**Avaya Solution & Interoperability Test Lab**

# Application Notes for Configuring OneStream Networks Global SIP Trunking with Avaya Aura® Communication Manager Evolution Server, Avaya Aura® Session Manager, and Acme Packet 3800 Net-Net Session Border Controller – Issue 1.0

## Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the OneStream Networks Global SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

Enterprise customers with an Avaya SIP-enabled solution can communicate with OneStream Networks' Global SIP Infrastructure over the public Internet, the private OneStream Networks MPLS network or via a third-party MPLS provider and access the PSTN by subscribing to OneStream Networks Global SIP Trunking.

OneStream Networks' Global SIP Trunking service helps businesses maximize their investment in their Avaya IP Telephony infrastructure by delivering reliable, scalable and cost-effective connections that provide global consolidation, redundancy and simplified management of voice traffic.

OneStream Networks is a member of the Avaya 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 the OneStream Networks Global SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, Acme Packet 3800 Net-Net Session Border Controller (SBC) and various Avaya endpoints.

Enterprise customers with an Avaya SIP-enabled solution can communicate with OneStream Networks' Global SIP Infrastructure over the public Internet, the private OneStream Networks MPLS network or via a third-party MPLS provider and access the PSTN by subscribing to OneStream Networks Global SIP Trunking.

OneStream Networks' Global SIP Trunking service helps businesses maximize their investment in their Avaya IP Telephony infrastructure by delivering reliable, scalable and cost-effective connections that provide global consolidation, redundancy and simplified management of voice traffic.

Throughout the remainder of the document, Onestream Networks will be referred to simply as OneStream.

# 2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Onestream Global SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Acme Packet 3800 Net-Net SBC.

## 2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various phone types
  Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types
  Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client)
  Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X® Communicator also supports two

Voice Over IP (VoIP) protocols: H.323 and SIP. Both protocol versions of Communicator were tested.
- Various call types including: local, long distance, international, outbound toll-free, and local directory assistance (411).
- Codec G.711MU and G.729A.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Use of the REFER method.

Items not supported or not tested included the following:
- Inbound toll-free and emergency calls are supported but were not tested.
- Operator services (0) and operator assisted calls (0 + 10 digits) were not supported in the OneStream test environment.
- Codec G.722 was not tested.
- T.38 Fax was not supported in the OneStream test environment.
- Handling of a 302 redirected response was not tested.

## 2.2. Test Results

Interoperability testing of OneStream Global SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **REFER**: If Network Call Redirection is enabled on Communication Manager, the Communication Manager will use the REFER method for transfer operations. The OneStream network returns a 403 Forbidden message in response to the REFER message sent by the enterprise. Thus, Network Call Redirection should be disabled on **Page 4** of the Communication Manager trunk group form (See **Section 5.7**)
- **302 Redirected Response**: A 302 redirected response is another means of requesting the network to redirect the call, similar to the use of the REFER method. Due to the known issue with the use of REFER, this functionality was not tested.

## 2.3. Support

For technical support on OneStream Global SIP Trunking, contact OneStream using the Contact links at www.onestreamnetworks.com or by calling 1-800-869-0315 option 1.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Selecting the **Support Contact Options** link followed by **Maintenance Support** provides the worldwide support directory for Avaya Global Services. Specific numbers are provided for both customers and partners based on the specific type of support or consultation services needed. Some services may require specific Avaya service support agreements. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

# 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to OneStream Global SIP Trunking. This is the configuration used for compliance testing.

The Avaya components used to create the simulated customer site included:

- Avaya S8300D Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya 9600-Series IP telephones (H.323 and SIP)
- Avaya 4600-Series IP telephones (H.323)
- Avaya 1600-Series IP telephones (H.323)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the SBC. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The SBC provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that can not be routed by the PSTN.

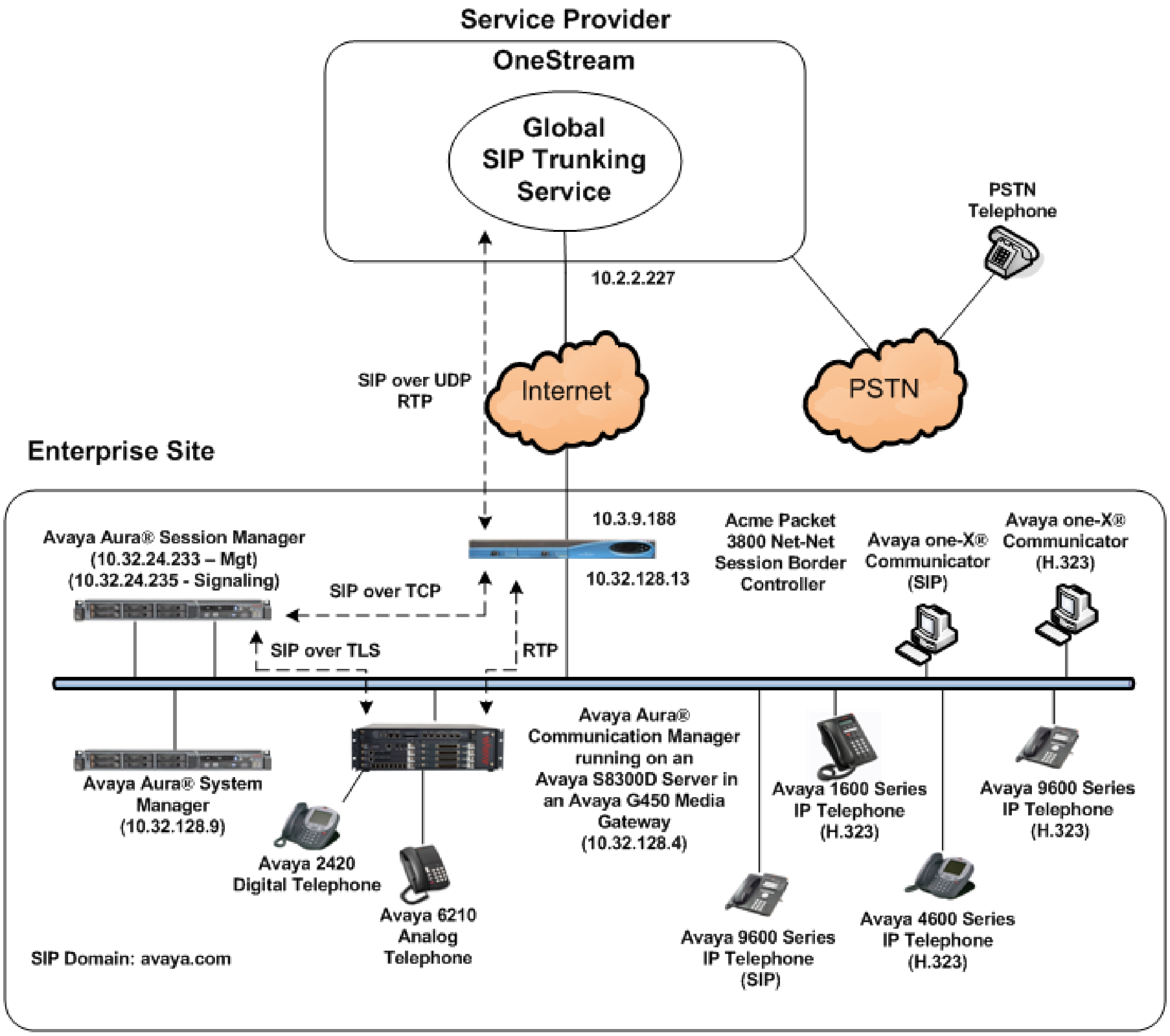



**Figure 1: Avaya IP Telephony Network using OneStream Global SIP Trunking**

A separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the SBC then to Session Manager. Session Manager uses the configured dial patterns (or regular expressions) and routing policies to determine the recipient (in this case the Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the SBC. From the SBC, the call is sent to OneStream Global SIP Trunking.

For the compliance test, the enterprise sent 11 digits in the destination headers (e.g., Request-URI and To) and sent 10 digits in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). OneStream sent 10 digits in both the source and destination headers.

# 4. Equipment and Software Validated

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

| **Avaya IP Telephony Solution Components** | |
|---|---|
| Component | Release |
| Avaya Aura® Communication Manager running on an Avaya S8300D Server | 6.0 SP1<br>(R016x.00.0.345.0-18444)<br>(System Platform 6.0.1.0.5) |
| Avaya G450 Media Gateway | 30.14.0 |
| Avaya Aura® Session Manager running on an Avaya S8800 Server | 6.0 SP1<br>(Build asm-6.0.1.0.601009) |
| Avaya Aura® System Manager running on an Avaya S8800 Server | 6.0 SP1<br>(Build 6.0.7.0)<br>(System Platform 6.0.0.1.11) |
| Avaya 1608 IP Telephone (H.323) | Avaya one-X® Deskphone Value Edition 1.2.2 |
| Avaya 4621SW IP Telephone (H.323) | 2.9.1 |
| Avaya 9640 IP Telephone (H.323) | Avaya one-X® Deskphone Edition 3.1.1 |
| Avaya 9630 IP Telephone (H.323) | Avaya one-X® Deskphone SIP Edition 2.6 |
| Avaya one-X® Communicator (H.323) | 6.0.0.26 |
| Avaya one-X® Communicator (SIP) | 6.0.0.26 |
| Avaya 2420 Digital Telephone | n/a |
| Avaya 6210 Analog Telephone | n/a |
| Acme Packet 3800 Net-Net Session Border Controller | SCX6.2.0 MR-3 GA (Build 691) |
| **OneStream Global SIP Trunking Components** | |
| Component | Release |
| Genband S3 MSX/SBC | 5.2.2.13 |

**Table 1: Equipment and Software Tested**

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

# 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for OneStream Global SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from OneStream. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed and is not discussed here.

The 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. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

## 5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 4000 SIP trunks are available and 25 are in use. 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.

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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 4000  36
           Maximum Concurrently Registered IP Stations: 2400  3
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  25
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

## 5.2. System Features

Use the **change system-parameters feature** command to set the **Trunk-to-Trunk Transfer** field to ***all*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to ***none***.

```
change system-parameters features                              Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

On **Page 9,** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of ***anonymous*** for both.

```
change system-parameters features                              Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code:
          International Access Code:

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

## 5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8300D Server running Communication Manager ***(procr***) and for Session Manager (***sessionMgr***). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                              Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
cmm                  10.32.128.4
default              0.0.0.0
procr                10.32.128.4
procr6               ::
sessionMgr           10.32.24.235
```

## 5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, codecs G.729A and G.711mu were tested using ip-codec-set 2. To use these codecs, enter ***G.729A*** and ***G.711MU*** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields. OneStream Global SIP Trunking also supports G.722 but this codec was not tested.

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

                           IP Codec Set

    Codec Set: 2

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

On **Page 2**, the **Fax Mode** was set to ***off*** since T.38 fax was not supported in the OneStream test environment.

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

                           IP Codec Set

                               Allow Direct-IP Multimedia? n

                    Mode                Redundancy
    FAX             off                  0
    Modem           off                  0
    TDD/TTY         US                   3
```

## 5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 2 was chosen for the service provider trunk. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***avaya.com***. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to ***yes***. This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                        Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              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
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for ip network region 2 will automatically create a complementary table entry on the ip network region 1 form for destination region 2. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4**.

```
change ip-network-region 2                                     Page   4 of  20

 Source Region: 2     Inter Network Region Connection Management     I        M
                                                                     G  A     t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G     c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L     e
 1    2     y    NoLimit                                             n        t
 2    2                                                                all
 3
```

## 5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). For ease of troubleshooting during testing, part of the compliance test was conducted with the **Transport Method** set to ***tcp***. The transport method specified here is used between the Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). This is necessary so Session Manager can distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5062***.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and can not be changed via administration. Later, the **Peer-Server** field will automatically change to ***SM*** once Communication Manager detects its peer as a Session Manager.

- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Avaya S8300D Server running Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***sessionMgr***. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to ***15***. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

```
add signaling-group 3                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                            SIP Enabled LSP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others



   Near-end Node Name: procr                Far-end Node Name: sessionMgr
 Near-end Listen Port: 5062               Far-end Listen Port: 5062
                                       Far-end Network Region: 2

Far-end Domain: avaya.com
                                            Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? n                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 15
```

## 5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 3 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 3                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 3                   Group Type: sip           CDR Reports: y
  Group Name: SP Trunk                  COR: 1        TN: 1        TAC: 1003
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     Number of Members: 5
```

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value comparable to the **Alternate Route Timer** on the signaling group form described in **Section 5.6**.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of ***600*** seconds was used.

