattern Details. The left sidebar shows a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and includes a 'General' section with the following fields:

- Pattern:** +44207
- Min:** 12
- Max:** 36
- Emergency Call:**
- SIP Domain:** rom2.bt.com
- Notes:** Inbound DDI 324X for Rom CM5.2

Below the general section is the 'Originating Locations and Routing Policies' section, which includes 'Add' and 'Remove' buttons. A table below shows one item:

| <input type="checkbox"/> | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|--------------------------|---------------------------|----------------------------|-------------------------|------|--------------------------|----------------------------|----------------------|
| <input type="checkbox"/> | NOAS SIP Service | | NOAS Calls to Rom CM5.2 | 0 | <input type="checkbox"/> | Romford CM5.2 | |

At the bottom of the table, there is a 'Select' dropdown menu with options 'All, None'.

7. Configure Acme Packet 4500 Net-Net Session Director

This section describes the configuration of the Acme Packet net-net 4500 Session Director. 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 interoperability test will be covered. For completeness the running configuration used during the interoperability testing is displayed in **Appendix A**.

7.1. Accessing Acme Packet 4500 Net-Net Session Director

Connect to the Acme Packet session director and login with the appropriate credentials. At the prompt enter the **enable** command and then the superuser password. Once in superuser mode enter the command **configure terminal** to enter the 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 acme packet session director. In this case, the default gateway is **192.168.1.1**.
- **source-routing**: Set to **enabled**.

```
system-config
  hostname
  description
  location

  < text removed for brevity >

  call-trace                disabled
  internal-trace            disabled
  log-filter                all
  default-gateway          192.168.1.1
  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 0 was connected to the inside enterprise network. Access the **System** → **phy-interface** element and set the following element parameters:

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

```
phy-interface
  name           M10
  operation-type Media
  port           0
  slot           1
  virtual-mac    00:08:25:a1:90:0E
  admin-state    enabled
  auto-negotiation enabled
  duplex-mode    FULL
  speed          100
  last-modified-by admin@console
  last-modified-date 2010-09-07 15:15:33
phy-interface
  name           M00
  operation-type Media
  port           0
  slot           0
  virtual-mac    00:08:25:a1:8f:4E
  admin-state    enabled
  auto-negotiation enabled
  duplex-mode    FULL
  speed          100
  last-modified-by admin@console
  last-modified-date 2010-09-07 15:15:49
```

7.4. Network Interfaces

A network interface was defined for each physical interface to assign a routable IP address. Access the **System** → **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.
- **pri-utility-addr/ sec-utility-addr**: The physical address of the primary and secondary Acme Packet Session Director in the high availability pair. **Note**: The high availability configuration of the Acme Packet Session Director is outside the scope of these application notes and these fields are included here to avoid confusion.
- **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 M10
  sub-port-id 0
  description Facing Avaya
  hostname
  ip-address 192.168.3.9
  pri-utility-addr 192.168.3.170
  sec-utility-addr 192.168.3.171
  netmask 255.255.255.0
  gateway 192.168.3.1
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 32
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout 11
  hip-ip-list 192.168.3.9
  ftp-address
  icmp-address 192.168.3.9
  snmp-address
  telnet-address
  last-modified-by admin@192.168.1.6
  last-modified-date 2010-09-08 14:18:22
```

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

```
network-interface
  name M00
  sub-port-id 0
  description Facing Noas
  hostname
  ip-address 192.168.4.9
  pri-utility-addr 192.168.1.130
  sec-utility-addr 192.168.1.132
  netmask 255.255.255.0
  gateway 192.168.1.1
  sec-gateway
  gw-heartbeat
    state enabled
    heartbeat 10
    retry-count 3
    retry-timeout 3
    health-score 30
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout 11
  hip-ip-list 192.168.4.9
  ftp-address
  icmp-address 192.168.4.9
  snmp-address
  telnet-address
  last-modified-by admin@192.168.1.6
  last-modified-date 2010-09-08 12:11:55
```

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 **media-manager** → **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                access-noas
  description               Access Realm for NOAS SAG
  addr-prefix               0.0.0.0
  network-interfaces

  mm-in-realm              M00:0
                           disabled
  mm-in-network            enabled

< text removed for brevity >

realm-config
  identifier                core-noas
  description               Core Realm calls from NOAS SAG to AVAYA
  addr-prefix               0.0.0.0
  network-interfaces

  mm-in-realm              M10:0
                           disabled
  mm-in-network            enabled

< text removed for brevity >
```

7.6. SIP Configuration

The SIP configuration defines the global system-wide SIP parameters. Access the **session-router** → **sip-config** element and set the following parameters:

- **home-realm-id**: The name of the realm on the internal enterprise side of the Acme Packet Session Director.
- **nat-mode**: set to **public** which indicates that IPv4 addresses are encoded in SIP messages received from the external realm defined by the SIP NAT. The IPv4 addresses are decoded in messages that are sent to the realm for further information on SIP NAT see reference [9-11].
- **registrar-domain**: An asterisk * is specified to allow any domain.
- **registrar-host**: An asterisk * is specified to allow any host.
- **registrar-port**: port used for registration.

