Avaya Solution & Interoperability Test Lab

Application Notes for Configuring OneStream Networks Global SIP Trunking with Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Acme Net-Net 3820 Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between OneStream Networks Global SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, Acme Net-Net 3820 Session Border Controller and various Avaya endpoints. OneStream 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 OneStream Networks Global SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, Acme Net-Net 3820Session Border Controller (Acme SBC) and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with OneStream Networks Global SIP Trunking are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. 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. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.
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.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the OneStream Networks 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 Acme SBC. Communication Manager and Session Manager were running on a single server as part of the Avaya Aura® Solution for Midsize Enterprise. However, these compliance test results are applicable to other server and media gateway platforms running similar versions of Communication Manager and Session Manager.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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 including Avaya 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 including 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 can place calls from the local computer or control a remote phone. Both of these modes were tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP.
- Various call types including: local, long distance, international, outbound toll-free, operator and local directory assistance (411).
- Codecs 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
- Voicemail Message Waiting Indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and enterprise mobility (extension to cellular)

Items not supported or not tested included the following:

- OneStream Networks Global SIP Trunking was not configured to send SIP OPTIONS messages during the compliance test but will respond to the OPTIONS messages sent by the Acme SBC.
- Inbound toll-free, operator services (0 + 10 digits) and emergency calls (911) are supported but were not tested as part of the compliance test.
- A "302 Moved Temporarily" response with new Contact header is not supported for network redirection.
- Avaya one-X® Communicator Road Warrior with SIP is supported but was not tested as part of the compliance test.

2.2. Test Results

Interoperability testing of OneStream Networks Global SIP Trunking was completed successfully.

2.3. Support

For technical support on the OneStream Networks Global SIP Trunking Service, contact OneStream Networks Business Customer Care via Email at engineering@onestreamnetworks.com or by calling 877-877-1220 option 2.

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 Complete SIP Trunking. This is the configuration used for compliance testing.

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

- Communication Manager
- System Manager
- Session Manager
- Net-Net 3800 Acme SBC
- Avaya G450 Media Gateway
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya one-X® Communicator (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Acme SBC. The Acme SBC 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 Acme SBC. In this way, the Acme SBC can protect the enterprise against any SIP-based attacks. The Acme 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.

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 settings 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.

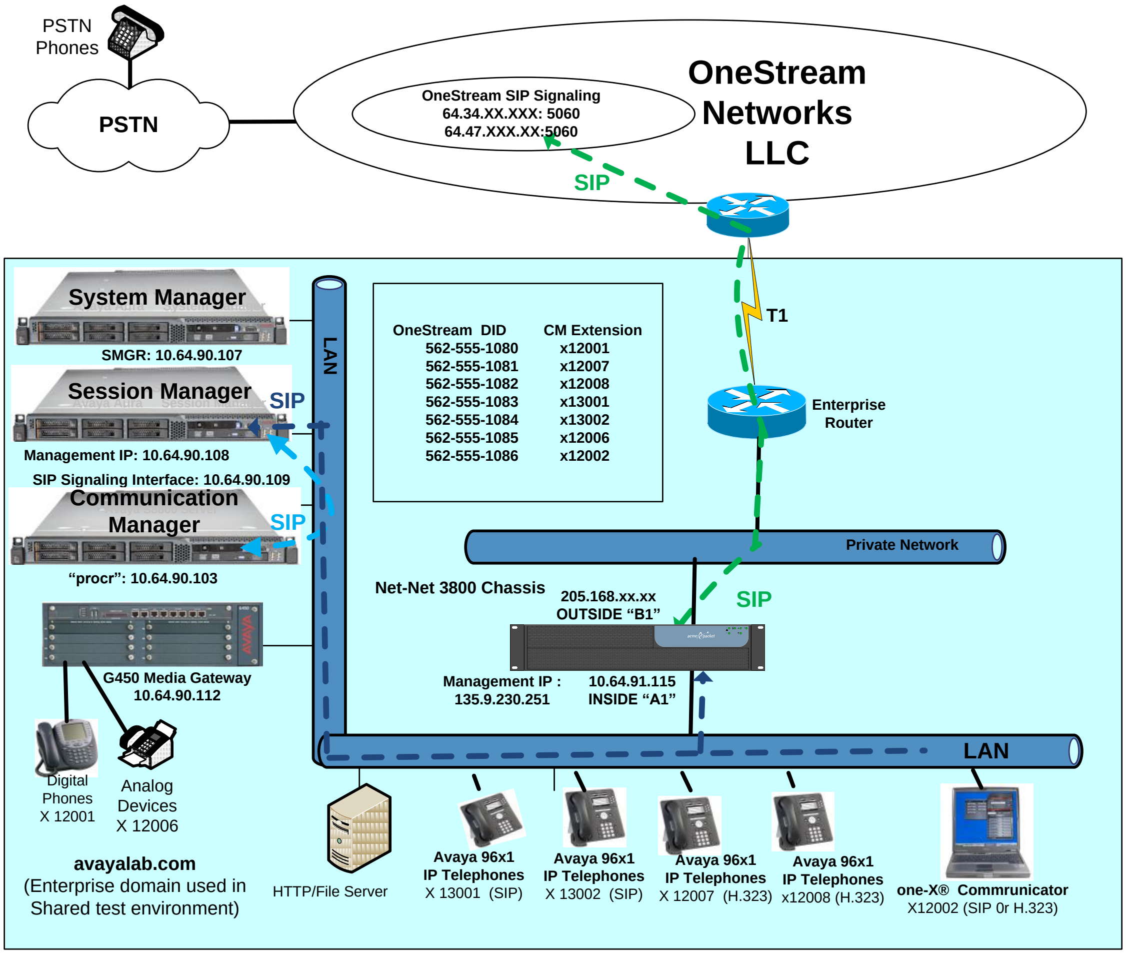


Figure 1: Avaya IP Telephony Network using OneStream Complete SIP Trunking

For inbound calls, the calls flow from the service provider to the Acme 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 Acme SBC. From the Acme SBC, the call is sent to OneStream Complete 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)) of the SIP messaging. 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	
Equipment/Software	Release/Version
- Avaya Aura® System Manager - Avaya Aura® Session Manager - Avaya Aura® Communication Manager	6.2.0 SP3 (Build 6.2.0.0.15669-6.2.12.307) (Software Update Revision 6.2.14.1.1959) 6.2.3.0.623006 (Build 6.2.0.0.15669-6.2.12.307) (Software Update Revision 6.2.14.1.1959) 6.02.2.823.0
Avaya G450 Media Gateway	3.1.20.1
Avaya 9630G IP Telephone (H.323) running Avaya one-X® Deskphone Edition	R6_2_2_09-071012
Avaya 9641G IP Telephone (H.323) running Avaya one-X® Deskphone Edition	R6_2_2_09-071012
Avaya 9620 IP Telephone (SIP) running Avaya one-X® Deskphone SIP Edition	R6_2_0_082012
Avaya 96XX IP Telephone (SIP) running Avaya one-X® Deskphone SIP Edition	R6_2_0_082012
Avaya one-X® Communicator (H.323 or SIP)	6.1.3.08 (SP3-Patch2-35791)
Avaya 2420 Digital Telephone	n/a
Avaya 6211 Analog Telephone	n/a
Acme Net-Net 3820Session Border Controller	SCX6.2.0 MR-6 Patch 4 (Build 908)
OneStream SIP Trunking Solution Components	
Component	Release
Genband S3 Session Border Controller (SBC)	Release 8.0.3.