```
add trunk-group 3                                               Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 15000

           SCCAN? n                                Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

                                     Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with OneStream. Thus, the **Numbering Format** was set to ***private*** and the **Numbering Format** in the route pattern was set to ***unk-unk*** (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

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

                     Numbering Format: private
                                                 UUI Treatment: service-provider

                                                  Replace Restricted Numbers? y
                                                 Replace Unavailable Numbers? y

                                 Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

On **Page 4**, set the **Network Call Redirection** field to ***n***. Set the **Send Diversion Header** field to ***y***. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to ***101***, the value preferred by OneStream.

```
add trunk-group 3                                               Page   4 of  21
                              PROTOCOL VARIATIONS

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


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
                            Enable Q-SIP? n
```

## 5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the sample configuration, three DID numbers were assigned for testing. These three numbers were assigned to the three extensions 40003, 40005 and 40010. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these three extensions.

```
change private-numbering 0                                      Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext             Trk        Private      Total
Len Code            Grp(s)     Prefix        Len
                                                  Total Administered: 4
 5  4                                        5       Maximum Entries: 240
 5  40003          3         7325551234      10
 5  40005          3         7325551235      10
 5  40010          3         7325551236      10
```

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 4 will send the calling party number as the **Private Prefix** plus the extension number.

```
change private-numbering 0                                      Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext             Trk        Private      Total
Len Code            Grp(s)     Prefix        Len
                                                  Total Administered: 1
 5  4              3         73255           10     Maximum Entries: 240
```

Even though private numbering was selected, currently the number used in the SIP Diversion header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table.

```
change public-unknown-numbering 0                                Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                  Total Administered: 4
 5  4                                       5        Maximum Entries: 240
 5  40003         3         7325551234      10
 5  40005         3         7325551235      10    Note: If an entry applies to
 5  40010         3         7325551236      10    a SIP connection to Avaya
                                                  Aura(tm) Session Manager,
                                                  the resulting number must
                                                  be a complete E.164 number.
```

## 5.9. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration is illustrated below with little elaboration. Use the **change dialplan analysis** command to define a dialed string beginning with 9 of length 1 as a feature access code (**fac**).

```
change dialplan analysis                                        Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1           4   dac
   4           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

Use the **change feature-access-codes** command to configure ***9*** as the **Auto Route Selection (ARS) – Access Code 1**.

```
change feature-access-codes                                     Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *01    All: *02    Deactivation: *03
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 2 which contains the SIP trunk to the service provider (as defined next).

```
change ars analysis 0                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 2

          Dialed           Total      Route     Call   Node  ANI
          String          Min  Max   Pattern    Type   Num   Reqd
    0                     1    1      2         op           n
    0                     11   11     2         op           n
    00                    2    2      2         op           n
    011                   10   18     2         intl         n
    1800                  11   11     2         fpna         n
    1877                  11   11     2         fpna         n
    1908                  11   11     2         fpna         n
    411                   3    3      2         svcl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 2 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 3 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: ***1*** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format**: ***unk-unk*** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 5.7**.
- **LAR**: ***next***

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

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               unk-unk   next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
```

# 6. Configure Avaya Aura® Session Manager

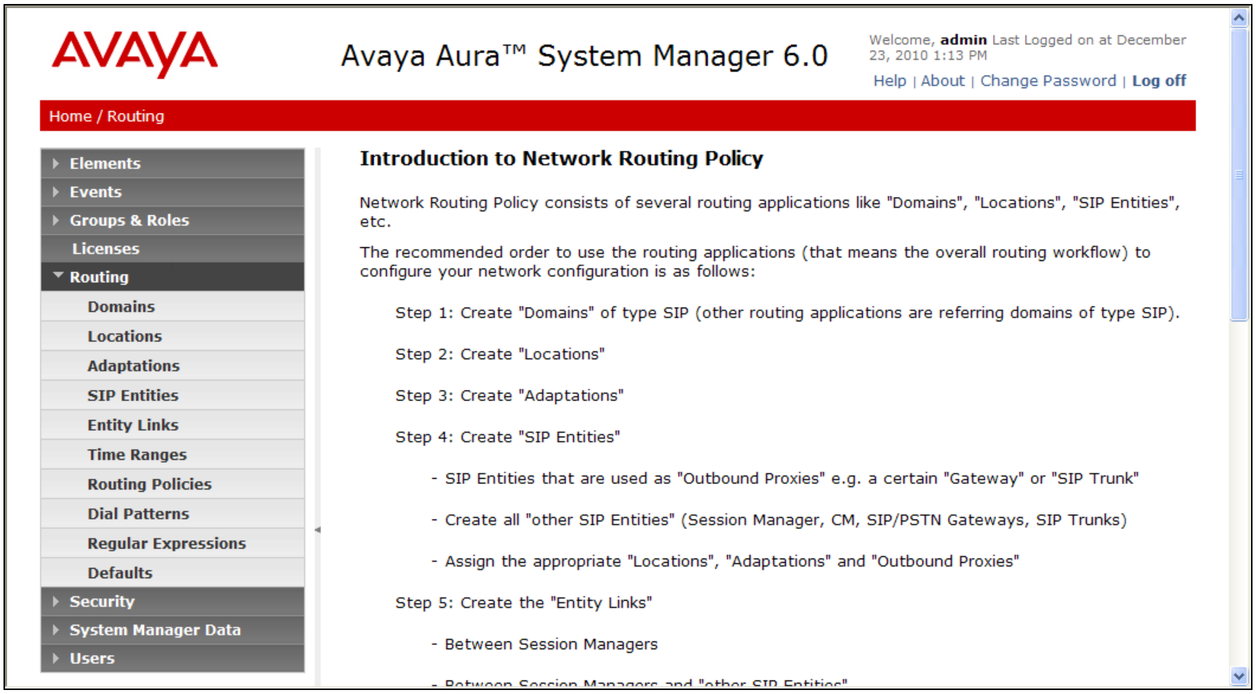
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- Adaptation module to perform dial plan manipulation
- SIP Entities corresponding to Communication Manager, the SBC and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Regular Expressions, which also can be used to route calls
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

## 6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The screen shown below is then displayed. The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Routing** link shown below.

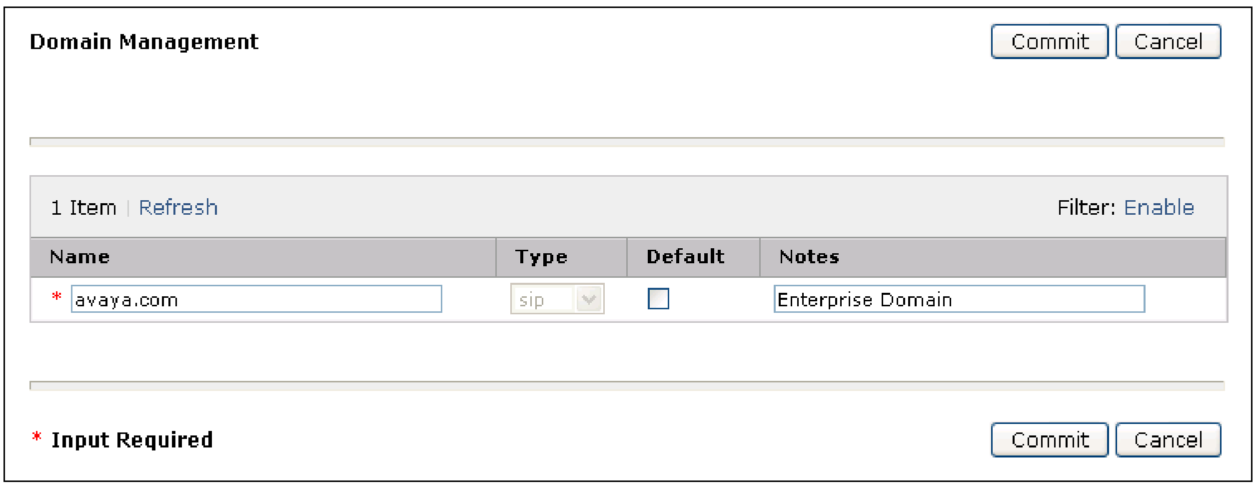


## 6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (***avaya.com***). Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select ***sip*** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the enterprise domain.



## 6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown).

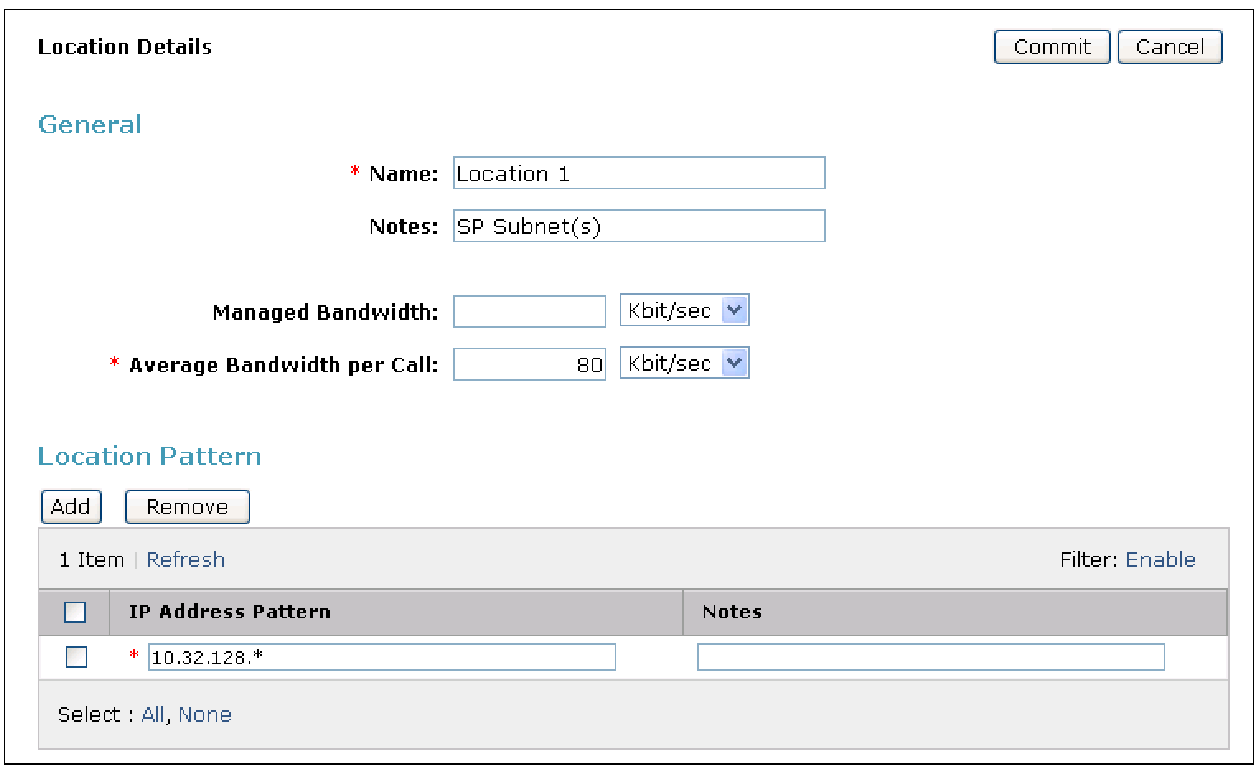
In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

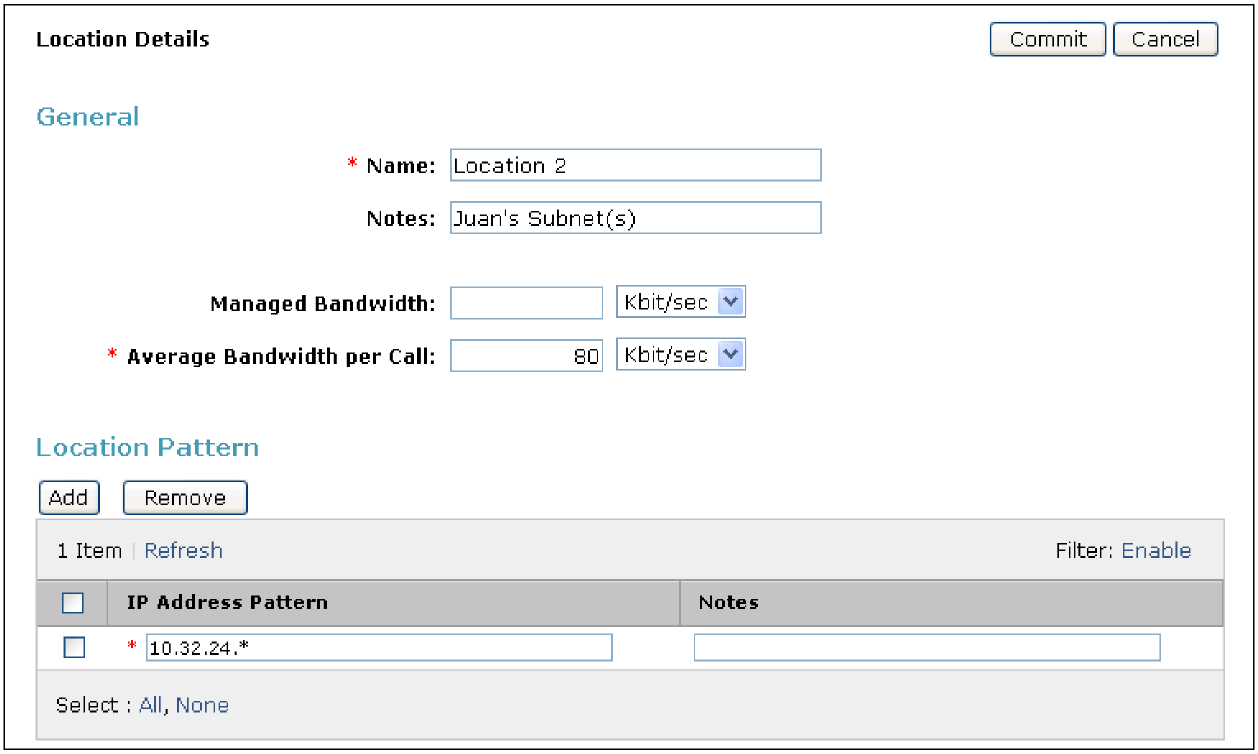
In the **Location Pattern** section, click **Add** and enter the following values. Use default values for all remaining fields.