```
sip-config
  state                enabled
  operation-mode       dialog
  dialog-transparency  disabled
  home-realm-id        core-noas
  egress-realm-id
  nat-mode             public
  registrar-domain     *
  registrar-host       *
  registrar-port       5060
  register-service-route always
  init-timer           500
  max-timer            4000
  register-service-route always
  init-timer           500
  max-timer            4000
  trans-expire         32
  invite-expire        180
  inactive-dynamic-conn 32

< text removed for brevity >
```


7.7. 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 **session-router** → **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 **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 **sip-config** (**Section 7.6**) will be used.

```
sip-interface
state                enabled
realm-id           core-noas
description          Core NOAS SAG SIP Interface
sip-port
  address          192.168.3.9
  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           access-noas
description          Interface
sip-port
  address          192.168.4.9
  port             5060
  transport-protocol  UDP
  tls-profile
  allow-anonymous   agents-only
  ims-aka-profile
carriers
trans-expire      4
invite-expire    185

< text removed for brevity >
```

7.8. Session Agent

A session agent defines the characteristics of a signalling peer to the Acme Packet Session Director such as Session Manager. During testing, BT SIP Trunk Service had multiple SBCs; a session agent must be defined for each SIP peer. Access the **session-router** → **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**: 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 **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                rom2.bt.com
  ip-address              192.168.1.18
  port                    5060
  state                   enabled
  app-protocol            SIP
  app-type
  transport-method       UDP
  realm-id                core-noas
  egress-realm-id
  description             Avaya SM 6.0
  carriers
< text removed for brevity >
  response-map
  ping-method             OPTIONS;hops=0
  ping-interval           60
  ping-send-mode          keep-alive
< text removed for brevity >
  in-manipulationid
  out-manipulationid     CoreNoasEgress
  manipulation-string
```

The settings for the session agent relating to BT SBC1 are shown below.

```
session-agent
  hostname          192.168.5.62
  ip-address        192.168.5.62
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          access-noas
  egress-realm-id
  description       NOAS SBC1
  carriers

< text removed for brevity >

  response-map
  ping-method       OPTIONS;hops=66
  ping-interval     60
  ping-send-mode    keep-alive
  ping-in-service-response-codes 200-407,409-499,501-502,505-699
  out-service-response-codes

< text removed for brevity >

  li-trust-me       disabled
  in-manipulationid AccessNoasIngress
  out-manipulationid AccessNoasEgress
  manipulation-string NOASSBC1
```

The settings for the session agent relating to BT SBC2 are shown below.

```
session-agent
  hostname          192.168.5.58
  ip-address        192.168.5.58
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          access-noas
  egress-realm-id
  description       NOAS SBC2
  carriers

< text removed for brevity >

  response-map
  ping-method       OPTIONS;hops=66
  ping-interval     60
  ping-send-mode    keep-alive
  ping-in-service-response-codes 200-407,409-499,501-502,505-699
  out-service-response-codes

< text removed for brevity >

  li-trust-me       disabled
  in-manipulationid AccessNoasIngress
  out-manipulationid AccessNoasEgress
  manipulation-string NOASSBC2
```

The settings for the session agent relating to BT SBC3 are shown below.

```
session-agent
  hostname          192.168.5.54
  ip-address        192.168.5.54
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          access-noas
  egress-realm-id
  description       NOAS SBC3
  carriers

< text removed for brevity >

  response-map
  ping-method       OPTIONS;hops=66
  ping-interval     60
  ping-send-mode    keep-alive
  ping-in-service-response-codes 200-407,409-499,501-502,505-699
  out-service-response-codes

< text removed for brevity >

  li-trust-me       disabled
  in-manipulationid AccessNoasIngress
  out-manipulationid AccessNoasEgress
  manipulation-string NOASSBC3
```

The settings for the session agent relating to BT SBC4 are shown below.

```
session-agent
  hostname          192.168.5.50
  ip-address        192.168.5.50
  port              5060
  state             enabled
  app-protocol      SIP
  app-type
  transport-method  UDP
  realm-id          access-noas
  egress-realm-id
  description       NOAS SBC4
  carriers

< text removed for brevity >

  response-map
  ping-method       OPTIONS;hops=66
  ping-interval     60
  ping-send-mode    keep-alive
  ping-in-service-response-codes 200-407,409-499,501-502,505-699
  out-service-response-codes

< text removed for brevity >

  li-trust-me       disabled
  in-manipulationid AccessNoasIngress
  out-manipulationid AccessNoasEgress
  manipulation-string NOASSBC4
```