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 Complete 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 **12000** SIP trunks are available and **265** 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: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 12000 265
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
```

5.2. System Features

Use the **change system-parameters features** 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**.

```
display system-parameters features                            Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    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.

```
display 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: 1
          International Access Code: 011

SCCAN 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 server running Communication Manager **(procr**) and for Session Manager (**SM**). 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
ACME                10.64.91.115
GW                  10.64.90.112
SM                  10.64.90.109
default             0.0.0.0
procr               10.64.90.103
```

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. The list should include the codecs and preferred order defined by OneStream. For the compliance test, codecs G.729B and G.711MU were tested using ip-codec-set 2. To configure the codecs, enter the codecs in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

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

On **Page 2**, set the **Fax Mode** to **t.38-standard**.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

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 **avayalab.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: avayalab.com
    Name: SIP Trunks
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                     IP Audio Hairpinning? n
   UDP Port Max: 40001
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 1 and region 2. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 2. 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 2** command and navigating to **Page 4** (not shown).

```
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    1     y    NoLimit                                             n       t
 4
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and 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 1 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tcp**. 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 Communication Manager and Session Manager.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- 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 Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- 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). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS or TCP. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5060**.
- 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 **6.** 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 1                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: Others



   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 2

Far-end Domain: avayalab.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? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

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 1 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 1                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SIP Trunk to SP             COR: 1        TN: 1        TAC: *01
   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: 1
                                                     Number of Members: 10
```

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 equal 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 **900** seconds was used.

```
Add trunk-group 1                                             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): 900

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

On **Page 3**, set the **Numbering Format** field to **public**. 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 1                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                     Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y



                                Modify Tandem Calling Number: no
```

On **Page 4**, set the **Network Call Redirection** field to **n**. Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** field provides additional information to the network if the call has been re-directed. These settings are needed by OneStream 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 1                                               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
                     Shuffling with SDP? n

       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                           Enable Q-SIP? n
```

5.8. Calling Party Information

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

In the sample configuration, six DID numbers were assigned for testing. These six numbers were assigned to the six extensions 12001,06,07,08, and 13001-02. 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 six extensions.

```
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: 14
 5  1                                        5       Maximum Entries: 9999
 5  2                                        5
 5  3                                        5    Note: If an entry applies to
 5  4                                        5    a SIP connection to Avaya
 5  5                                        5    Aura(R) Session Manager,
 5  6                                        5    the resulting number must
 5  7                                        5    be a complete E.164 number.
 5  8                                        5
 5  12001         1         5825551080      10
 5  12006         1         5625551085      10
 5  12007         1         5625551081      10
 5  12008         1         5625551082      10
 5  13001         1         5625551083      10
 5  13002         1         5625551084      10
```

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
   0           1   attd
   1           5   ext
   2           5   ext
   3           5   ext
   4           5   ext
   5           5   ext
   6           5   ext
   7           5   ext
   8           5   ext
   9           1   fac
   *           3   dac
   #           3   dac
```

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: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *33    Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
   Call Forwarding Enhanced Status:        Act:        Deactivation:
```

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 **1** 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: 0

          Dialed           Total     Route    Call   Node  ANI
          String         Min  Max  Pattern    Type   Num   Reqd
    0                    1    1     1         op           n
    0                    11   11    1         op           n
    01                   9    17    1         iop          n
    011                  8    18    1         intl         n
    1                    11   11    1         fnpa         n
    1303                 11   11    1         fnpa         n
    562                  10   10    1         natl         n
    1720                 11   11    1         fnpa         n
    1800                 11   11    1         fnpa         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 route pattern in the following manner. The example below shows the values used for route pattern 1 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 1 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.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: SIP Trunk
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                          DCS/ IXC
    No          Mrk Lmt List Del  Digits                            QSIG
                             Dgts                                   Intw
 1: 1    0       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                                          none
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
```

6. Configure Avaya Aura® Session Manager

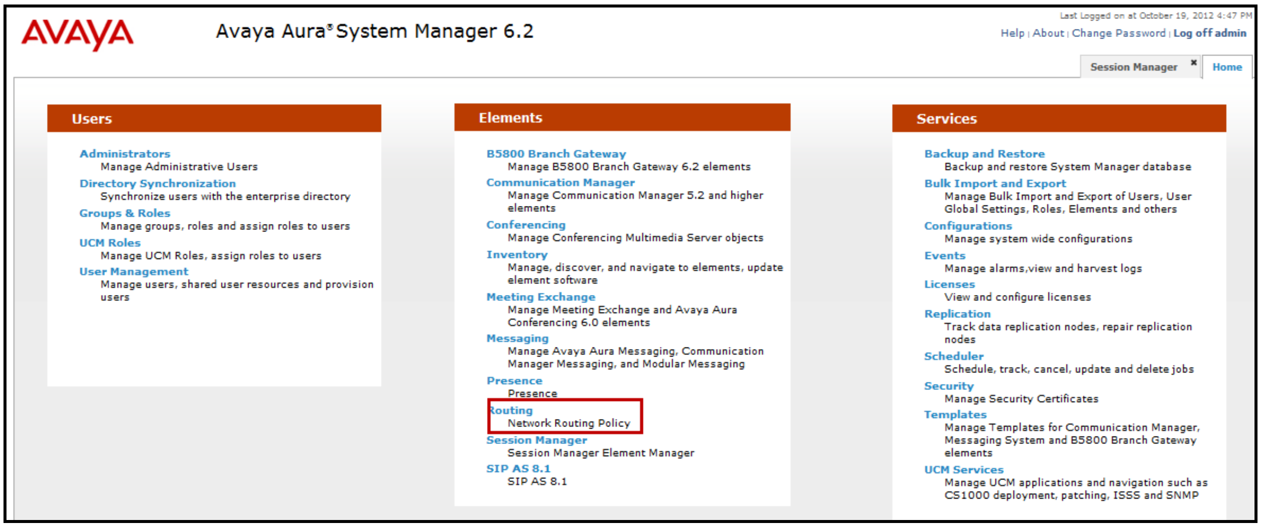
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- 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 Acme 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 governs which Routing Policy is used to service a call
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager

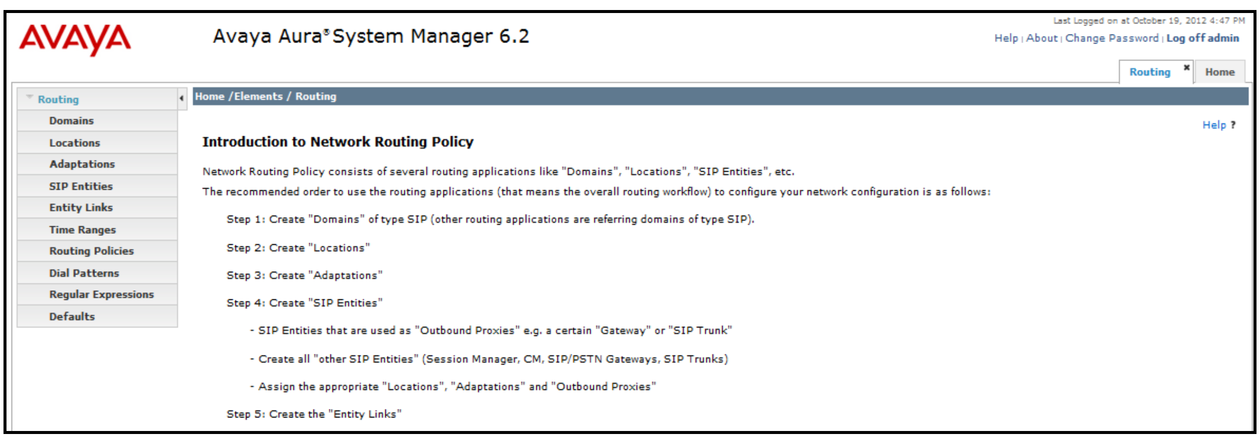
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Avaya Aura® 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 **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements → Routing** link highlighted below.



Clicking the **Elements → Routing** link, displays the **Introduction to Network Routing Policy** page. In the left-hand pane is a navigation tree containing many of the items to be configured in the following sections.

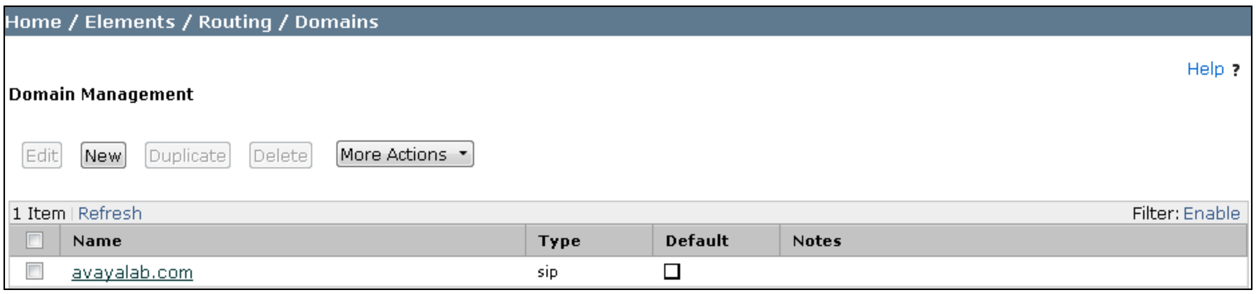


6.2. Specify SIP Domain

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 (**sip.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.



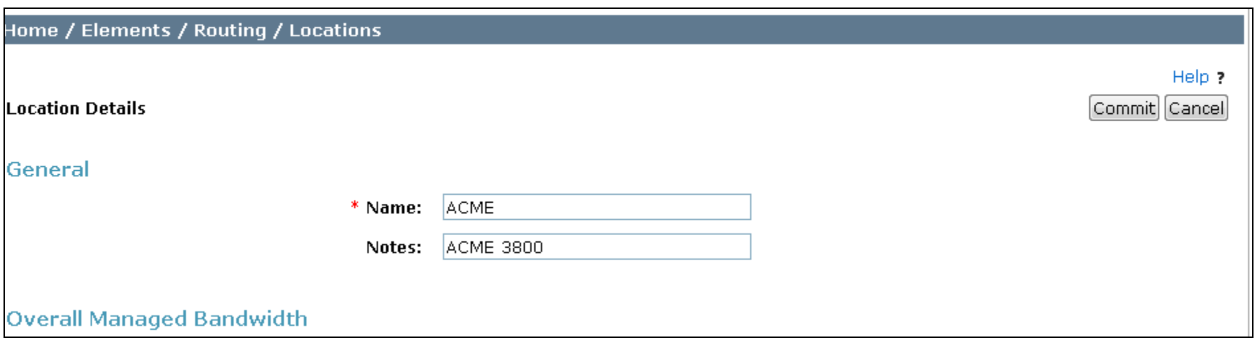
6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the location named **ACME**, which includes all equipment on the enterprise including Communication Manager, Session Manager and the Acme SBC.

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 new right pane that appears (shown below), fill in the following:

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).



6.4. Add Adaptation Module

No adaptation was used for this compliance test. The mappings of internal extensions to OneStream DID numbers may be done in Session Manager (via Digit Conversion in adaptations) or in Communication Manager (via public-unknown-numbering, and incoming call handling treatment for the inbound trunk group) as set in **Section 5.8**.

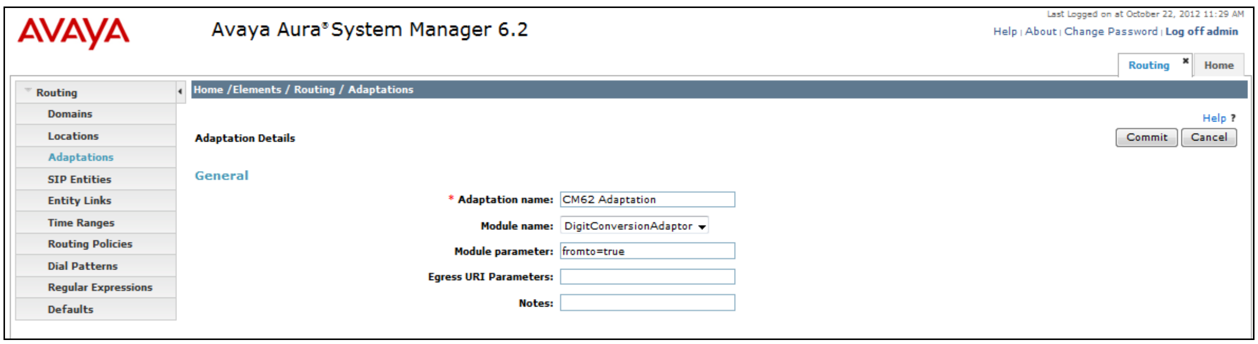
The example below is the sample of the generic adaptation module **DigitConversionAdapter.**

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.

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 new right pane that appears (shown below), fill in the following:

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=sip.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 5.7**.