- **IP Address Pattern:** An IP address pattern used to identify the location.
- **Notes:** Add a brief description (optional).

The screen below shows the addition of the location named ***Location 1***, which includes all equipment on the ***10.32.128.x*** subnet including Communication Manager, and the SBC. Click **Commit** to save.



Repeat the preceding procedure to create **Location 2** which includes all equipment on the ***10.32.24.x*** subnet which includes the Session Manager.



## 6.4. Add Adaptation Module

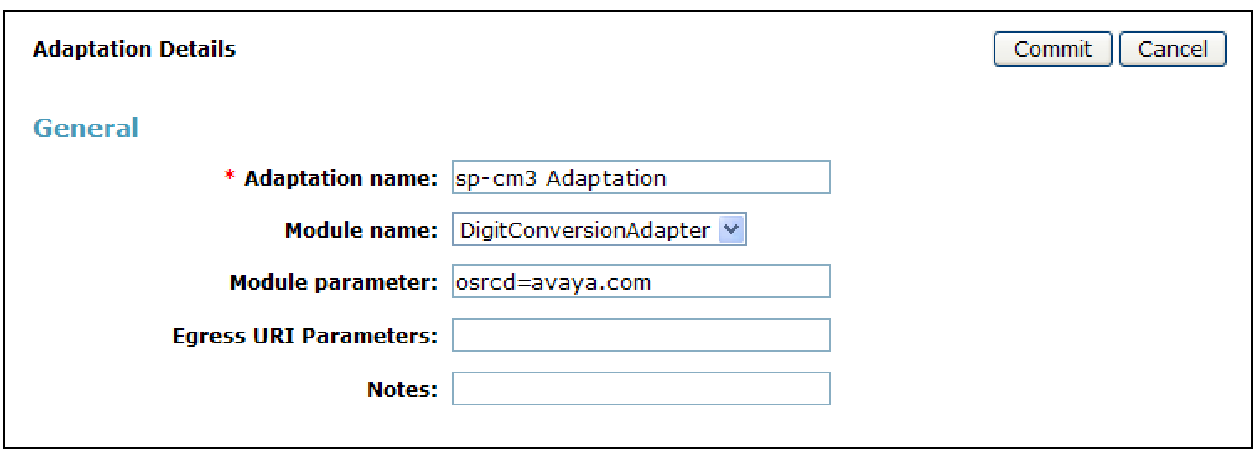
Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products.

For OneStream interoperability, two adaptations are needed. The first adaptation is applied to the Communication Manager SIP entity and maps inbound DID numbers from OneStream to local Communication Manager extensions. In addition, this adaptation converts the domain part of the inbound PAI header to the enterprise domain (***avaya.com***). The second adaptation is applied to the SBC SIP entity and converts the domain part of the outbound Request URI header from Session Manager containing the enterprise domain to the OneStream SIP proxy IP address.

To create the adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields.

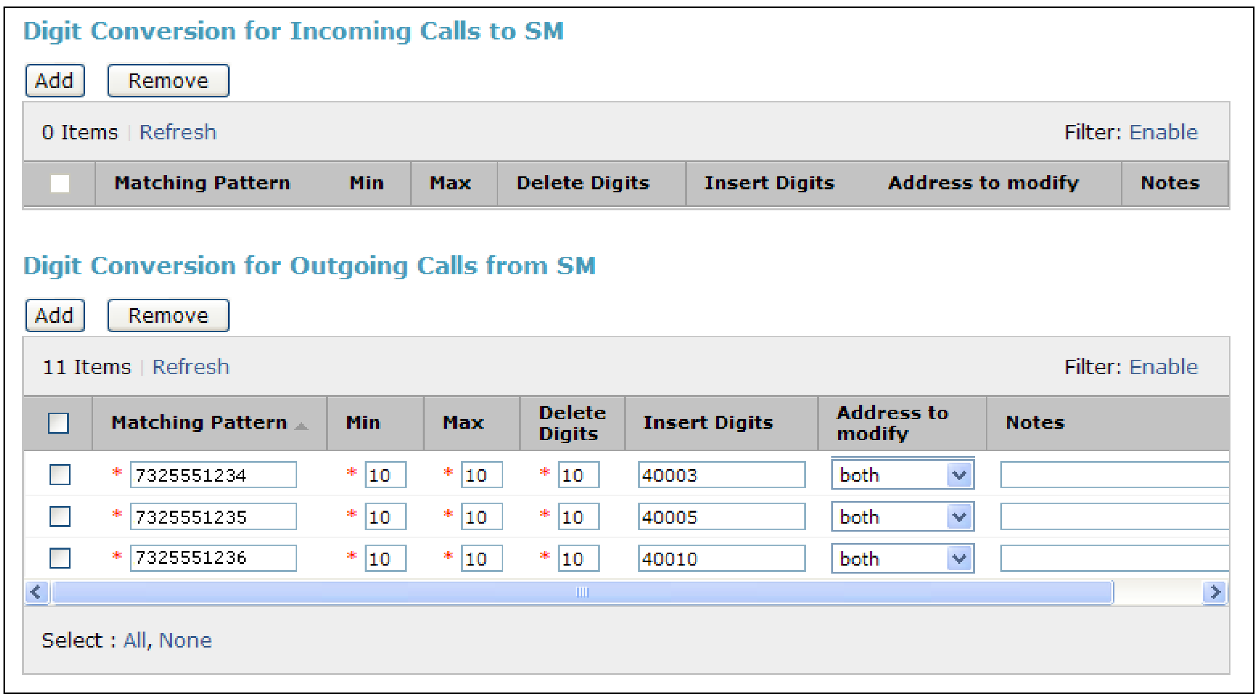
- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***osrcd=avaya.com***. This is the OverrideSourceDomain parameter. This parameter replaces the domain in the inbound PAI header with the given value. This parameter must match the value used for the **Far-end Domain** setting on the Communication Manager signaling group form in **Section 5.6**.



To map inbound DID numbers from OneStream to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select **both**.

Click **Commit** to save.



Digit Conversion for Incoming Calls to SM

Add Remove

0 Items | Refresh Filter: Enable

| | Matching Pattern | Min | Max | Delete Digits | Insert Digits | Address to modify | Notes |
|---|---|---|---|---|---|---|---|

Digit Conversion for Outgoing Calls from SM

Add Remove

11 Items | Refresh Filter: Enable

| | Matching Pattern | Min | Max | Delete Digits | Insert Digits | Address to modify | Notes |
|---|---|---|---|---|---|---|---|
| | * 7325551234 | * 10 | * 10 | * 10 | 40003 | both | |
| | * 7325551235 | * 10 | * 10 | * 10 | 40005 | both | |
| | * 7325551236 | * 10 | * 10 | * 10 | 40010 | both | |

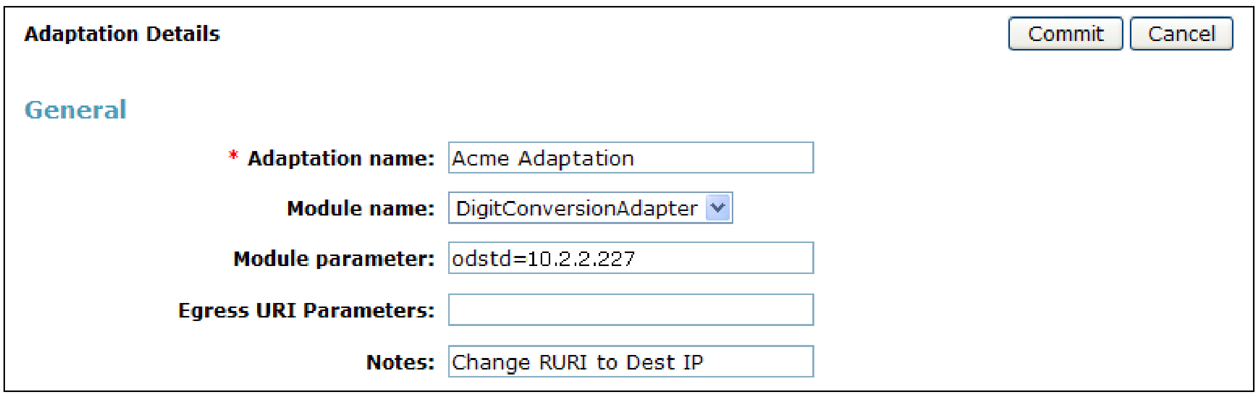
Select : All, None

To create the adaptation that will be applied to the SBC SIP entity, navigate to **Routing → Adaptations** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***odstd=10.2.2.227***. This is the OverrideDestinationDomain parameter. This parameter replaces the domain in the Request URI header with the given value for outbound only.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



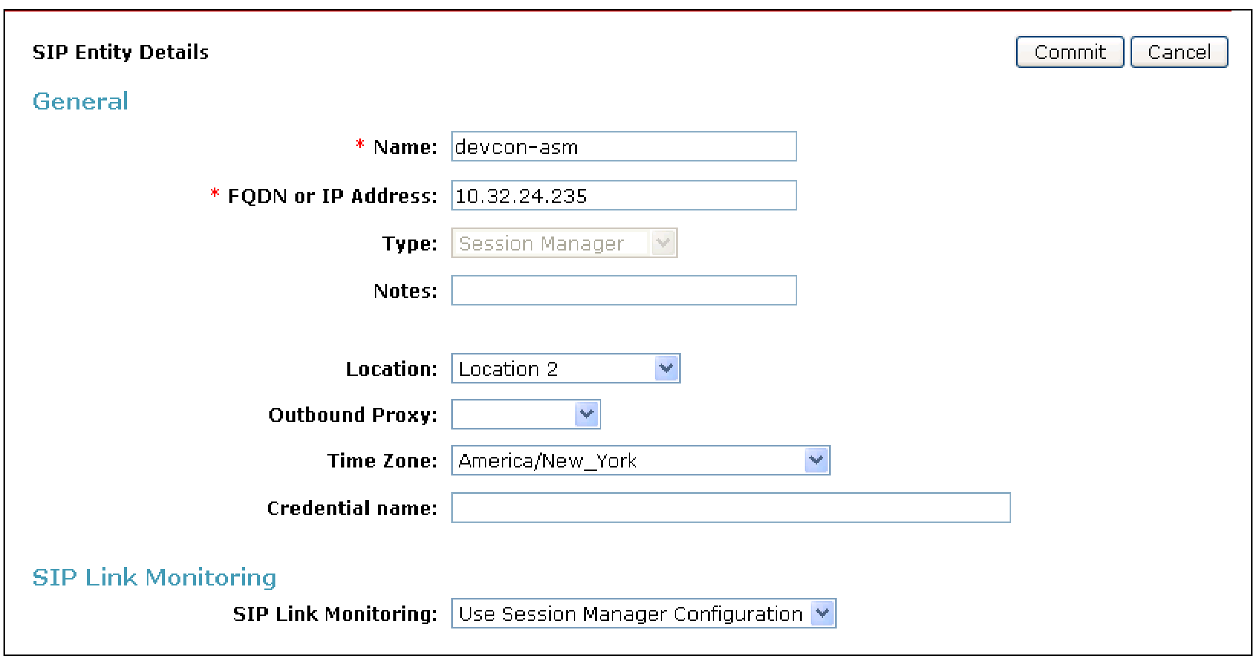
## 6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the SBC. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** for the SBC.
- **Adaptation:** This field is only present if **Type** is not set to ***Session Manager***. If applicable, select the appropriate **Adaptation name** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the virtual SM-100 Security Module is entered for **FQDN or IP Address**.