7.9. Session Agent Group

Where multiple session agents exist, a session group is used to define a list of session agents and the hunting order in which the specified session agents will be used. Access the **session-router** → **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:** List of the session agents defined in **Section 7.8** available to the session agent group in priority order.

| | |
|----------------------|---------------------------------|
| session-group | |
| group-name | ACCESS-NOAS |
| description | NOAS SBC Hunt Group |
| state | enabled |
| app-protocol | SIP |
| strategy | Hunt |
| dest | 192.168.5.62 |
| | 192.168.5.58 |
| | 192.168.5.54 |
| | 192.168.5.50 |
| trunk-group | |
| sag-recursion | enabled |
| stop-sag-recurse | 404,422-423,480,484,486,505-599 |
| last-modified-by | admin@192.168.1.6 |
| last-modified-date | 2010-09-14 15:49:08 |

7.10. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages. During the compliance test, three sip manipulations were used; these were assigned to session agents configured in **Section 7.8**. Multiple header rules can exist for each sip manipulation. As an example, the first sip manipulation and first header rule within that sip manipulation will be discussed in this section. Additional header rules and additional sip manipulations are listed in **Appendix A**.

Access the **session-router** → **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 **AccessNoasEgress** is shown. The first header rule called **ModFrom** specifies that the **From** header in SIP request messages will be manipulated based on the element rule defined. The **element-rule** called **AcmeNatFromHost** specifies that the host part of the URI in the **From** header should be replaced with the value of **\$LOCAL_IP**. The value of **\$LOCAL_IP** is an Acme Packet variable used to represent the IP address of the SIP interface that message is being sent from.

```

sip-manipulation
  name                AccessNoasEgress
  description          Access NOAS Egress HMR
  header-rule
    name              ModFrom
    header-name       From
    action             manipulate
    comparison-type    case-sensitive
    match-value
    msg-type          any
    new-value
    methods
    element-rule
      name            AcmeNatFromHost
      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 >

7.11. 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 **media-manager** → **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 number of the port that begins the range.
- **end-port:** The number of the port that ends the range.
- **realm-id:** The realm to which this steering pool is assigned, as defined in **Section 7.5**.

```
steering-pool
  ip-address          192.168.4.9
  start-port         49152
  end-port           65535
  realm-id           access-noas
  network-interface
  last-modified-by   admin@192.168.1.6
  last-modified-date 2010-09-08 11:57:15
steering-pool
  ip-address          192.168.3.9
  start-port         49152
  end-port           65535
  realm-id           core-noas
  network-interface
  last-modified-by   admin@console
  last-modified-date 2010-09-07 15:28:21
```

7.12. Local Policy

Local policy controls the routing of SIP calls from one realm to another. Access the **session-router** → **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 **core-noas** realm are to be sent to the **access-noas** realm using the SAG defined in **Section 7.9**.

```
local-policy
  from-address          *
  to-address            *
  source-realm          core-noas
  description           Avaya To NOAS SAG
  activate-time         N/A
  deactivate-time       N/A
  state                 enabled
  policy-priority       none
  last-modified-by      admin@console
  last-modified-date    2010-06-28 12:56:52
  policy-attribute
    next-hop            SAG: ACCESS-NOAS
    realm               access-noas
    action               replace-uri
< text removed for brevity >
```

The settings for the second **local-policy** are shown below. This policy indicates that messages originating from the **access-noas** realm are to be sent to the **core-noas** realm using IP address 192.168.1.18.

```
local-policy
  from-address          *
  to-address            *
  source-realm         access-noas
  description          NOAS SAG To Avaya
  activate-time        N/A
  deactivate-time      N/A
  state                enabled
  policy-priority      none
  last-modified-by    admin@192.168.1.6
  last-modified-date  2011-02-03 17:26:35
  policy-attribute
    next-hop           192.168.1.18
    realm              core-noas
    action              none
< text removed for brevity >
```

8. Verification Steps

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

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

The screenshot shows the Avaya Aura System Manager 6.1 interface. The breadcrumb trail is: Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring. The page title is "SIP Entity, Entity Link Connection Status". Below the title, it says "All Entity Links to SIP Entity: Romford SBC Acme 4500 net-net". There is a "Summary View" button. A table shows the connection status for one item, "Romford SM 6.1". The table has columns: Details, Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn-Status, Reason-Code, and Link-Status. The values for the row are: Show, Romford SM 6.1, 192.168.3.9, 5060, UDP, Up, 200 OK, and Up. The "Up" values in the Conn-Status and Link-Status columns are highlighted with a red box.

| Details | Session Manager Name | SIP Entity Resolved IP | Port | Proto. | Conn-Status | Reason-Code | Link-Status |
|---------|----------------------|------------------------|------|--------|-------------|-------------|-------------|
| Show | Romford SM 6.1 | 192.168.3.9 | 5060 | UDP | Up | 200 OK | Up |

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