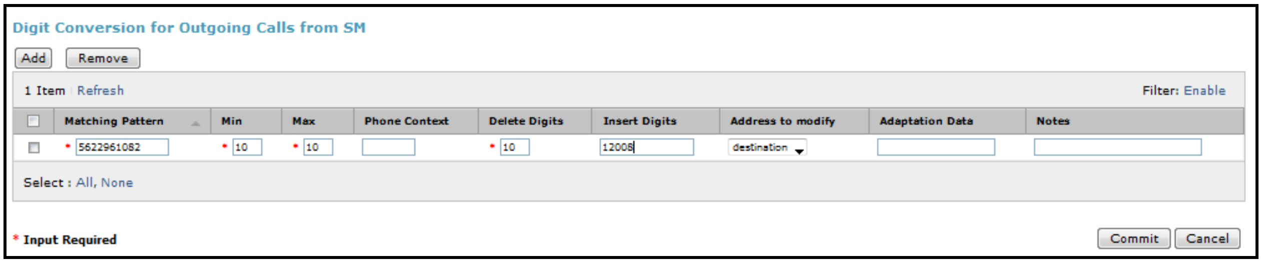
The adaptation sample above can be applied to the Communication Manager SIP entity that supports digit conversion of telephone numbers in specific headers of SIP messages.

To map inbound DID numbers from OneStream to Communication Manager extensions in Session Manager, 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 **destination** since this digit conversion only applies to the destination number.

Click **Commit** to save.



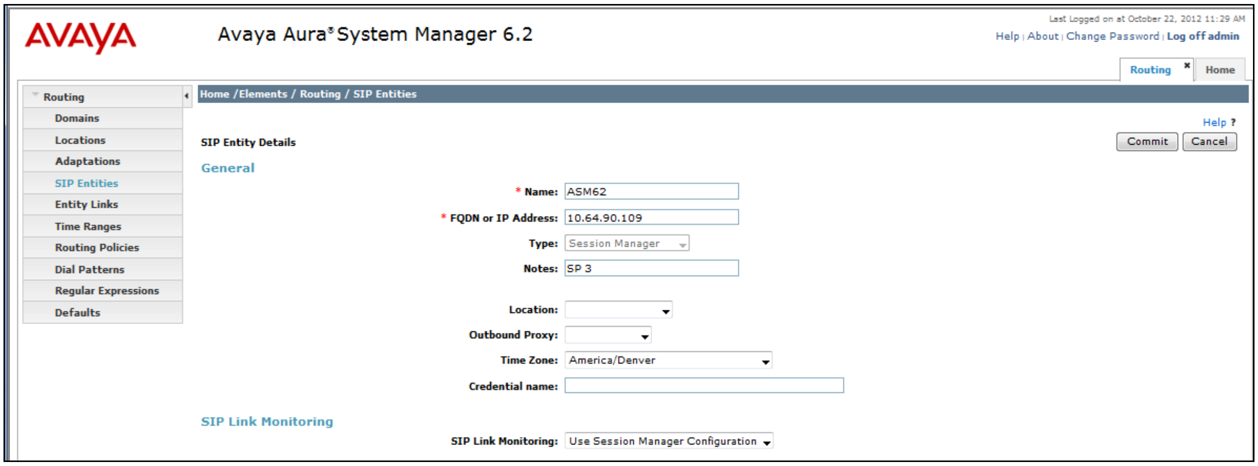
6.5. Add SIP Entities

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 Acme 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 new right pane that appears (shown below), fill in the following:

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 Acme 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 the location that applies to the SIP entity being created. For the compliance test, all components were located in location_1
- **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**.



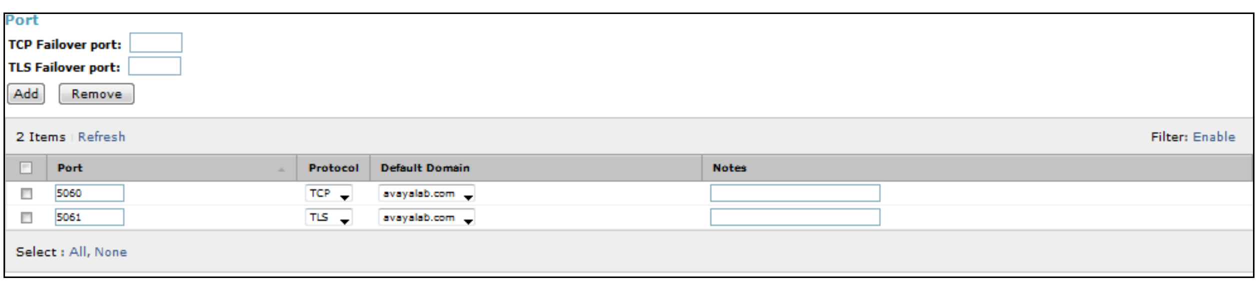
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

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

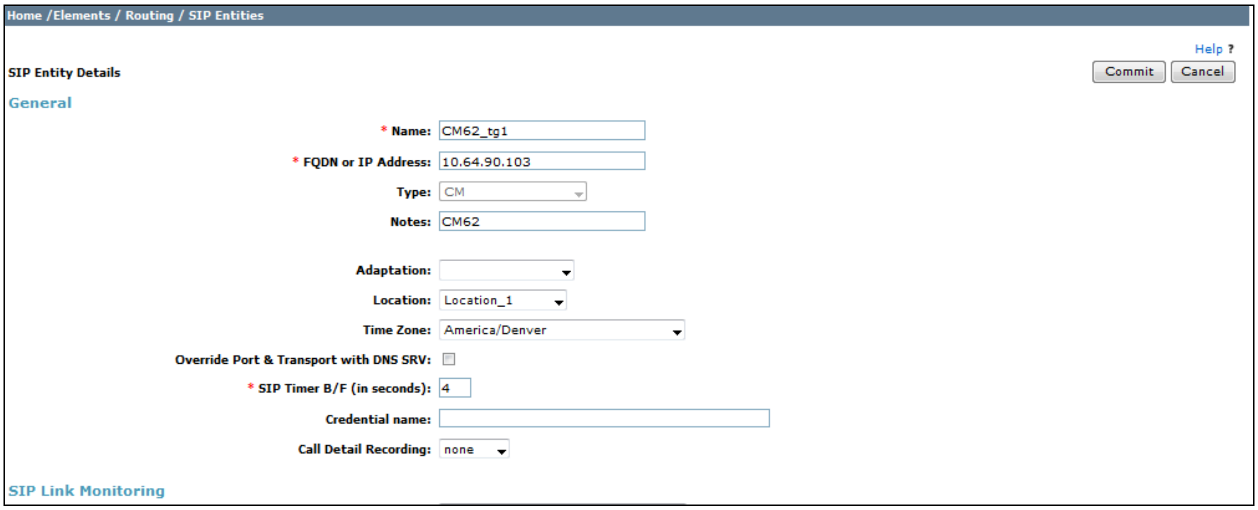
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.
- **Note** Optional note relating to the entry.