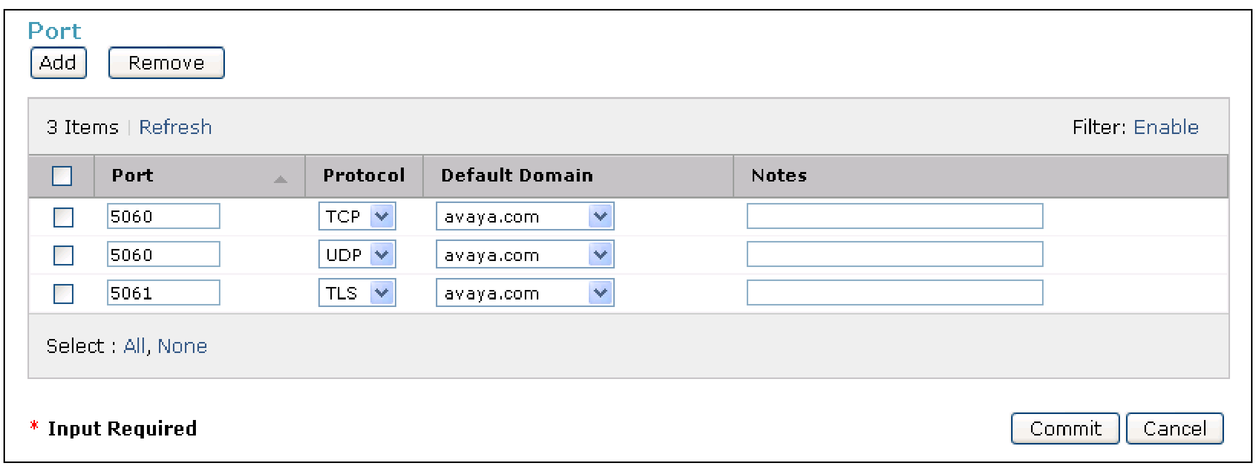
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

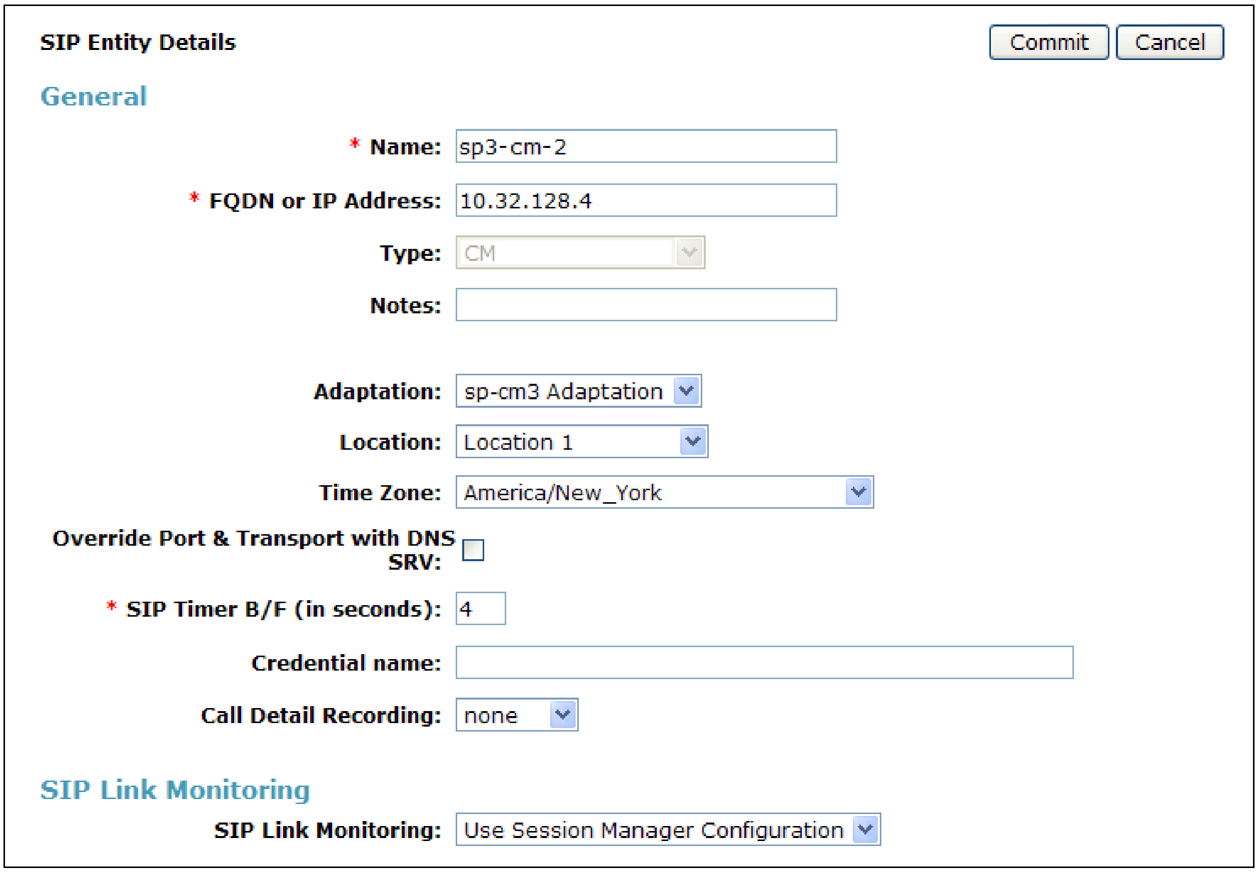
- **Port:** Port number on which the Session Manager can listen for SIP requests. To achieve interoperability for the compliance test, it was not necessary to add to this table the non-standard port (5062) used for the entity link between Communication Manager and Session Manager. This port is specified in the SIP entity link definition in **Section 6.6**. However, as a best practice, all ports used by the Session Manager to listen for SIP requests should be defined in this table. This includes all ports that are defined for use by an entity link such as port 5062.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.

Defaults can be used for the remaining fields. Click **Commit** to save.

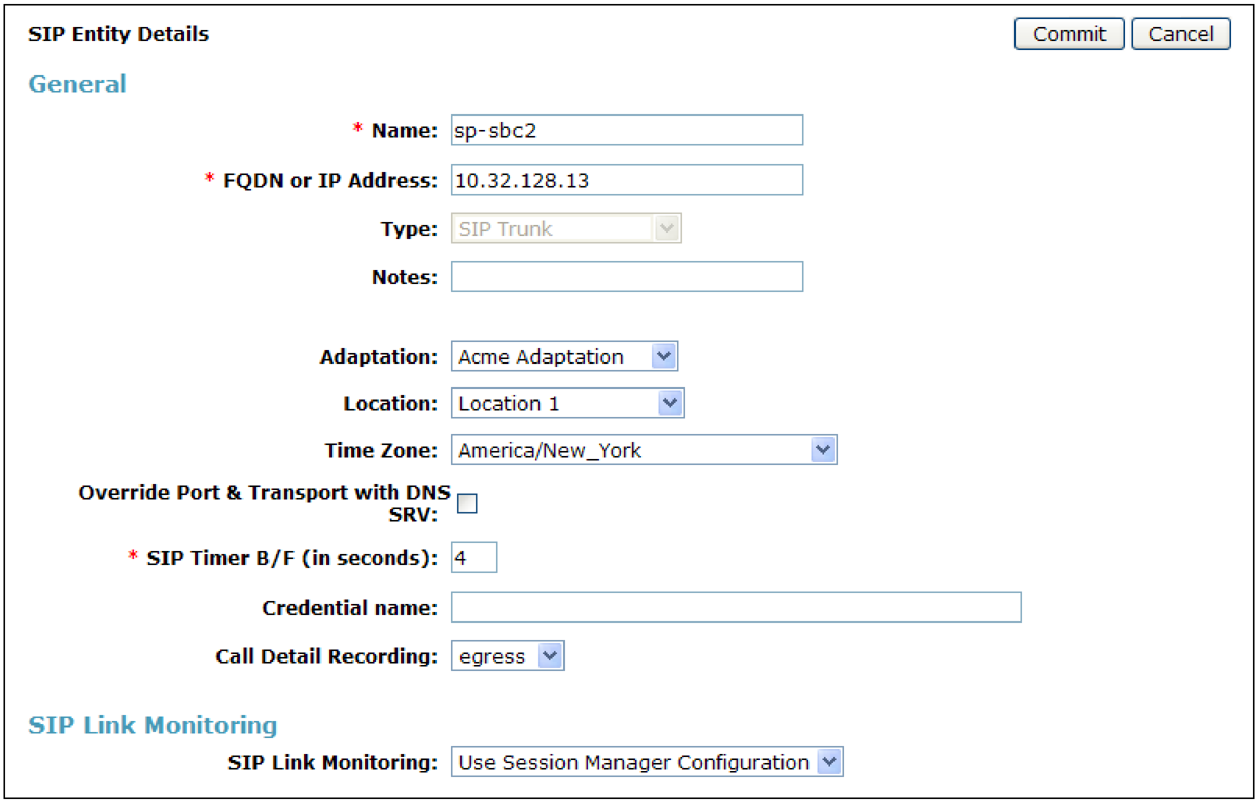
For the compliance test, three **Port** entries were added.



The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, this requires the creation of a separate SIP entity for Communication Manager than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the Avaya S8300D Server running Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 6.4**.



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



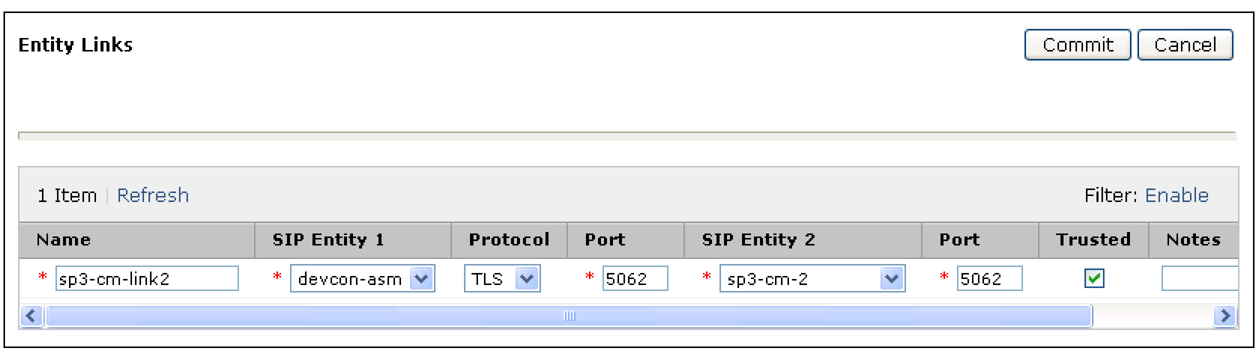
## 6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

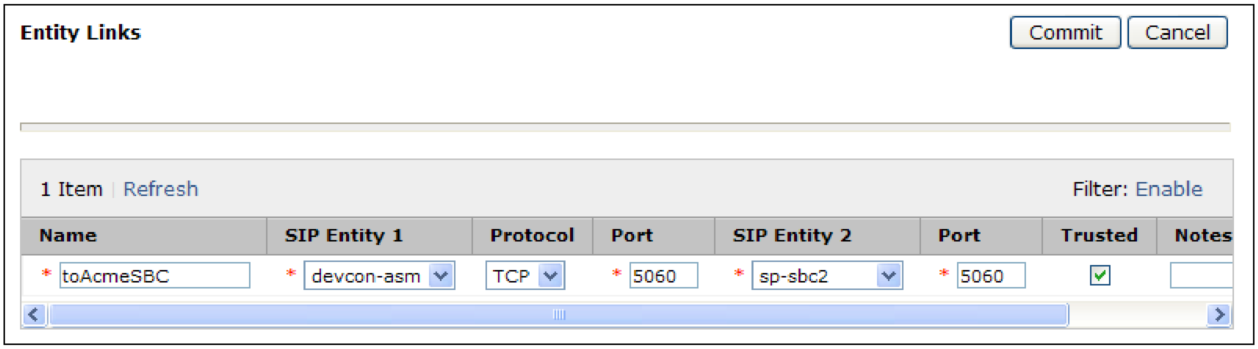
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.*

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and the SBC. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager:



Entity Link to the SBC:



## 6.7. Add Routing Policies

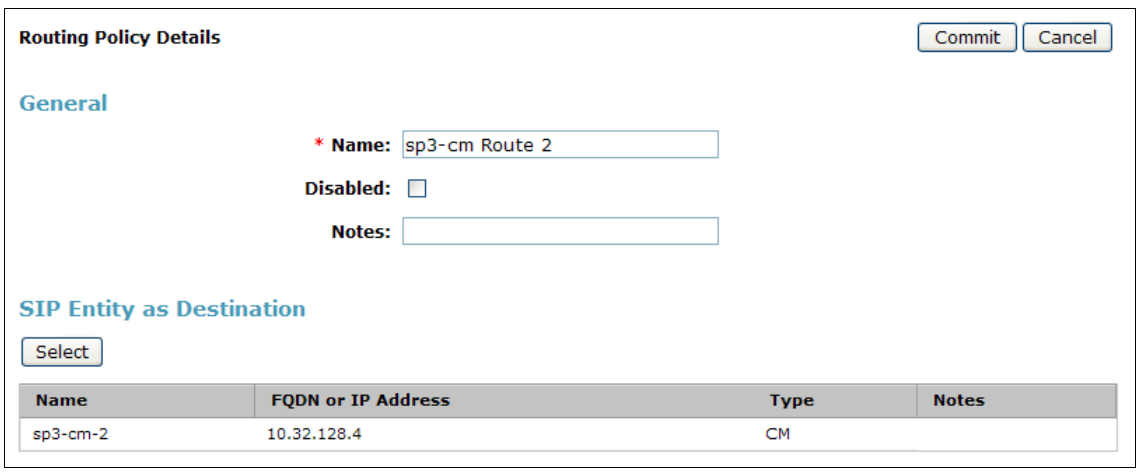
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