```
status trunk 35

                                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 remains 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.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Acme Packet 4500 Net-Net Session Director to SIP Trunk Service. BT SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

10. References

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

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

Product documentation for the Session Director can be obtained from Acme Packet's support web site <https://support.acmepacket.com>. (login required)

- [9] *Net-Net Session Director Installation Guide*, Acme Packet Documentation Set.
- [10] *Net-Net 4000 ACLI Configuration Guide, Release Version S-C6.1.0*, Acme Packet Documentation Set.
- [11] *Net-Net 4000 ACLI Reference Guide, Release Version S-C6.1.0*, Acme Packet Documentation Set

©2011 Avaya Inc. All Rights Reserved.

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

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

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.

```
# sh running-config
access-control
  realm-id          core-noas
  description       Avaya To NOAS SAG
  source-address    0.0.0.0
  destination-address 192.168.3.9:22
  application-protocol NONE
  transport-protocol ALL
  access            permit
  average-rate-limit 0
  trust-level       high
  minimum-reserved-bandwidth 0
  invalid-signal-threshold 1
  maximum-signal-threshold 12000
  untrusted-signal-threshold 0
  nat-trust-threshold 0
  deny-period       30
  last-modified-by  admin@console
  last-modified-date 2010-09-07 15:58:33
access-control
  realm-id          core-noas
  description       ACL for Avaya devices in the core side
  source-address    192.168.1.183
  destination-address 192.168.3.9:5060
  application-protocol SIP
  transport-protocol UDP
  access            permit
  average-rate-limit 0
  trust-level       high
  minimum-reserved-bandwidth 0
  invalid-signal-threshold 1
  maximum-signal-threshold 12000
  untrusted-signal-threshold 0
  nat-trust-threshold 0
  deny-period       30
  last-modified-by  admin@ console
  last-modified-date 2011-02-09 11:37:53
access-control
  realm-id          core-noas
```

```

description          ACL for Avaya devices in the core side
source-address       192.168.1.18
destination-address  192.168.3.9:5060
application-protocol SIP
transport-protocol  UDP
access               permit
average-rate-limit   0
trust-level          high
minimum-reserved-bandwidth 0
invalid-signal-threshold 1
maximum-signal-threshold 12000
untrusted-signal-threshold 0
nat-trust-threshold 0
deny-period          30
last-modified-by     admin@ console
last-modified-date   2011-02-09 11:38:46
access-control
  realm-id            access-noas
  description         ACL for NOAS SBCs
  source-address      192.168.5.62
  destination-address 192.168.4.9:5060
  application-protocol SIP
  transport-protocol  UDP
  access              permit
  average-rate-limit   0
  trust-level          medium
  minimum-reserved-bandwidth 0
  invalid-signal-threshold 1
  maximum-signal-threshold 12000
  untrusted-signal-threshold 4
  nat-trust-threshold 0
  deny-period          30
  last-modified-by     admin@ console
  last-modified-date   2011-02-09 10:59:37
access-control
  realm-id            access-noas
  description         ACL for NOAS SBCs
  source-address      192.168.5.58
  destination-address 192.168.4.9:5060
  application-protocol SIP
  transport-protocol  UDP
  access              permit
  average-rate-limit   0
  trust-level          medium
  minimum-reserved-bandwidth 0
  invalid-signal-threshold 1

```



```

maximum-signal-threshold 12000
untrusted-signal-threshold 4
nat-trust-threshold 0
deny-period 30
last-modified-by admin@ console
last-modified-date 2011-02-09 11:02:46
access-control
realm-id access-noas
description ACL for NOAS SBCs
source-address 192.168.5.54
destination-address 192.168.4.9:5060
application-protocol SIP
transport-protocol UDP
access permit
average-rate-limit 0
trust-level medium
minimum-reserved-bandwidth 0
invalid-signal-threshold 1
maximum-signal-threshold 12000
untrusted-signal-threshold 4
nat-trust-threshold 0
deny-period 30
last-modified-by admin@console
last-modified-date 2011-02-09 11:05:13
access-control
realm-id access-noas
description ACL for NOAS SBCs
source-address 192.168.5.50
destination-address 192.168.4.9:5060
application-protocol SIP
transport-protocol UDP
access permit
average-rate-limit 0
trust-level medium
minimum-reserved-bandwidth 0
invalid-signal-threshold 1
maximum-signal-threshold 12000
untrusted-signal-threshold 4
nat-trust-threshold 0
deny-period 30
last-modified-by admin@ console
last-modified-date 2011-02-09 11:36:00
capture-receiver
state enabled
address 192.168.1.6
network-interface M00:0