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

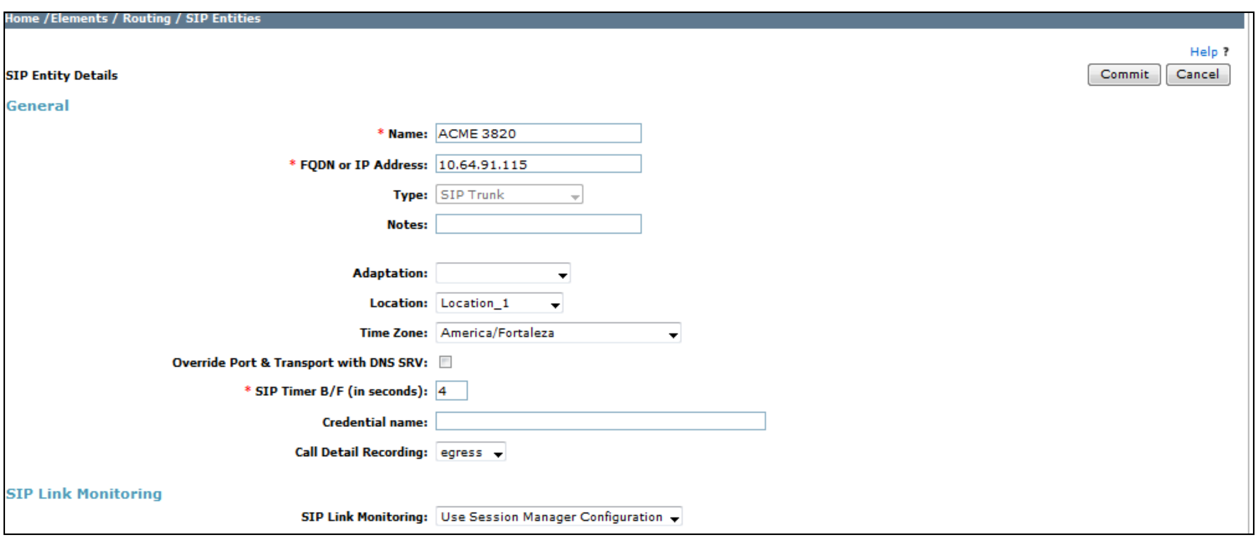
For the compliance test, four port entries were used. The first three are the standard ports used for SIP traffic: port 5060 for UDP/TCP and port 5061 for TLS. In addition, port 5260 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.



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 other 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 Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **Section 6.4**. The **Location** field is set to **Location_1** which is the location defined for the subnet where Communication Manager resides.



The following screen shows the addition of the Acme SBC. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The **Location** field is set to **Location_1** which is the location defined for the subnet where the Acme SBC resides.

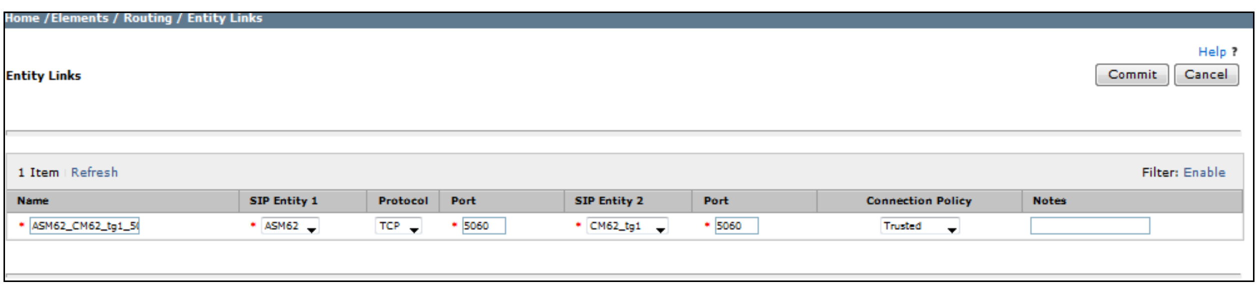


6.6. Add Entity Links

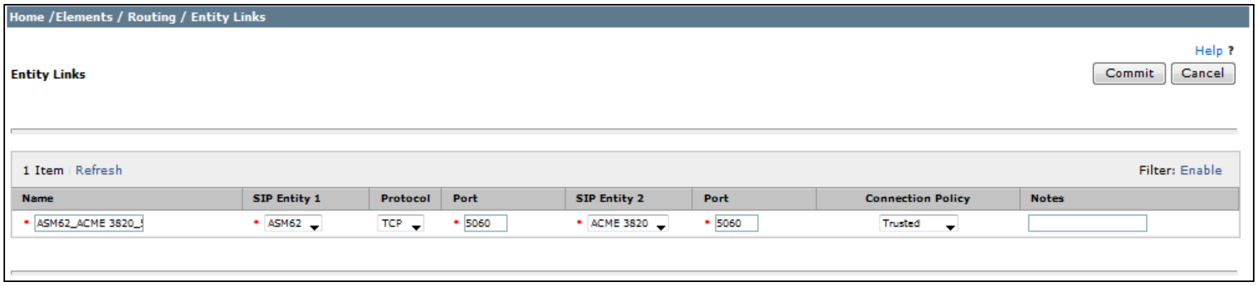
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the Acme SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation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

- **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**.
- **Connection Policy:** Select **Trusted** from pull-down menu.

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



The following screen illustrates the Entity Link to the Acme SBC.



6.7. Add Routing Policies

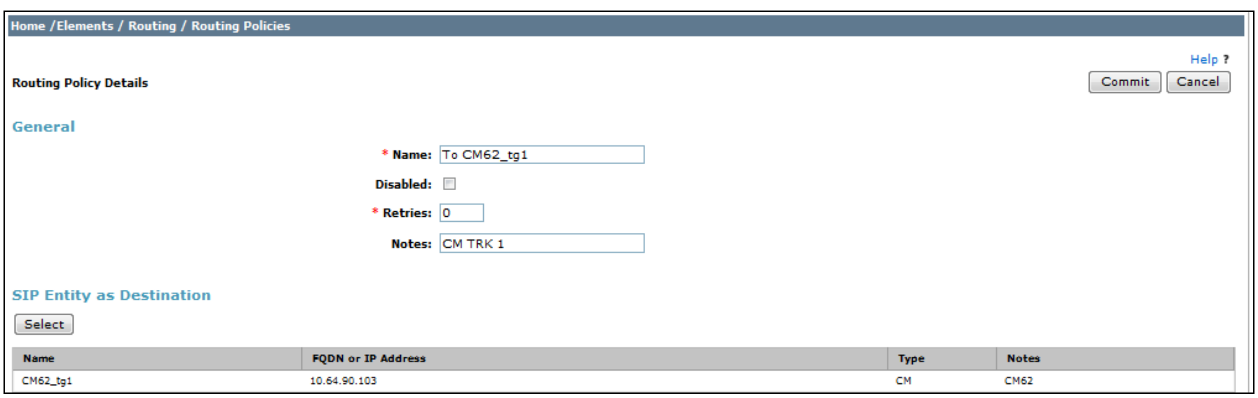
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the Acme SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand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