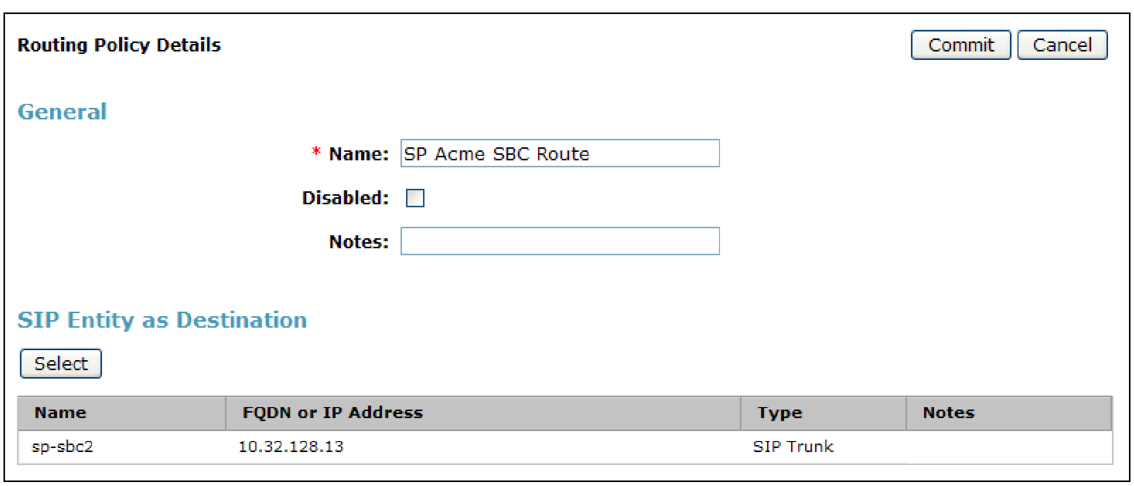
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select.** The selected SIP Entity displays on the Routing Policy Details page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager and the SBC.



## 6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to OneStream and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

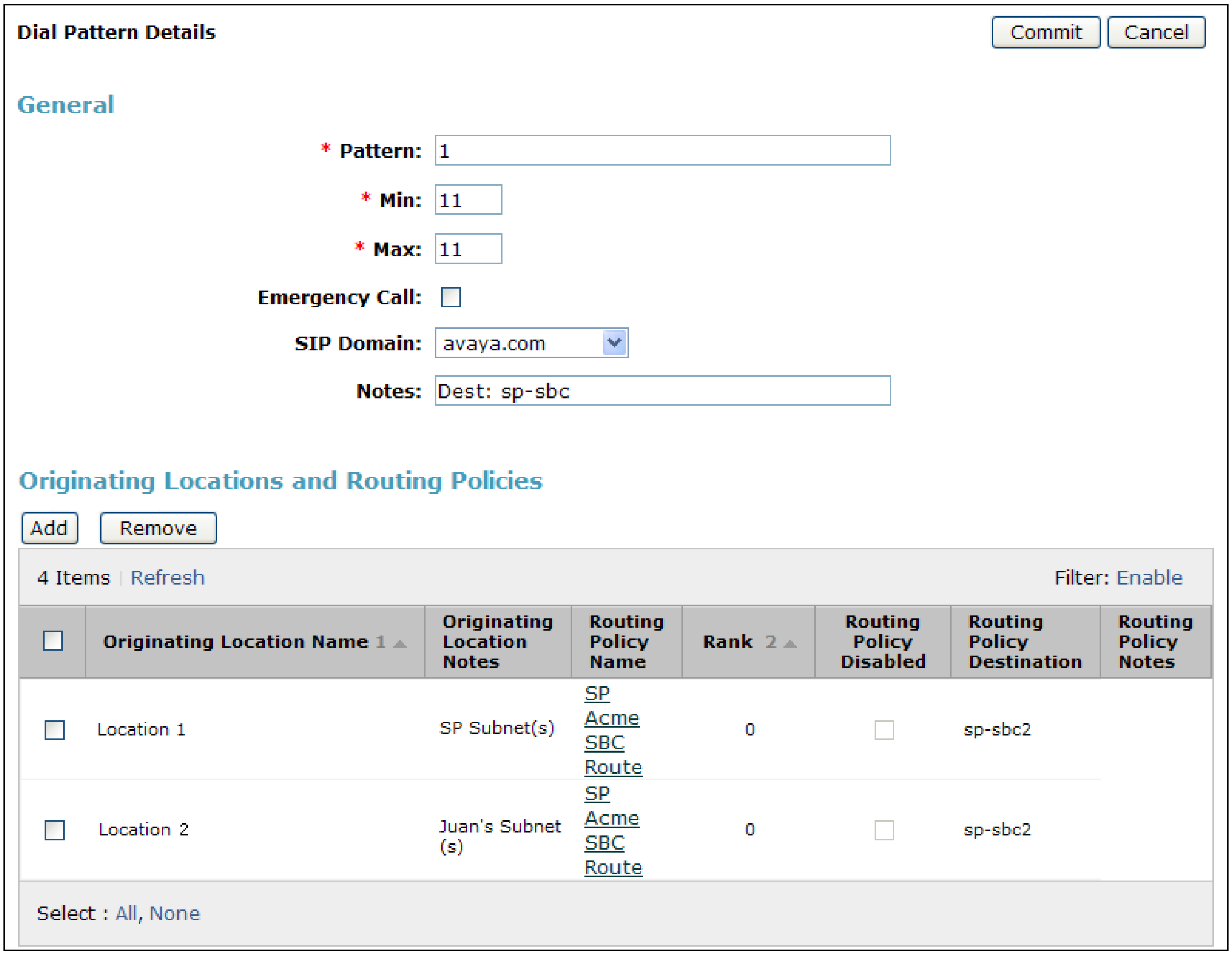
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that 11 digit numbers that begin with a 1 and have a destination domain of ***avaya.com*** from ***Location 1*** or ***Location 2*** uses route policy ***SP AcmeSBC route***.



**Dial Pattern Details** Commit Cancel

**General**

* **Pattern:** 1

* **Min:** 11

* **Max:** 11

**Emergency Call:**

**SIP Domain:** avaya.com

**Notes:** Dest: sp-sbc

**Originating Locations and Routing Policies**

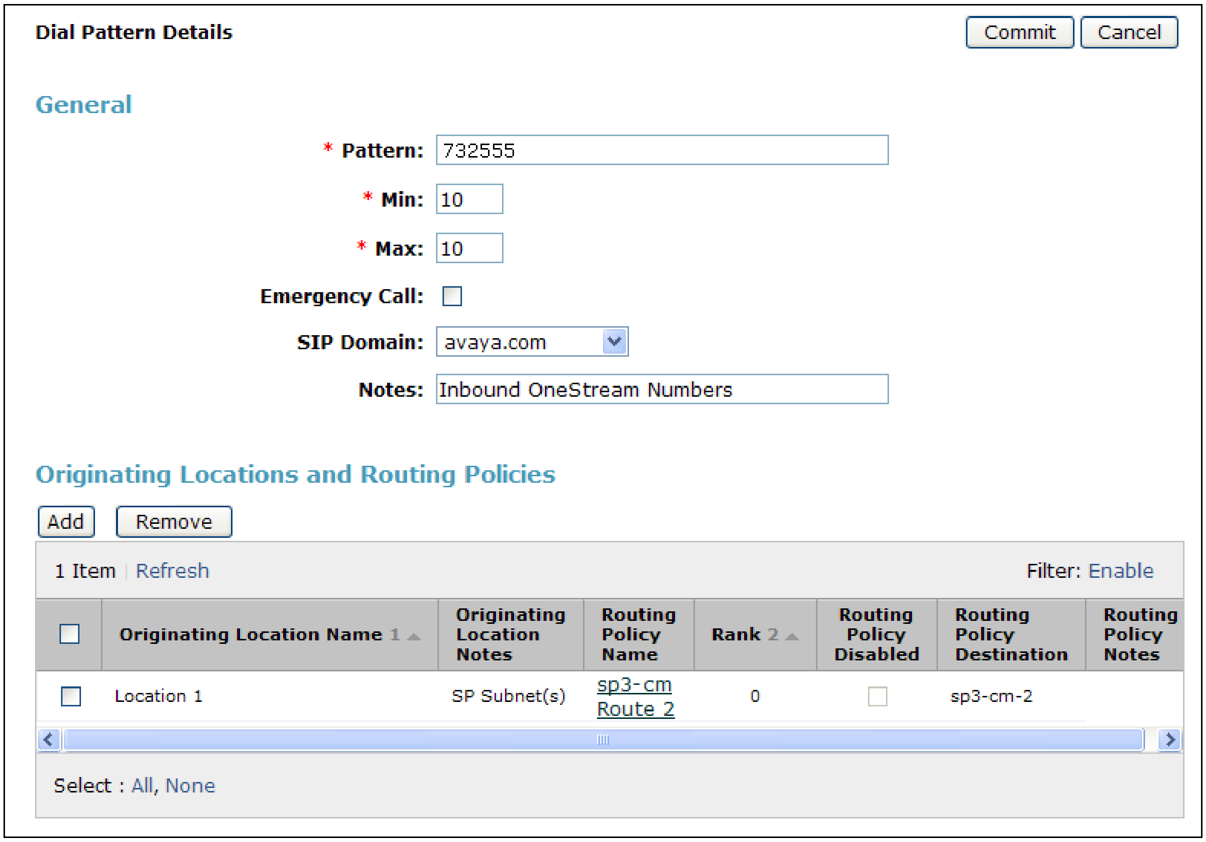
Add Remove

4 Items | Refresh Filter: Enable

| | Originating Location Name 1 | Originating Location Notes | Routing Policy Name | Rank 2 | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|---|---|---|---|---|---|---|---|
| | Location 1 | SP Subnet(s) | SP Acme SBC Route | 0 | | sp-sbc2 | |
| | Location 2 | Juan's Subnet (s) | SP Acme SBC Route | 0 | | sp-sbc2 | |

Select : All, None

The second example shows that 11 digit numbers that start with ***732555*** to domain ***avaya.com*** and originating from ***Location 1*** uses route policy ***sp3-cm Route 2***. These are the DID numbers assigned to the enterprise from OneStream. Location 1 is selected because these calls come from the SBC which resides in Location 1.


**Dial Pattern Details** Commit Cancel

**General**

* Pattern: 732555

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Inbound OneStream Numbers

**Originating Locations and Routing Policies**

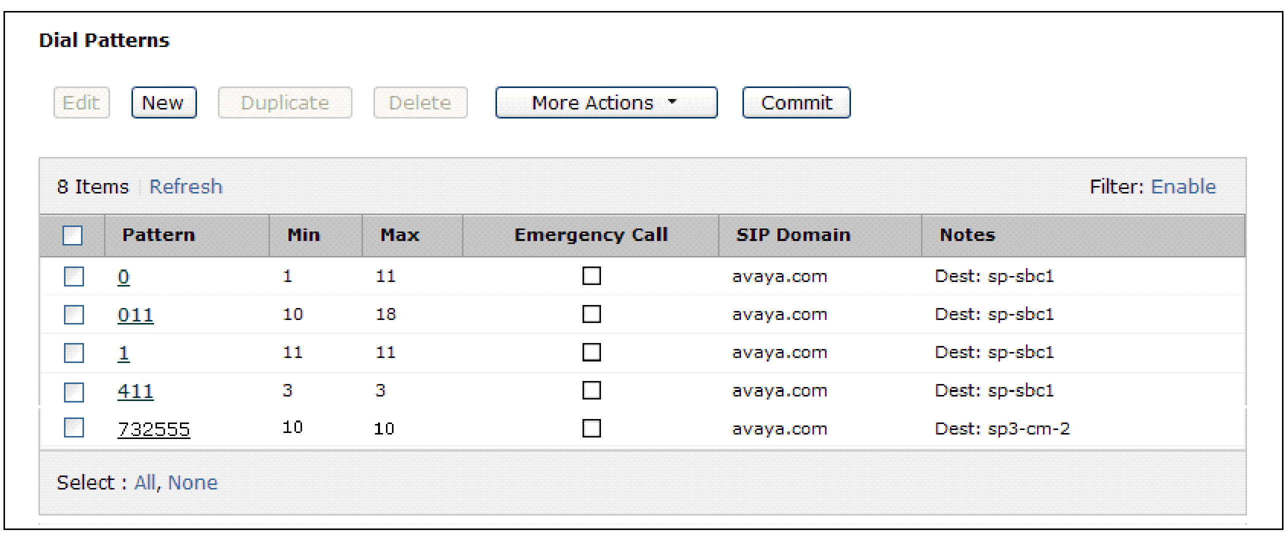
Add Remove

1 Item | Refresh Filter: Enable

| ☐ | Originating Location Name 1 | Originating Location Notes | Routing Policy Name | Rank 2 | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|---|---|---|---|---|---|---|---|
| ☐ | Location 1 | SP Subnet(s) | sp3-cm Route 2 | 0 | ☐ | sp3-cm-2 | |

Select : All, None

The complete list of dial patterns defined for the compliance test is shown below.