```

| | |
|---------------------|---------------------|
| last-modified-by | admin@192.168.1.6 |
| last-modified-date | 2010-09-08 12:17:10 |
| local-policy | |
| from-address | * |
| to-address | * |
| source-realm | core-noas |
| description | Avaya To NOAS SAG |
| activate-time | N/A |
| deactivate-time | N/A |
| state | enabled |
| policy-priority | none |
| last-modified-by | admin@ console |
| last-modified-date | 2010-06-28 12:56:52 |
| policy-attribute | |
| next-hop | SAG:ACCESS-NOAS |
| realm | access-noas |
| action | replace-uri |
| terminate-recursion | enabled |
| 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 | access-noas |
| description | NOAS SAG To Avaya |
| activate-time | N/A |
| deactivate-time | N/A |
| state | enabled |
| policy-priority | none |
| last-modified-by | admin@192.168.1.6 |
| last-modified-date | 2011-02-03 17:26:35 |
| policy-attribute | |
| next-hop | 192.168.1.18 |

| | |
|------------------------------|------------|
| realm | core-noas |
| action | none |
| terminate-recursion | enabled |
| 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 |
| options | active-arp |
| red-flow-port | 1985 |
| red-mgcp-port | 0 |
| red-max-trans | 10000 |
| red-sync-start-time | 5000 |
| red-sync-comp-time | 1000 |
| media-policing | enabled |
| max-signaling-bandwidth | 775880 |
| max-untrusted-signaling | 1 |
| min-untrusted-signaling | 1 |
| app-signaling-bandwidth | 0 |
| tolerance-window | 30 |
| rtcp-rate-limit | 0 |
| min-media-allocation | 2000 |
| min-trusted-allocation | 4000 |
| deny-allocation | 64000 |
| 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
dnssalg-server-failover disabled
last-modified-by admin@ console
last-modified-date 2011-02-09 11:46:23
network-interface
name wancom1
sub-port-id 0
description
hostname
ip-address
pri-utility-addr 169.254.1.1
sec-utility-addr 169.254.1.2
netmask 255.255.255.252
gateway
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
ftp-address
icmp-address
snmp-address
telnet-address
last-modified-by admin@console
last-modified-date 2010-09-07 15:00:12

```

```

network-interface
name wancom2
sub-port-id 0
description
hostname
ip-address
pri-utility-addr 169.254.2.1
sec-utility-addr 169.254.2.2
netmask 255.255.255.252
gateway
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
ftp-address
icmp-address
snmp-address
telnet-address
last-modified-by     admin@console
last-modified-date   2010-09-07 15:00:12
network-interface
name                 M10
sub-port-id          0
description           Facing Avaya
hostname
ip-address            192.168.3.9
pri-utility-addr     192.168.3.170
sec-utility-addr     192.168.3.171
netmask              255.255.255.0
gateway              192.168.3.1
sec-gateway
gw-heartbeat
state                disabled
heartbeat            0
retry-count          0
retry-timeout        1
health-score         32
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout          11
hip-ip-list          192.168.3.9
ftp-address
icmp-address          192.168.3.9
snmp-address
telnet-address
last-modified-by     admin@192.168.1.6
last-modified-date   2010-09-08 14:18:22

```

```

network-interface
  name          M00
  sub-port-id   0
  description   Facing Noas
  hostname
  ip-address    192.168.4.9
  pri-utility-addr 192.168.1.130
  sec-utility-addr 192.168.1.132
  netmask       255.255.255.0
  gateway       192.168.1.1
  sec-gateway
  gw-heartbeat
    state       enabled
    heartbeat   10
    retry-count 3
    retry-timeout 3
    health-score 30
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout   11
  hip-ip-list   192.168.4.9
  ftp-address
  icmp-address  192.168.4.9
  snmp-address
  telnet-address
  last-modified-by admin@192.168.1.6
  last-modified-date 2010-09-08 12:11:55
ntp-config
  last-modified-by admin@192.168.1.6
  last-modified-date 2010-09-22 15:06:51
phy-interface
  name          wancom1
  operation-type Control
  port          1
  slot          0
  virtual-mac
  wancom-health-score 8
  last-modified-by admin@console
  last-modified-date 2010-09-07 15:00:12
phy-interface
  name          wancom2
  operation-type Control
  port          2
  slot          0

```