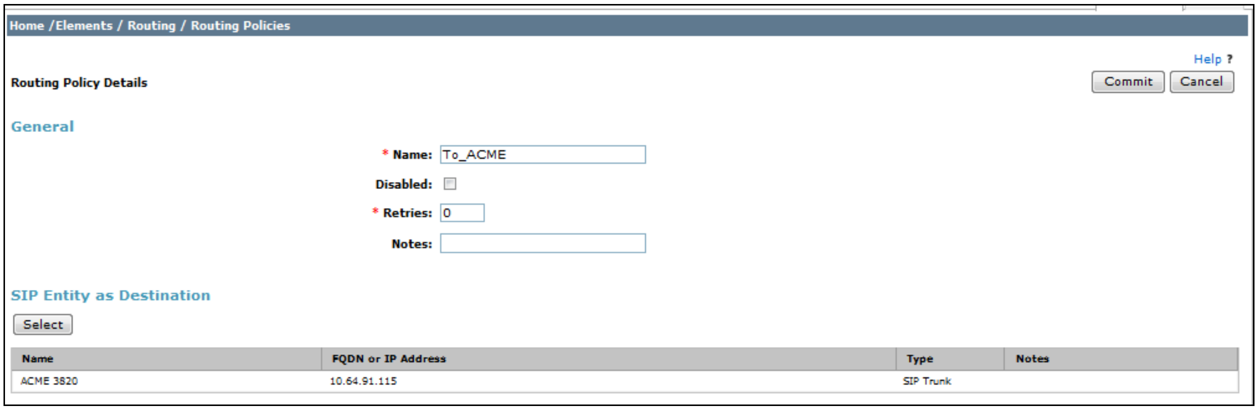
In the **General** section, enter the following values. Use default values for all remaining fields.

- **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 Acme 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). In the new right pane that appears (shown below), fill in the following:

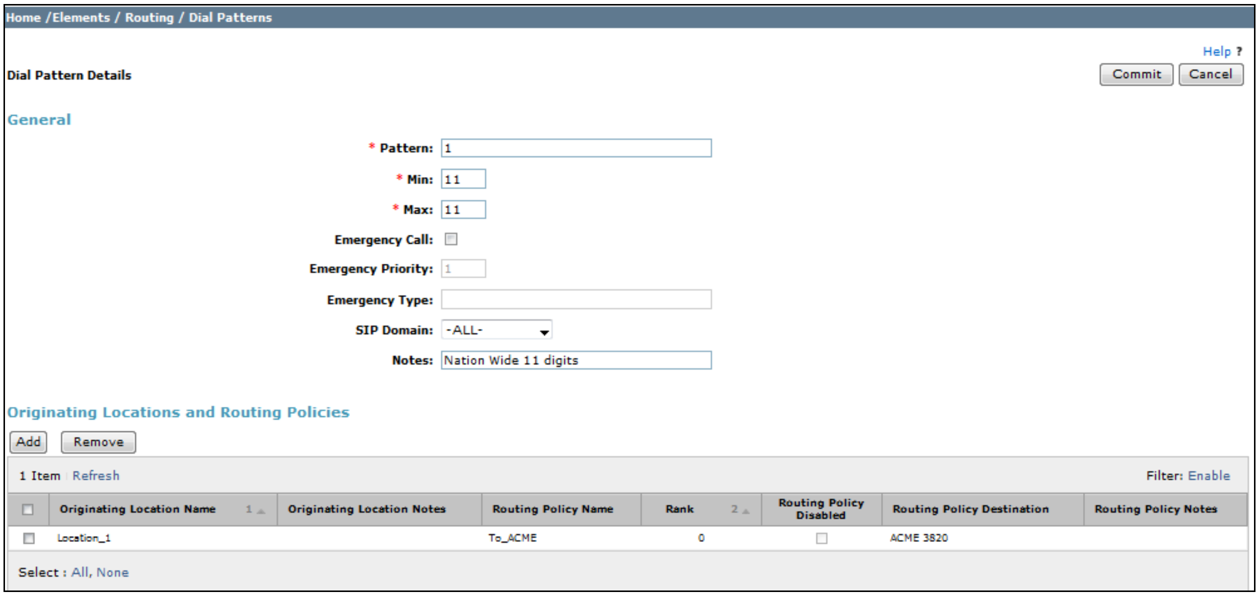
In the **General** section, enter the following values. Use default values for all remaining fields.

- **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).

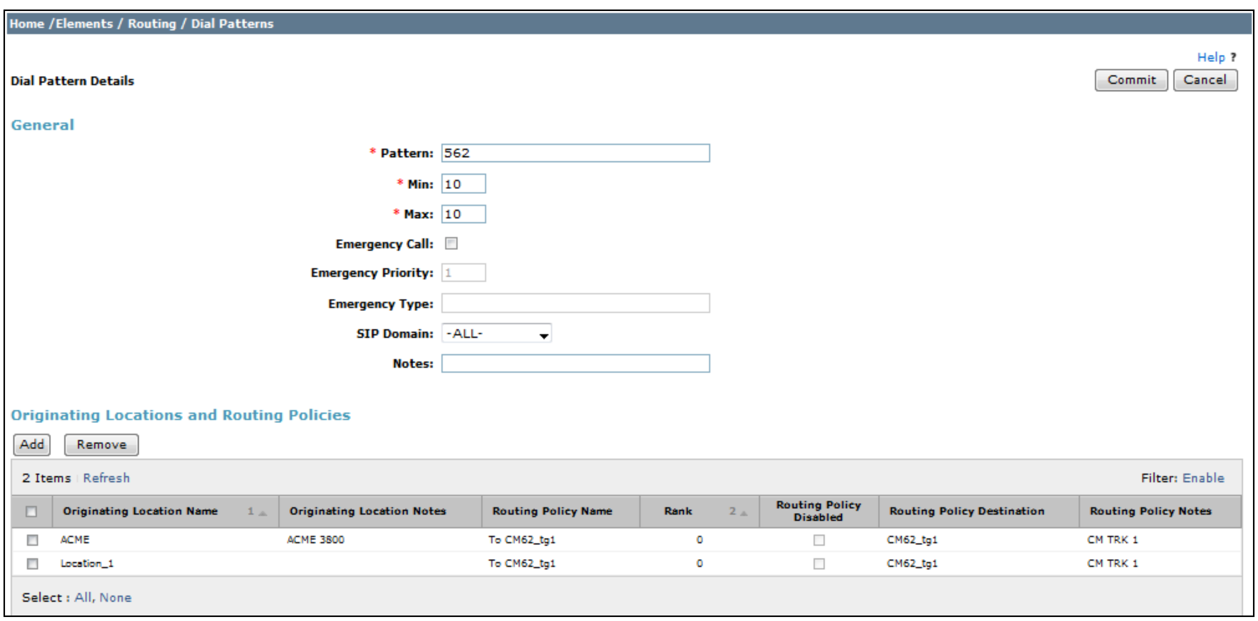
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