**Dial Patterns**

Edit New Duplicate Delete More Actions Commit

8 Items | Refresh Filter: Enable

| ☐ | Pattern | Min | Max | Emergency Call | SIP Domain | Notes |
|---|---|---|---|---|---|---|
| ☐ | 0 | 1 | 11 | ☐ | avaya.com | Dest: sp-sbc1 |
| ☐ | 011 | 10 | 18 | ☐ | avaya.com | Dest: sp-sbc1 |
| ☐ | 1 | 11 | 11 | ☐ | avaya.com | Dest: sp-sbc1 |
| ☐ | 411 | 3 | 3 | ☐ | avaya.com | Dest: sp-sbc1 |
| ☐ | 732555 | 10 | 10 | ☐ | avaya.com | Dest: sp3-cm-2 |

Select : All, None

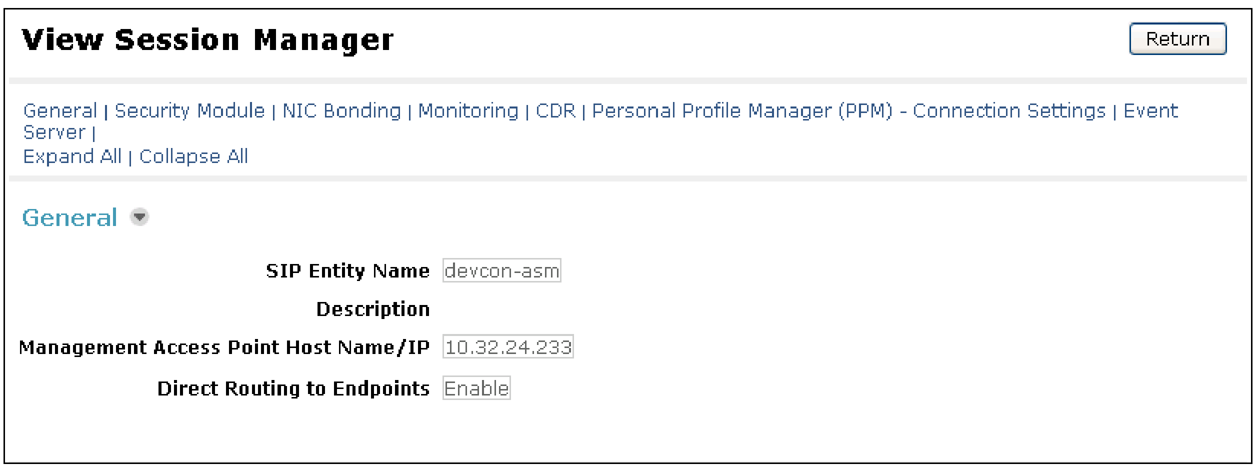
## 6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

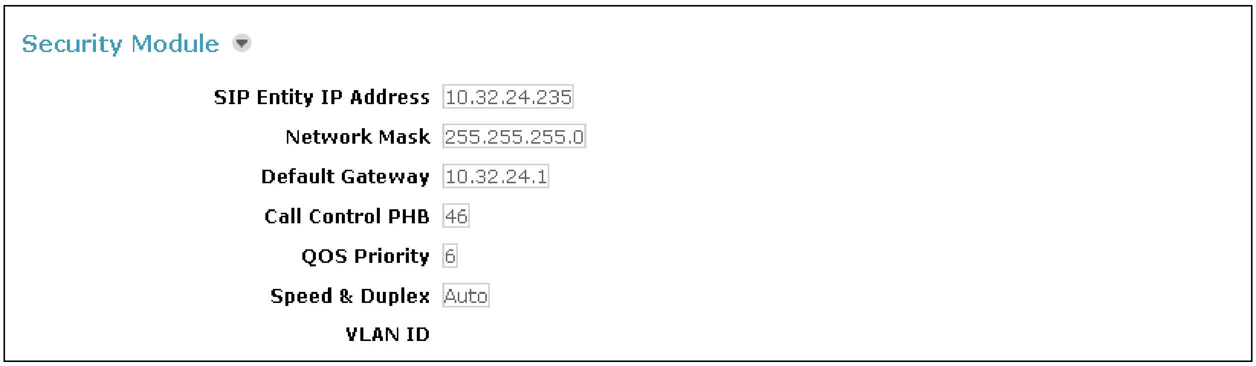
The screen below shows the Session Manager values used for the compliance test.



In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.



# 7. Configure Acme Packet 3800 Net-Net Session Border Controller

The following sections describe the provisioning of the Acme Packet 3800 Net-Net SBC. Only the Acme Packet provisioning required for the reference configuration is described in these Application Notes. The resulting SBC configuration file is shown in **Appendix A**.

The Acme Packet SBC was configured using the Acme Packet CLI via a serial console port connection. An IP remote connection to a management port is also supported. The following are the generic steps for configuring various elements.

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to (*configure)#*.
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4-8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until returned to the Superuser prompt.
10. Type **save-configuration** to save the configuration.
11. Type **activate-configuration** to activate the configuration.

Once the provisioning is complete, the configuration may be verified by entering the ***show running-config*** command.

## 7.1. Physical Interfaces

This section defines the physical interfaces to the private enterprise and public networks.

### 7.1.1. Public Interface

Create a phy-interface to the public side of the Acme.

1. Enter **system → phy-interface**
2. Enter **name → s0p0**
3. Enter **operation-type → Media**
4. Enter **port → 0**
5. Enter **slot → 0**
6. Enter **duplex-mode → FULL**
7. Enter **speed → 100**
8. Enter **done**
9. Enter **exit**

### 7.1.2. Private Interface

Create a phy-interface to the private enterprise side of the Acme.

1. Enter **system → phy-interface**
2. Enter **name → s1p0**
3. Enter **operation-type → Media**
4. Enter **port → 0**
5. Enter **slot → 1**
6. **virtual-mac → 00:08:25:a0:f4:8a**

   Virtual MAC addresses are assigned based on the MAC address assigned to the Acme. This MAC address is found by entering the command *show prom-info mainboard* (e.g. **00 08 25 a0 fa 80**). To define a virtual MAC address, replace the last digit with **8** thru **f**.
7. Enter **duplex-mode → FULL**
8. Enter **speed → 100**
9. Enter **done**
10. Enter **exit**

## 7.2. Network Interfaces

This section defines the network interfaces to the private enterprise and public IP networks.

### 7.2.1. Public Interface

Create a network-interface to the public side of the Acme.

1. Enter **system → network-interface**
2. Enter **name → s0p0**
3. Enter **ip-address → 10.3.9.188**
4. Enter **netmask → 255.255.255.128**
5. Enter **gateway → 10.3.9.129**
6. Enter **dns-ip-primary → 10.3.16.67**
7. Enter **hip-ip-list → 10.3.9.188**
8. Enter **icmp-ip-list → 10.3.9.188**
9. Enter **done**
10. Enter **exit**

### 7.2.2. Private Interface

Create a network-interface to the private enterprise side of the Acme.

1. Enter **system → network-interface**
2. Enter **name → s1p0**
3. Enter **ip-address → 10.32.128.13**
4. Enter **netmask → 255.255.255.0**
5. Enter **gateway → 10.32.128.254**
6. Enter **hip-ip-list → 10.32.128.13**
7. Enter **icmp-ip-list → 10.32.128.13**
8. Enter **done**
9. Enter **exit**

## 7.3. Realms

Realms are used as a basis for determining egress and ingress associations between physical and network interfaces as well as applying header manipulation such as NAT.

### 7.3.1. Outside Realm

Create a realm for the external network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → EXTERNAL**
3. Enter **network-interfaces → s0p0:0**
4. Enter **done**
5. Enter **exit**

### 7.3.2. Inside Realm

Create a realm for the internal network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → INTERNAL2**
3. Enter **network-interfaces → s1p0:0**
4. Enter **done**
5. Enter **exit**

## 7.4. Steering-Pools

Steering pools define sets of ports that are used for steering media flows thru the Acme.

### 7.4.1. Outside Steering-Pool

Create a steering-pool for the outside network.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 10.3.9.188**
3. Enter **start-port → 49152**
4. Enter **end-port → 65535**
5. Enter **realm-id → EXTERNAL**
6. Enter **done**
7. Enter **exit**

### 7.4.2. Inside Steering-Pool

Create a steering-pool for the inside network.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 10.32.128.13**
3. Enter **start-port → 2048**
4. Enter **end-port → 65535**
5. Enter **realm-id → INTERNAL2**
6. Enter **done**
7. Enter **exit**

## 7.5. Media-Manager

Verify that the media-manager process is enabled.

1. Enter **media-manager → media-manager**
2. Enter **select → show** Verify that the media-manager state is enabled. If not, perform steps 3-5.
3. Enter **state → enabled**
4. Enter **done**
5. Enter **exit**

## 7.6. SIP Configuration

This command sets the values for the Acme Packet SIP operating parameters. The home-realm defines the SIP daemon location, and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere.

1. Enter **session-router → sip-config**
2. Enter **state → enabled**
3. Enter **operation-mode → dialog**
4. Enter **home-realm-id → INTERNAL2**
5. Enter **egress-realm-id →**
6. Enter **nat-mode → Public**
7. Enter **done**
8. Enter **exit**

## 7.7. SIP Interfaces

The SIP interface defines the SIP signaling interface (IP address and port) on the Acme Packet. SIP header manipulations can be applied to the SIP interface level.

### 7.7.1. Outside SIP Interface

Create a sip-interface for the outside network.

1. Enter **session-router → sip-interface**
2. Enter **state → enabled**
3. Enter **realm-id → EXTERNAL**
4. Enter **sip-port**
   a. Enter **address → 10.3.9.188**
   b. Enter **port → 5060**
   c. Enter **transport-protocol → UDP**
   d. Enter **allow-anonymous → agents-only**
   e. Enter **done**
   f. Enter **exit**
5. Enter **stop-recurse → 401,407**
6. Enter **done**
7. Enter **exit**

### 7.7.2. Inside SIP Interface

Create a sip-interface for the inside network.

1. Enter **session-router → sip-interface**
2. Enter **state → enabled**
3. Enter **realm-id → INTERNAL2**
4. Enter **sip-port**
    a. Enter **address → 10.32.128.13**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → TCP**
    d. Enter **allow-anonymous → all**
    e. Enter **done**
    f. Enter **exit**
5. Enter **stop-recurse → 401,407**
6. Enter **done**
7. Enter **exit**

## 7.8. Session-Agents

A session-agent defines an internal "next hop" signaling entity for the SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent is defined for the service provider (outside) and Session Manager (inside). SIP header manipulations can be applied to the SIP agent level.

### 7.8.1. Outside Session-Agent

Create a session-agent for the outside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 10.2.2.227**
3. Enter **ip-address → 10.2.2.227**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP**
8. Enter **realm-id → EXTERNAL**
9. Enter **description → OneStream**
10. Enter **ping-method →**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **out-manipulationid → outManToSP**
14. Enter **done**
15. Enter **exit**

### 7.8.2. Inside Session-Agent

Create a session-agent for the inside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 10.32.24.235**
3. Enter **ip-address → 10.32.24.235**

4. Enter **port → 5060**
5. Enter **transport-method → StaticTCP**
6. Enter **realm-id → INTERNAL2**
7. Enter **description → SM_SPenv**
8. Enter **ping-method →**
9. Enter **ping-interval → 60**
10. Enter **ping-send-mode → keep-alive**
11. Enter **in-manipulationid → inManFromSM**
12. Enter **done**
13. Enter **exit**

## 7.9. Local Policies

Local policies allow SIP requests from the **INTERNAL2** realm to be routed to the Service Provider Session Agent in the **EXTERNAL** realm (and vice-versa).

### 7.9.1. INTERNAL2 to EXTERNAL

Create a local-policy for the **INSIDE** realm.

1. Enter **session-router → local-policy**
2. Enter **from-address → ***
3. Enter **to-address → ***
4. Enter **source-realm → INTERNAL2**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 10.2.2.227**
    b. Enter **realm → EXTERNAL**
    c. Enter **terminate-recursion → enabled**
    d. Enter **app-protocol → SIP**
    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

### 7.9.2. EXTERNAL to INTERNAL2

Create a local-policy for the **EXTERNAL** realm.