```

virtual-mac
wancom-health-score      9
last-modified-by        admin@console
last-modified-date      2010-09-07 15:00:12
phy-interface
name                     M10
operation-type           Media
port                     0
slot                     1
virtual-mac              00:08:25:a1:90:0E
admin-state              enabled
auto-negotiation         enabled
duplex-mode              FULL
speed                    100
last-modified-by        admin@console
last-modified-date      2010-09-07 15:15:33
phy-interface
name                     M00
operation-type           Media
port                     0
slot                     0
virtual-mac              00:08:25:a1:8f:4E
admin-state              enabled
auto-negotiation         enabled
duplex-mode              FULL
speed                    100
last-modified-by        admin@console
last-modified-date      2010-09-07 15:15:49
realm-config
identifier                access-noas
description                Access Realm for NOAS SAG
addr-prefix                0.0.0.0
network-interfaces
M00:0
mm-in-realm                disabled
mm-in-network              enabled
mm-same-ip                 enabled
mm-in-system               enabled
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 | medium |
| invalid-signal-threshold | 1 |
| maximum-signal-threshold | 1 |
| untrusted-signal-threshold | 1 |
| nat-trust-threshold | 0 |
| deny-period | 60 |
| 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@console
last-modified-date   2011-02-09 11:42:10
realm-config
  identifier          core-noas
  description         Core Realm calls from NOAS SAG to AVAYA
  addr-prefix         0.0.0.0
  network-interfaces
    M10:0
  mm-in-realm         disabled
  mm-in-network       enabled
  mm-same-ip          enabled
  mm-in-system        enabled
  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  high
  invalid-signal-threshold  1
  maximum-signal-threshold  1
  untrusted-signal-threshold  0
  nat-trust-threshold  0
  deny-period         60
  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@console
last-modified-date       2011-02-09 12:35:58
redundancy-config
state                    enabled
log-level                INFO
health-threshold         75
emergency-threshold      50
port                     9090
advertisement-time       500
percent-drift            210
initial-time             1250
becoming-standby-time    180000
becoming-active-time     100
cfg-port                 1987
cfg-max-trans            10000
cfg-sync-start-time      5000
cfg-sync-comp-time       1000
gateway-heartbeat-interval 0

```

```

gateway-heartbeat-retry    0
gateway-heartbeat-timeout  1
gateway-heartbeat-health   0
media-if-peercheck-time   0
peer
  name                      SBC1
  state                     enabled
  type                      Primary
  destination
    address                 169.254.1.1:9090
    network-interface       wancom1:0
  destination
    address                 169.254.2.1:9090
    network-interface       wancom2:0
peer
  name                      SBC2
  state                     enabled
  type                      Secondary
  destination
    address                 169.254.1.2:9090
    network-interface       wancom1:0
  destination
    address                 169.254.2.2:9090
    network-interface       wancom2:0
last-modified-by          admin@console
last-modified-date        2010-09-07 15:00:12
session-agent
hostname                  192.168.1.183
ip-address                 192.168.1.183
port                      5060
state                     enabled
app-protocol              SIP
app-type
transport-method          UDP
realm-id                  core-noas
egress-realm-id
description                Avaya SIP Port For NOAS SAG
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 | 60 |
| 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 | CoreNoasEgress |
| 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 | TCP |
| tcp-keepalive | none |

```

tcp-reconn-interval      0
max-register-burst-rate  0
register-burst-window    0
last-modified-by        admin@192.168.1.6
last-modified-date      2010-09-14 18:14:20
session-agent
hostname                 192.168.5.62
ip-address               192.168.5.62
port                    5060
state                   enabled
app-protocol            SIP
app-type
transport-method        UDP
realm-id                access-noas
egress-realm-id
description              NOAS SBC1
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=66
ping-interval           60
ping-send-mode          keep-alive
ping-in-service-response-codes 200-407,409-499,501-502,505-699
out-service-response-codes

```

| | |
|---------------------------|---------------------|
| options | trans-timeouts=2 |
| 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 | AccessNoasIngress |
| out-manipulationid | AccessNoasEgress |
| manipulation-string | NOASSBC1 |
| 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@console |
| last-modified-date | 2010-09-07 15:43:06 |
| session-agent | |
| hostname | 192.168.5.58 |
| ip-address | 192.168.5.58 |
| port | 5060 |
| state | enabled |
| app-protocol | SIP |
| app-type | |
| transport-method | UDP |
| realm-id | access-noas |
| egress-realm-id | |
| description | NOAS SBC2 |
| 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=66 |
| ping-interval | 60 |
| ping-send-mode | keep-alive |
| ping-in-service-response-codes | 200-407,409-499,501-502,505-699 |
| out-service-response-codes | |
| options | trans-timeouts=2 |
| 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 | AccessNoasIngress |
| out-manipulationid | AccessNoasEgress |
| manipulation-string | NOASSBC2 |
| 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@192.168.1.6 |
| last-modified-date | 2010-09-08 11:51:38 |
| session-agent | |
| hostname | 192.168.5.54 |
| ip-address | 192.168.5.54 |
| port | 5060 |
| state | enabled |
| app-protocol | SIP |
| app-type | |
| transport-method | UDP |
| realm-id | access-noas |
| egress-realm-id | |
| description | NOAS SBC3 |
| carriers | |
| allow-next-hop-ip | 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=66
 ping-interval 60
 ping-send-mode keep-alive
 ping-in-service-response-codes 200-407,409-499,501-502,505-699
 out-service-response-codes
 options trans-timeouts=2
 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 AccessNoasIngress
 out-manipulationid AccessNoasEgress
 manipulation-string NOASSBC3
 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@192.168.1.6
 last-modified-date 2010-09-08 11:52:41
 session-agent
 hostname 192.168.5.50
 ip-address 192.168.5.50
 port 5060
 state enabled
 app-protocol SIP
 app-type
 transport-method UDP
 realm-id access-noas