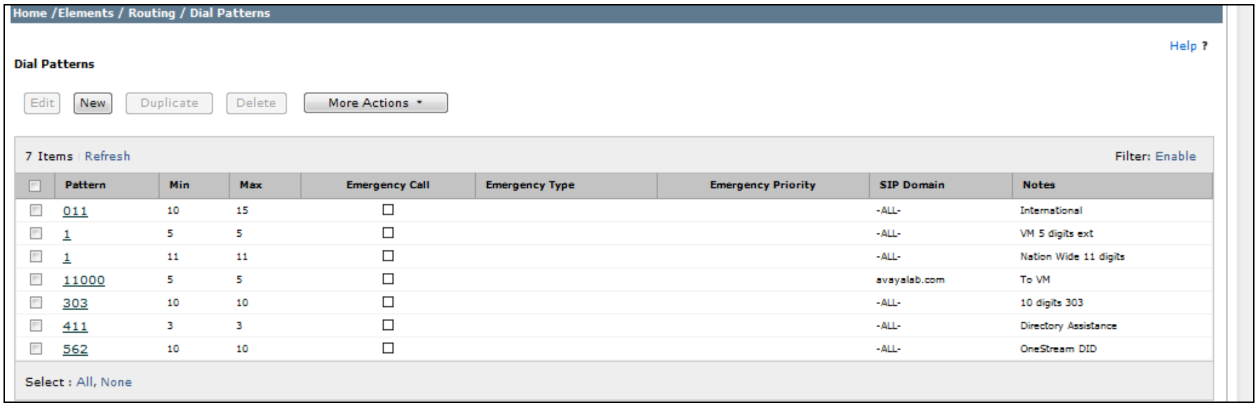
Two examples of the dial patterns used for the compliance test are shown below. The first example shows that numbers that begin with 1 and have a destination domain of **ALL** from **Locations_1** use route policy **To_ACME**.



The second example shows that 10 digit numbers that start with **562** to domain **ALL** and originating from **Location_1** and **ACME** use route policy **CM62_tg1**. These are the DID numbers assigned to the enterprise from OneStream.



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


Home /Elements / Routing / Dial Patterns

Help ?

Dial Patterns

Edit | New | Duplicate | Delete | More Actions

7 Items Refresh

Filter: Enable

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
011	10	15	☐			-ALL-	International
1	5	5	☐			-ALL-	VM 5 digits ext
1	11	11	☐			-ALL-	Nation Wide 11 digits
11000	5	5	☐			avayalab.com	To VM
303	10	10	☐			-ALL-	10 digits 303
411	3	3	☐			-ALL-	Directory Assistance
562	10	10	☐			-ALL-	OneStream DID

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, from the **Home** page, 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, select the appropriate Session Manager and 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:

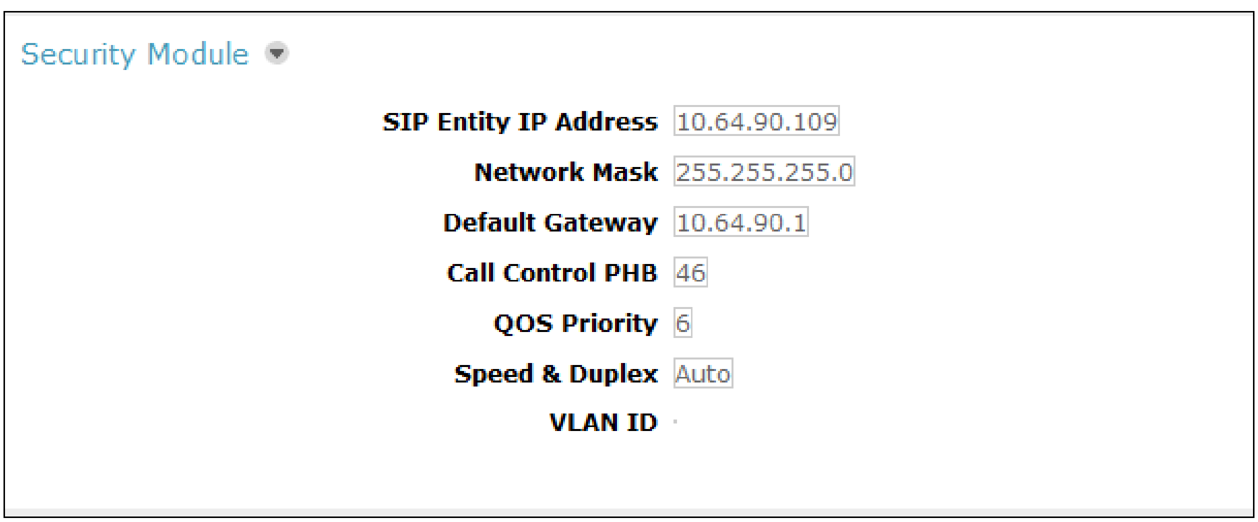
- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description**: Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

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 Net-Net 3820 Session Border Controller

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

1. Access the console port of the Acme Packet 3820 using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the 3820 for cable connection). Use the following settings for the serial port on the PC.
    - Bits per second: 9600
    - Data bits: 8
    - Parity : None
    - Stop bits: 1
    - Flow control: None