1. Enter **session-router → local-policy**
2. Enter **from-address → ***
3. Enter **to-address → "7325551234 7325551235 7325551236"**
4. Enter **source-realm → EXTERNAL**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 10.32.24.235**
    b. Enter **realm → INTERNAL2**
    c. Enter **terminate-recursion → enabled**
    d. Enter **app-protocol → SIP**

    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

## 7.10. SIP Manipulations

SIP manipulation specifies rules for manipulating the contents of specified SIP headers. Two separate sets of SIP manipulations were required for the compliance test listed below.

- inManFromSM – A set of SIP header manipulation rules (HMRs) on traffic from Session Manager to the SBC.
- outManToSP - A set of SIP header manipulation rules on traffic from the SBC to service provider (OneStream).

### 7.10.1. Session Manager to SBC

The following set of SIP HMRs is applied to traffic from the Session Manager to the SBC. In some call flows the user part of the SIP Contact header sent from the Session Manager was not passed unaltered to the public side of the SBC. To correct this, the user part of the Contact header is stored when received from the Session Manager and used to create a temporary header called X-Contact that will be deleted on the outbound (public) side of the SBC. The information contained in the X-Contact header will be used to recreate the proper Contact header on the public side of the SBC as shown in **Sections 7.10.2.8** and **7.10.2.9**.

To create this set of SIP HMRs:

1. Enter **session-router → sip-manipulation**
2. Enter **name → inManFromSM**
3. Enter **description → "Inbound SIP HMRs From SM"**
4. Proceed to the following sections. Once all sections are completed then proceed with **Steps 5** and **6** below.
5. Enter **done**
6. Enter **exit**

#### 7.10.1.1 Store Contact

This rule stores the user part of the incoming Contact header.

1. Enter **header-rule**
2. Enter **name → strcon**
3. Enter **header-name → Contact**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **methods → INVITE,UPDATE**
8. Enter **element-rule**
    a. Enter **name → strval**
    b. Enter **type → uri-user**

c. Enter **action → store**
d. Enter **match-val-type → any**
e. Enter **comparison-type → case-sensitive**
f. Enter **match-value → (.*)**
g. Enter **done**
h. Enter **exit**

9. Enter **done**
10. Enter **exit**

#### 7.10.1.2 Create X-Contact

This rule creates a temporary header called X-Contact containing only the user part of the incoming Contact header as stored by the rule defined in the previous section.

1. Enter **header-rule**
2. Enter **name → addXcontact**
3. Enter **header-name → X-Contact**
4. Enter **action → add**
5. Enter **comparison-type → pattern-rule**
6. Enter **msg-type → request**
7. Enter **methods → INVITE,UPDATE**
8. Enter **element-rule**
    a. Enter **name → add-X**
    b. Enter **type → header-value**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → pattern-rule**
    f. Enter **new-value → $strcon.$strval.$0**
    g. Enter **done**
    h. Enter **exit**
9. Enter **done**
10. Enter **exit**

### 7.10.2. SBC to OneStream

The following set of SIP HMRs is applied to traffic from the SBC to OneStream.

To create this set of SIP HMRs:

1. Enter **session-router → sip-manipulation**
2. Enter **name → outManFromSP**
3. Enter **description → "outbound SIP HMRs From SP"**
4. Proceed to the following sections. Once all sections are completed then proceed with **Steps 5** and **6** below.
5. Enter **done**
6. Enter **exit**

### 7.10.2.1 Change Host of the To Header

This rule replaces the host part of the To header with the service provider's IP address. A similar manipulation is performed on the Request-URI by the Session Manager. The Request-URI could have also been manipulated by the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipTo**
3. Enter **header-name** → **To**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
    a. Enter **name** → **chgToHost**
    b. Enter **type** → **uri-host**
    c. Enter **action** → **replace**
    d. Enter **match-val-type** → **any**
    e. Enter **comparison-type** → **case-sensitive**
    f. Enter **new-value** → **$REMOTE_IP**
8. Enter **done**
9. Enter **exit**

### 7.10.2.2 Change Host of the From Header

This rule replaces the host part of the From header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipFrom**
3. Enter **header-name** → **From**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**
6. Enter **msg-type** → **request**
7. Enter **element-rule** →
    a. Enter **name** → **From**
    b. Enter **type** → **uri-host**
    c. Enter **action** → **replace**
    d. Enter **match-val-type** → **any**
    e. Enter **comparison-type** → **case-sensitive**
    f. Enter **new-value** → **$LOCAL_IP**
8. Enter **done**
9. Enter **exit**

### 7.10.2.3 Change Host of the History Info Header

This rule replaces the host part of the History-Info header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name** → **manipHistInfo**
3. Enter **header-name** → **History-Info**
4. Enter **action** → **manipulate**
5. Enter **comparison-type** → **case-sensitive**

6. Enter **msg-type → request**
7. Enter **element-rule →**
    a. Enter **name → HistoryInfo**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $LOCAL_IP**
8. Enter **done**
9. Enter **exit**

#### 7.10.2.4 Change Host of the PAI Header

This rule replaces the host part of the P-Asserted-Identity header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name → manipPAI**
3. Enter **header-name → P-Asserted-Identity**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule →**
    a. Enter **name → Pai**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $LOCAL_IP**
8. Enter **done**
9. Enter **exit**

#### 7.10.2.5 Change Host of the Diversion Header

This rule replaces the host part of the Diversion header with the public IP address of the SBC.

1. Enter **header-rule**
2. Enter **name → manipDiversion**
3. Enter **header-name → Diversion**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule →**
    a. Enter **name → Diversion**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $LOCAL_IP**

8. Enter **done**
9. Enter **exit**

#### 7.10.2.6 Change Host of the Refer-To Header

This rule stores the user part of the Refer-To header with the service provider's IP address.

1. Enter **header-rule**
2. Enter **name → manipRefer**
3. Enter **header-name → Refer-To**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule →**
    a. Enter **name → chgHostRefer**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $REMOTE_IP**
8. Enter **done**
9. Enter **exit**

#### 7.10.2.7 Store X-Contact Header

This rule stores the contents of the X-Contact header so it can be used later. The X-Contact header contains the only the user part of the Contact header as it was originally received from the Session Manager as described in **Section 7.10.1**.

1. Enter **header-rule**
2. Enter **name → storexcontact**
3. Enter **header-name → X-Contact**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **methods → INVITE,UPDATE**
8. Enter **element-rule →**
    a. Enter **name → storexcontact**
    b. Enter **type → header-value**
    c. Enter **action → store**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **match-value → (.*)**
9. Enter **done**
10. Enter **exit**

#### 7.10.2.8 Replace Contact Header

This rule uses the data stored from the X-Contact header to overwrite the user part of the outbound Contact header.

1. Enter **header-rule**
2. Enter **name → replacecontact**
3. Enter **header-name → Contact**
4. Enter **action → manipulate**
5. Enter **comparison-type → pattern-rule**
6. Enter **msg-type → request**
7. Enter **methods → INVITE,UPDATE**
8. Enter **element-rule**
    a. Enter **name → replacecontact**
    b. Enter **type → uri-user**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → pattern-rule**
    f. Enter **match-value → (.*)**
    g. Enter **new-value $storexcontact.$storexcontact.$0**
9. Enter **done**
10. Enter **exit**

#### 7.10.2.9 Delete X-Contact Header

This rule deletes the temporary X-Contact header before sending the message to the service provider.

1. Enter **header-rule**
2. Enter **name → delxcontact**
3. Enter **header-name → X-Contact**
4. Enter **action → delete**
5. Enter **comparison-type → pattern-rule**
6. Enter **msg-type → request**
7. Enter **methods → INVITE,UPDATE**
8. Enter **done**
9. Enter **exit**

Continue with the next step in **Section 7.10.2**.

# 8. OneStream Global SIP Trunking Configuration

To use OneStream Global SIP Trunking, a customer must request the service from OneStream using their sales processes. The process can be started by contacting OneStream Networks via email to sales@onestreamnetworks.com or by calling 800-869-0315 option 2. Customers may also contact OneStream Networks via the corporate web site at www.onestreamnetworks.com.

During the signup process, OneStream will require that the customer provide the public IP address used to reach the SBC at the edge of the enterprise. OneStream will provide the IP address of the OneStream SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager, and the SBC configuration discussed in the previous sections.

The configuration between OneStream and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the OneStream network.

# 9. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Troubleshooting:

1. Communication Manager:
    - **list trace station** <extension number> - Traces calls to and from a specific station.
    - **list trace tac** <trunk access code number> - Traces calls over a specific trunk group.
    - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
    - **status trunk** <trunk access code number> - Displays trunk group information.
    - **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.
2. Session Manager:
    - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.

# 10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Acme Packet 3800 Net-Net Session Border Controller to OneStream Global SIP Trunking. OneStream Global SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. OneStream Global SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. OneStream Global SIP Trunking passed compliance testing. Please refer to **Section 2.2** for any exceptions or workarounds.

# 11. References

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


[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6, June 2010.
[2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
[3] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* May 2009, Document Number 555-245-205.
[5] *Installing and Upgrading Avaya Aura® System Manager 5.2 GA Version*, January 2010.
[6] *Installing Avaya Aura® Session Manager*, January 2010.
[7] *Administering Avaya Aura® Session Manager,* March 2010, Document Number 03-603324.
[8] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x,* February 2010, Document Number 16-601443.
[9] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.
[10] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.
[11] *Avaya one-X® Communicator Getting Started, November 2009.*
[12] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/
[13] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/
[14] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