| | |
|--------------------------------|---------------------------------|
| egress-realm-id | |
| description | NOAS SBC4 |
| 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=66 |
| ping-interval | 60 |
| ping-send-mode | keep-alive |
| ping-in-service-response-codes | 200-407,409-499,501-502,505-699 |
| out-service-response-codes | |
| options | trans-timeouts=2 |
| 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 | AccessNoasIngress |
| out-manipulationid | AccessNoasEgress |
| manipulation-string | NOASSBC4 |

```

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@192.168.1.6
last-modified-date           2010-09-14 15:46:00
session-agent
hostname                      rom2.bt.com
ip-address                    192.168.1.18
port                          5060
state                          enabled
app-protocol                  SIP
app-type
transport-method              UDP
realm-id                      core-noas
egress-realm-id
description                   Avaya SM 6.0
carriers
allow-next-hop-ip             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 | 60 |
| 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 | CoreNoasEgress |
| 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 | TCP |
| tcp-keepalive | none |
| tcp-reconn-interval | 0 |
| max-register-burst-rate | 0 |
| register-burst-window | 0 |
| last-modified-by | admin@console |
| last-modified-date | 2011-02-09 12:32:21 |
| session-group | |
| group-name | ACCESS-NOAS |
| description | NOAS SBC Hunt Group |
| state | enabled |

| | |
|--------------------------|---------------------------------|
| app-protocol | SIP |
| strategy | Hunt |
| dest | 192.168.5.62 |
| | 192.168.5.58 |
| | 192.168.5.54 |
| | 192.168.5.50 |
| trunk-group | |
| sag-recursion | enabled |
| stop-sag-recurse | 404,422-423,480,484,486,505-599 |
| last-modified-by | admin@192.168.1.6 |
| last-modified-date | 2010-09-14 15:49:08 |
| sip-config | |
| state | enabled |
| operation-mode | dialog |
| dialog-transparency | disabled |
| home-realm-id | core-noas |
| egress-realm-id | |
| nat-mode | Public |
| registrar-domain | * |
| registrar-host | * |
| registrar-port | 5060 |
| 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
proxy-sub-events
last-modified-by        admin@console
last-modified-date      2010-10-11 18:49:49
sip-interface
state                    enabled
realm-id                 core-noas
description              Core NOAS SAG SIP Interface
sip-port
  address                192.168.3.9
  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
options                  max-udp-length=0
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@192.168.1.6
last-modified-date      2011-02-03 15:48:28
sip-interface
state                   enabled
realm-id                access-noas
description             Interface
sip-port
  address                192.168.4.9
  port                   5060
  transport-protocol     UDP
  tls-profile
  allow-anonymous        agents-only
  ims-aka-profile
carriers
trans-expire            4
invite-expire           185
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 | |
| options | set-inv-exp-at-100-resp |
| 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@console
last-modified-date      2011-02-09 11:50:27
sip-manipulation
name                    AccessNoasEgress
description              Access NOAS Egress HMR
header-rule
  name                  ModFrom
  header-name           From
  action                manipulate
  comparison-type       case-sensitive
  match-value
  msg-type              any
  new-value
  methods
  element-rule
    name                AcmeNatFromHost
    parameter-name
    type                uri-host
    action              replace
    match-val-type      any
    comparison-type     case-sensitive
    match-value
    new-value           $LOCAL_IP
  header-rule
    name                ModTo
    header-name         To
    action              manipulate
    comparison-type     case-sensitive
    match-value
    msg-type            any
    new-value
    methods
    element-rule
      name              AcmeNatToHost
      parameter-name
      type              uri-host
      action            replace
      match-val-type    any
      comparison-type   case-sensitive
      match-value

```

```

        new-value          $REMOTE_IP
header-rule
  name                    ModAlertInfoHost
  header-name             Alert-Info
  action                  find-replace-all
  comparison-type         pattern-rule
  match-value             avaya.com
  msg-type                any
  new-value               $LOCAL_IP
  methods
header-rule
  name                    ModPai
  header-name             P-Asserted-Identity
  action                  manipulate
  comparison-type         case-sensitive
  match-value
  msg-type                any
  new-value
  methods
element-rule
  name                    ModPaiHost
  parameter-name
  type                    uri-host
  action                  replace
  match-val-type         any
  comparison-type         case-sensitive
  match-value
  new-value               $LOCAL_IP
element-rule
  name                    ModPaiPort
  parameter-name
  type                    uri-port
  action                  replace
  match-val-type         any
  comparison-type         case-sensitive
  match-value
  new-value               $LOCAL_PORT
last-modified-by        admin@ console
last-modified-date      2010-06-28 18:32:02
sip-manipulation
  name                    ModAvayaUris
  description             Modify R-URI, From & To Host Parts For Avaya
  header-rule
    name                  ModRuri
    header-name           request-uri
    action                manipulate

```

| | |
|-----------------|----------------|
| comparison-type | case-sensitive |
| match-value | |
| msg-type | any |
| new-value | |
| methods | |
| element-rule | |
| name | ModRuriHost |
| parameter-name | |
| type | uri-host |
| action | replace |
| match-val-type | any |
| comparison-type | case-sensitive |
| match-value | |
| new-value | \$REMOTE_IP |
| header-rule | |
| name | ModFrom |
| header-name | From |
| action | manipulate |
| comparison-type | case-sensitive |
| match-value | |
| msg-type | any |
| new-value | |
| methods | |
| element-rule | |
| name | ModFromHost |
| parameter-name | |
| type | uri-host |
| action | replace |
| match-val-type | any |
| comparison-type | case-sensitive |
| match-value | |
| new-value | \$LOCAL_IP |
| header-rule | |
| name | ModTo |
| header-name | To |
| action | manipulate |
| comparison-type | case-sensitive |
| match-value | |
| msg-type | any |
| new-value | |
| methods | |
| element-rule | |
| name | ModToHost |
| 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@192.168.1.6 |
| last-modified-date | 2010-09-14 17:35:29 |
| sip-manipulation | |
| name | CoreNoasEgress |
| description | Core NOAS Egress HMR |
| header-rule | |
| name | CallModAvayaUris |
| header-name | From |
| action | sip-manip |
| comparison-type | case-sensitive |
| match-value | |
| msg-type | any |
| new-value | ModAvayaUris |
| methods | |
| header-rule | |
| name | ModFrom |
| header-name | From |
| action | manipulate |
| comparison-type | case-sensitive |
| match-value | |
| msg-type | any |
| new-value | |
| methods | |
| element-rule | |
| name | ModFromPort |
| parameter-name | |
| type | uri-port |
| action | replace |
| match-val-type | any |
| comparison-type | case-sensitive |
| match-value | |
| new-value | \$LOCAL_PORT |
| header-rule | |
| name | ModTo |
| header-name | To |
| action | manipulate |
| comparison-type | case-sensitive |
| match-value | |
| msg-type | any |
| new-value | |
| methods | |
| element-rule | |

| | |
|--------------------|-------------------------|
| name | ModToPort |
| parameter-name | |
| type | uri-port |
| action | replace |
| match-val-type | any |
| comparison-type | case-sensitive |
| match-value | |
| new-value | \$REMOTE_PORT |
| last-modified-by | admin@ console |
| last-modified-date | 2010-06-29 08:09:15 |
| sip-manipulation | |
| name | AccessNoasIngress |
| description | Access NOAS Ingress HMR |
| header-rule | |
| name | AddUserAgentToOptions |
| header-name | User-Agent |
| action | add |
| comparison-type | case-sensitive |
| match-value | |
| msg-type | reply |
| new-value | \$MANIP_STRING |
| methods | OPTIONS |
| last-modified-by | admin@ console |
| last-modified-date | 2010-09-29 17:24:08 |
| steering-pool | |
| ip-address | 192.168.4.9 |
| start-port | 49152 |
| end-port | 65535 |
| realm-id | access-noas |
| network-interface | |
| last-modified-by | admin@192.168.1.6 |
| last-modified-date | 2010-09-08 11:57:15 |
| steering-pool | |
| ip-address | 192.168.3.9 |
| start-port | 49152 |
| end-port | 65535 |
| realm-id | core-noas |
| network-interface | |
| last-modified-by | admin@console |
| last-modified-date | 2010-09-07 15:28:21 |
| system-config | |
| hostname | |
| description | |
| location | |
| 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     192.168.1.1
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
debug-timeout      0
trap-event-lifetime 0
cleanup-time-of-day 00:00
last-modified-by   admin@192.168.1.6
last-modified-date 2010-09-08 12:04:24

```

task done
SBC2#