# 12. Appendix A: Acme Packet 3800 Net-Net SBC Configuration File

```
host-routes
      dest-network                  10.32.0.0
      netmask                       255.255.0.0
      gateway                       10.32.128.254
      description                   DevConnectLAN
      last-modified-by              admin@135.11.141.118
      last-modified-date            2010-08-05 15:25:58
local-policy
      from-address
                                    *
      to-address
                                    *
      source-realm
                                    INTERNAL2
      description
      activate-time                 N/A
      deactivate-time               N/A
      state                         enabled
      policy-priority               none
      last-modified-by              admin@135.11.207.156
      last-modified-date            2010-12-16 17:22:04
      policy-attribute
            next-hop                      10.2.2.227
            realm                         EXTERNAL
            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
            lookup                        single
            next-key
            eloc-str-lkup                 disabled
            eloc-str-match
local-policy
      from-address
                                    *
      to-address
                                    7325551234
                                    7325551235
                                    7325551236
      source-realm
                                    EXTERNAL
      description
      activate-time                 N/A
      deactivate-time               N/A
```

```
      state                           enabled
      policy-priority                 none
      last-modified-by                admin@135.11.207.156
      last-modified-date              2010-12-16 17:21:38
      policy-attribute
            next-hop                        10.32.24.235
            realm                           INTERNAL2
            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
            lookup                          single
            next-key
            eloc-str-lkup                   disabled
            eloc-str-match
media-manager
      state                           enabled
      latching                        enabled
      flow-time-limit                 86400
      initial-guard-timer             300
      subsq-guard-timer               300
      tcp-flow-time-limit             86400
      tcp-initial-guard-timer         300
      tcp-subsq-guard-timer           300
      tcp-number-of-ports-per-flow    2
      hnt-rtcp                        disabled
      algd-log-level                  NOTICE
      mbcd-log-level                  NOTICE
      red-flow-port                   1985
      red-mgcp-port                   1986
      red-max-trans                   10000
      red-sync-start-time             5000
      red-sync-comp-time              1000
      media-policing                  enabled
      max-signaling-bandwidth         10000000
      max-untrusted-signaling         100
      min-untrusted-signaling         30
      app-signaling-bandwidth         0
      tolerance-window                30
      rtcp-rate-limit                 0
      trap-on-demote-to-deny          enabled
      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
      media-supervision-traps        disabled
      dnsalg-server-failover         disabled
      last-modified-by               admin@135.11.141.142
      last-modified-date             2010-06-16 05:40:01
network-interface
      name                           s0p0
      sub-port-id                    0
      description
      hostname
      ip-address                     10.3.9.188
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.128
      gateway                        10.3.9.129
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary                 10.3.16.67
      dns-ip-backup1                 10.3.16.68
      dns-ip-backup2
      dns-domain
      dns-timeout                    11
        hip-ip-list                    10.3.9.188
      ftp-address
        icmp-address                   10.3.9.188
      snmp-address
      telnet-address
      ssh-address
      last-modified-by               admin@135.11.207.156
      last-modified-date             2010-11-01 15:17:15
network-interface
      name                           s1p0
      sub-port-id                    0
      description
      hostname
      ip-address                     10.32.128.13
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        10.32.128.254
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
            retry-timeout                  1
            health-score                   0
      dns-ip-primary
      dns-ip-backup1
      dns-ip-backup2
```

```
      dns-domain
      dns-timeout                     11
        hip-ip-list                     10.32.128.13
      ftp-address
        icmp-address                    10.32.128.13
      snmp-address
      telnet-address
      ssh-address
      last-modified-by                admin@135.11.141.118
      last-modified-date              2010-08-17 16:10:28
phy-interface
      name                            s0p0
      operation-type                  Media
      port                            0
      slot                            0
      virtual-mac
      admin-state                     enabled
      auto-negotiation                enabled
      duplex-mode
      speed
      overload-protection             disabled
      last-modified-by                admin@135.11.141.118
      last-modified-date              2010-08-17 14:39:18
phy-interface
      name                            s1p0
      operation-type                  Media
      port                            0
      slot                            1
      virtual-mac                     00:08:25:a0:f4:8a
      admin-state                     enabled
      auto-negotiation                enabled
      duplex-mode                     FULL
      speed                           100
      overload-protection             disabled
      last-modified-by                admin@135.11.141.118
      last-modified-date              2010-08-17 16:02:46
realm-config
      identifier                      EXTERNAL
      description
      addr-prefix                     0.0.0.0
      network-interfaces
                                      s0p0:0
      mm-in-realm                     disabled
      mm-in-network                   enabled
      mm-same-ip                      enabled
      mm-in-system                    enabled
      bw-cac-non-mm                   disabled
      msm-release                     disabled
      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
media-sec-policy
in-translationid
out-translationid
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
class-profile
average-rate-limit              0
access-control-trust-level      none
invalid-signal-threshold        0
maximum-signal-threshold        0
untrusted-signal-threshold      0
nat-trust-threshold             0
deny-period                     30
ext-policy-svr
symmetric-latching              disabled
pai-strip                       disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching             none
restriction-mask                32
accounting-enable               enabled
user-cac-mode                   none
user-cac-bandwidth              0
user-cac-sessions               0
icmp-detect-multiplier          0
icmp-advertisement-interval     0
icmp-target-ip
monthly-minutes                 0
net-management-control          disabled
delay-media-update              disabled
refer-call-transfer             disabled
dyn-refer-term                  disabled
codec-policy
codec-manip-in-realm            disabled
constraint-name
call-recording-server-id
xnq-state                       xnq-unknown
hairpin-id                      0
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
sip-profile
sip-isup-profile
block-rtcp                      disabled
hide-egress-media-update        disabled
```

```
      last-modified-by               admin@135.11.207.156
      last-modified-date             2010-11-03 08:55:21
realm-config
      identifier                     INTERNAL2
      description
      addr-prefix                    0.0.0.0
      network-interfaces
                                     s1p0:0
      mm-in-realm                    disabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
      msm-release                    disabled
      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
      media-sec-policy
      in-translationid
      out-translationid
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      class-profile
      average-rate-limit             0
      access-control-trust-level     none
      invalid-signal-threshold       0
      maximum-signal-threshold       0
      untrusted-signal-threshold     0
      nat-trust-threshold            0
      deny-period                    30
      ext-policy-svr
      symmetric-latching             disabled
      pai-strip                      disabled
      trunk-context
      early-media-allow
      enforcement-profile
      additional-prefixes
      restricted-latching            none
      restriction-mask               32
      accounting-enable              enabled
      user-cac-mode                  none
      user-cac-bandwidth             0
      user-cac-sessions              0
      icmp-detect-multiplier         0
      icmp-advertisement-interval    0
      icmp-target-ip
```

```
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        dyn-refer-term                 disabled
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        xnq-state                      xnq-unknown
        hairpin-id                     0
        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
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
        last-modified-by               admin@135.11.207.156
        last-modified-date             2010-12-16 17:25:01
session-agent
        hostname                       10.32.24.235
        ip-address                     10.32.24.235
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               StaticTCP
        realm-id                       INTERNAL2
        egress-realm-id
        description                    SM_SPenv
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
```

```
      redirect-action
      loose-routing                   enabled
      send-media-session              enabled
      response-map
      ping-method
      ping-interval                   0
      ping-send-mode                  keep-alive
      ping-all-addresses              disabled
      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               inManFromSM
      out-manipulationid
      manipulation-string
      manipulation-pattern
      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
      sip-profile
      sip-isup-profile
      last-modified-by                admin@135.11.207.156
      last-modified-date              2010-11-01 12:06:13
session-agent
      hostname                        10.2.2.227
      ip-address                      10.2.2.227
      port                            5060
      state                           enabled
      app-protocol                    SIP
      app-type
      transport-method                UDP
      realm-id                        EXTERNAL
      egress-realm-id
      description                     OneStream
      carriers
      allow-next-hop-lp               enabled
```

```
constraints                    disabled
max-sessions                   0
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method
ping-interval                  0
ping-send-mode                 keep-alive
ping-all-addresses             disabled
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             outManToSP
manipulation-string
manipulation-pattern
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
      sip-profile
      sip-isup-profile
      last-modified-by               admin@135.11.207.156
      last-modified-date             2010-12-21 12:39:47
sip-config
      state                          enabled
      operation-mode                 dialog
      dialog-transparency            enabled
      home-realm-id                  INTERNAL2
      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             enabled
      registration-cache-limit       0
      register-use-to-for-lp         disabled
      options                        max-udp-length=0
      refer-src-routing              disabled
      add-ucid-header                disabled
      proxy-sub-events
      pass-gruu-contact              disabled
      sag-lookup-on-redirect         disabled
      last-modified-by               admin@135.11.207.156
      last-modified-date             2010-11-02 16:18:33
sip-interface
      state                          enabled
      realm-id                       EXTERNAL
      description
      sip-port
            address                        10.3.9.188
            port                           5060
```

```
            transport-protocol              UDP
            tls-profile
            allow-anonymous                 agents-only
            ims-aka-profile
      carriers
      trans-expire                    0
      invite-expire                   0
      max-redirect-contacts           0
      proxy-mode
      redirect-action
      contact-mode                    none
      nat-traversal                   none
      nat-interval                    30
      tcp-nat-interval                90
      registration-caching            disabled
      min-reg-expire                  300
      registration-interval           3600
      route-to-registrar              disabled
      secured-network                 disabled
      teluri-scheme                   disabled
      uri-fqdn-domain
      trust-mode                      all
      max-nat-interval                3600
      nat-int-increment               10
      nat-test-increment              30
      sip-dynamic-hnt                 disabled
      stop-recurse                    401,407
      port-map-start                  0
      port-map-end                    0
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      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
```

```
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      sip-profile
      sip-isup-profile
      last-modified-by               admin@135.11.207.156
      last-modified-date             2010-12-21 11:57:15
sip-interface
      state                          enabled
      realm-id                       INTERNAL2
      description
      sip-port
            address                        10.32.128.13
            port                           5060
            transport-protocol             TCP
            tls-profile
            allow-anonymous                all
            ims-aka-profile
      carriers
      trans-expire                   0
      invite-expire                  0
      max-redirect-contacts          0
      proxy-mode
      redirect-action
      contact-mode                   none
      nat-traversal                  none
      nat-interval                   30
      tcp-nat-interval               90
      registration-caching           disabled
      min-reg-expire                 300
      registration-interval          3600
      route-to-registrar             disabled
      secured-network                disabled
      teluri-scheme                  disabled
      uri-fqdn-domain
      trust-mode                     all
      max-nat-interval               3600
      nat-int-increment              10
      nat-test-increment             30
      sip-dynamic-hnt                disabled
      stop-recurse                   401,407
      port-map-start                 0
      port-map-end                   0
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      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
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      sip-profile
      sip-isup-profile
      last-modified-by               admin@135.11.141.118
      last-modified-date             2010-12-22 10:31:26
sip-manipulation
      name                           outManToSP
      description                    Outbound SIP HMRs To SP
      split-headers
      join-headers
      header-rule
            name                           manipTo
            header-name                    To
            action                         manipulate
            comparison-type                case-sensitive
            msg-type                       request
            methods
            match-value
            new-value
            element-rule
                  name                           chgToHost
                  parameter-name
                  type                           uri-host
                  action                         replace
                  match-val-type                 any
                  comparison-type                case-sensitive
                  match-value
                  new-value                      $REMOTE_IP
      header-rule
            name                           manipFrom
            header-name                    From
            action                         manipulate
            comparison-type                case-sensitive
            msg-type                       request
            methods
            match-value
            new-value
            element-rule
```

```
            name                                From
            parameter-name
            type                                uri-host
            action                              replace
            match-val-type                      any
            comparison-type                     case-sensitive
            match-value
            new-value                           $LOCAL_IP
header-rule
      name                                manipDiversion
      header-name                         Diversion
      action                              manipulate
      comparison-type                     case-sensitive
      msg-type                            request
      methods
      match-value
      new-value
      element-rule
            name                                Diversion
            parameter-name
            type                                uri-host
            action                              replace
            match-val-type                      any
            comparison-type                     case-sensitive
            match-value
            new-value                           $LOCAL_IP
header-rule
      name                                manipHistInfo
      header-name                         History-Info
      action                              manipulate
      comparison-type                     case-sensitive
      msg-type                            request
      methods
      match-value
      new-value
      element-rule
            name                                HistoryInfo
            parameter-name
            type                                uri-host
            action                              replace
            match-val-type                      any
            comparison-type                     case-sensitive
            match-value
            new-value                           $LOCAL_IP
header-rule
      name                                manipPAI
      header-name                         P-Asserted-Identity
      action                              manipulate
      comparison-type                     case-sensitive
      msg-type                            request
      methods
      match-value
      new-value
      element-rule
            name                                Pai
            parameter-name
```

```
            type                            uri-host
            action                          replace
            match-val-type                  any
            comparison-type                 case-sensitive
            match-value
            new-value                       $LOCAL_IP
header-rule
      name                            storeXcontact
      header-name                     X-Contact
      action                          manipulate
      comparison-type                 case-sensitive
      msg-type                        request
      methods                         INVITE,UPDATE
      match-value
      new-value
      element-rule
            name                            storeXcontact
            parameter-name
            type                            header-value
            action                          store
            match-val-type                  any
            comparison-type                 case-sensitive
            match-value                     (.*)
            new-value
header-rule
      name                            replacecontact
      header-name                     Contact
      action                          manipulate
      comparison-type                 pattern-rule
      msg-type                        request
      methods                         INVITE,UPDATE
      match-value
      new-value
      element-rule
            name                        replacecontact
            parameter-name
            type                        uri-user
            action                      replace
            match-val-type              any
            comparison-type             pattern-rule
            match-value                 (.*)
            new-value                   $storeXcontact.$storeXcontact.$0
header-rule
      name                            delXcontact
      header-name                     X-Contact
      action                          delete
      comparison-type                 pattern-rule
      msg-type                        request
      methods                         INVITE,UPDATE
      match-value
      new-value
header-rule
      name                            manipRefer
      header-name                     Refer-To
      action                          manipulate
      comparison-type                 case-sensitive
```

```
        msg-type                       request
        methods
        match-value
        new-value
        element-rule
              name                           chgHostRefer
              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@135.11.207.156
  last-modified-date             2010-12-21 10:24:38
sip-manipulation
  name                           inManFromSM
  description                    storecontact
  split-headers
  join-headers
  header-rule
        name                           strcon
        header-name                    Contact
        action                         manipulate
        comparison-type                case-sensitive
        msg-type                       request
        methods                        INVITE,UPDATE
        match-value
        new-value
        element-rule
              name                           strval
              parameter-name
              type                           uri-user
              action                         store
              match-val-type                 any
              comparison-type                case-sensitive
              match-value                    (.*)
              new-value
  header-rule
        name                           addXcontact
        header-name                    X-Contact
        action                         add
        comparison-type                pattern-rule
        msg-type                       request
        methods                        INVITE,UPDATE
        match-value
        new-value
        element-rule
              name                           addX
              parameter-name
              type                           header-value
              action                         replace
              match-val-type                 any
              comparison-type                pattern-rule
              match-value
              new-value                      $strcon.$strval.$0
```

```
      last-modified-by              admin@135.11.207.156
      last-modified-date            2010-12-21 12:21:51
steering-pool
      ip-address                    10.3.9.188
      start-port                    49152
      end-port                      65535
      realm-id                      EXTERNAL
      network-interface
      last-modified-by              admin@135.11.141.142
      last-modified-date            2010-06-16 15:58:07
steering-pool
      ip-address                    10.32.128.13
      start-port                    2048
      end-port                      65535
      realm-id                      INTERNAL2
      network-interface
      last-modified-by              admin@135.11.141.118
      last-modified-date            2010-10-06 11:28:26
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                    enabled
      internal-trace                enabled
      log-filter                    all
      default-gateway               0.0.0.0
      restart                       enabled
      exceptions
      telnet-timeout                0
      console-timeout               0
      remote-control                enabled
```

```
cli-audit-trail                 enabled
link-redundancy-state           disabled
source-routing                  disabled
cli-more                        disabled
terminal-height                 24
debug-timeout                   0
trap-event-lifetime             0
default-v6-gateway              ::
ipv6-support                    disabled
cleanup-time-of-day             00:00
last-modified-by                admin@135.11.141.142
last-modified-date              2010-07-09 23:23:00
```

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.