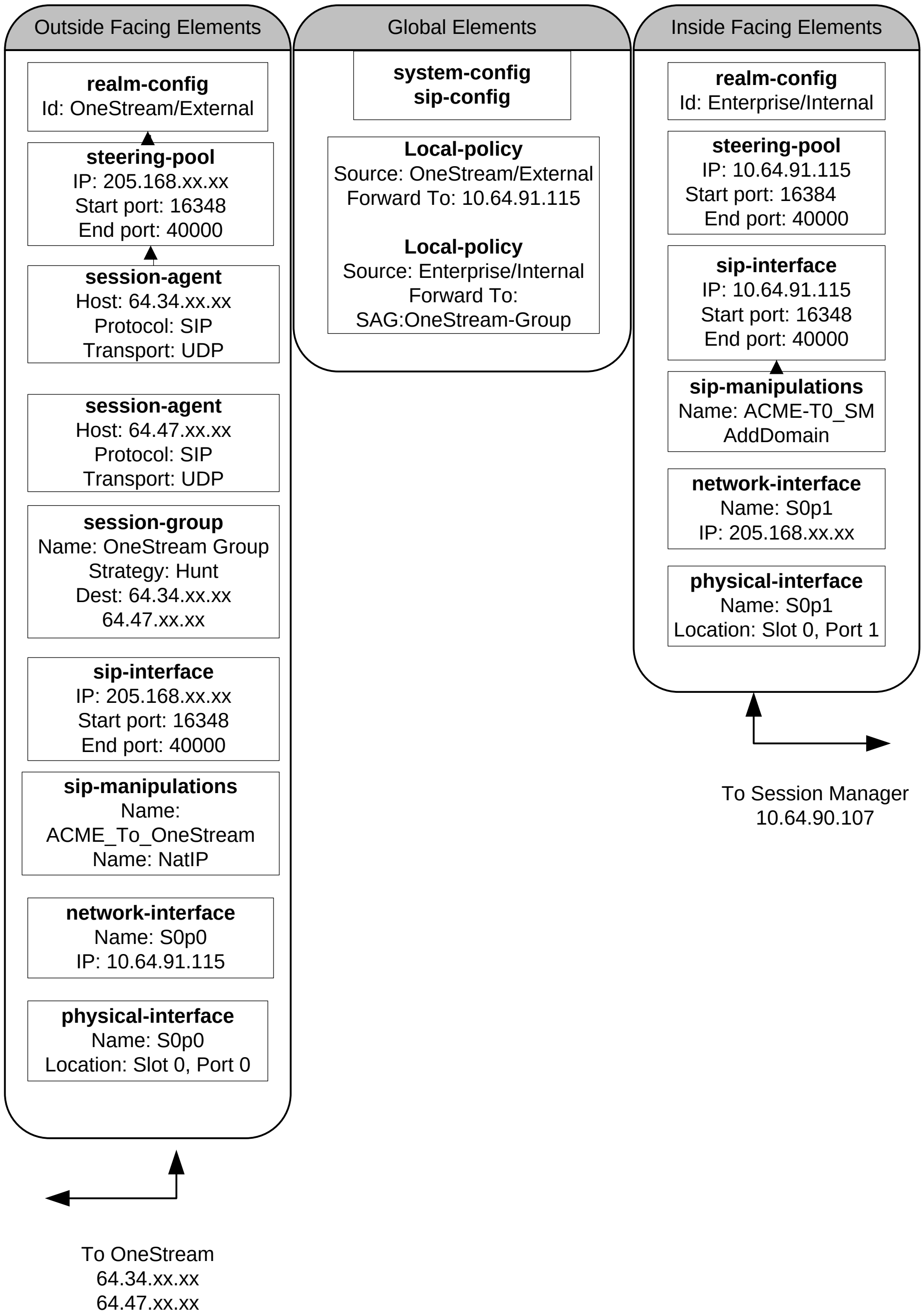
2. Log in to the Acme Packet 3820 with the user password.
3. Enable the Superuser mode by entering the **enable** command and then the superuser password. The command prompt will change to include a "#" instead of a ">" while in Superuser mode. This level of system access (i.e. at the "acmesystem#" prompt) will be referred to as the **main** level of the ACLI. Specific sub-levels of the ACLI will then be accessed to configure specific elements and specific parameters of those elements.
4. In Superuser mode, enter the **configure terminal** command. The **configure terminal** command is used to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the **configuration** level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface**).
7. Enter the name of an element parameter followed by its value (e.g., **name S0p0**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all the elements.
11. Enter **exit** to return to the main level.
12. Type **save-config** to save the entire configuration.
13. Type **activate-config** to activate the entire configuration.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

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

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to OneStream and Session Manager. These same fields are highlighted in **Appendix A**. The remaining fields are generally the default/standard value used by the Acme Packet 3820 for that field. For additional details on the administration of the Acme Packet 3820, see **Reference [16].**

A pictorial view of this configuration is shown below. It shows the internal components needed for the compliance test. Each of these components is defined in the Acme Packet 3820 configuration file contained in **Appendix A**. However, this section does not cover standard Acme Packet 3820 configurations that are not directly related to the interoperability test. The details of these configuration elements can be found in **Appendix A**.



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 → s0p1**
3. Enter **operation-type → Media**
4. Enter **port → 1**
5. Enter **slot →** 0
6. Enter **duplex-mode → FULL**
7. Enter **speed → 100**
8. Enter **done**
9. 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. The compliance test was performed with a direct Internet connection to the service using the settings below.

1. Enter **system → network-interface**
2. Enter **name → s0p1**
3. Enter **ip-address → 205.168.62.35**
4. Enter **netmask → 255.255.255.120**
5. Enter **gateway → 205.168.62.1**
6. Enter **hip-ip-list → 205.168.62.35**
7. Enter **icmp-ip-list → 205.168.62.35**
8. Enter **done**
9. 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 → s0p0**
3. Enter **ip-address → 10.64.91.115**
4. Enter **netmask → 255.255.255.0**
5. Enter **gateway → 10.64.91.1**
6. Enter **hip-ip-list → 10.64.91.115**
7. Enter **icmp-ip-list → 10.64.91.115**
8. Enter **done**
9. Enter **exit**

7.3. Realms

A realm represents a group of related Acme Packet 3820 components. Two realms were defined for the compliance test. The **outside** realm was defined for the external network and the **inside** realm was defined for the internal network.

out-manipulationid: For the **outside** realm **NatIP** was used and for the **inside** realm **AddDomain** was used. These names refer to a set of sip-manipulations (defined in **Section 7.10**) that are performed on outbound traffic from the Acme Packet 3820. These sip-manipulations are specified in each realm. Thus, these sip-manipulations are applied to outbound traffic from the public side (External) of the Acme Packet 3820 as well as to outbound traffic from the private side (Internal) of the Acme Packet 3820.

7.3.1. Outside Realm

Create a realm for the external network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → OneStream**
3. Enter **network-interfaces → s0p1:0**
4. Enter **out-manipulationid → NatIP**
5. Enter **done**
6. Enter **exit**

7.3.2. Inside Realm

Create a realm for the internal network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → Enterprise**
3. Enter **network-interfaces → s0p0:0**
4. Enter **out-manipulationid → addDomain**
5. Enter **done**

6. Enter **exit**

7.4. Steering-Pools

Steering pools define sets of ports that are used for steering media flows thru the 3800 Net-Net SBC.

7.4.1. Outside Steering-Pool

Create a steering-pool for the outside network. The start-port and end-port values should specify a range acceptable to the service provider. For the compliance test, no specific range was specified by the service provider, so the start and end ports shown below were chosen arbitrarily.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 205.168.xx.xx**
3. Enter **start-port → 16384**
4. Enter **end-port → 40000**
5. Enter **realm-id → OneStream**
6. Enter **done**
7. Enter **exit**

7.4.2. Inside Steering-Pool

Create a steering-pool for the inside network. The start-port and end-port values should specify a range acceptable to the internal enterprise network and include the port range used by Communication Manager. For the compliance test, a wide range was selected that included the default port range that Communication Manager uses and shown on the ip-network-region form in **Section 5.6**.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 10.64.91.115**
3. Enter **start-port → 16384**
4. Enter **end-port → 40000**
5. Enter **realm-id → Enterprise**
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 3820 Net-Net SBC SIP operating parameters. The home-realm is the internal default realm for the 3820 Net-Net SBC and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere. If the egress-realm is blank, the home-realm is used instead.

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 3800 Net-Net SBC.

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 → OneStream**
4. Enter **sip-port**
    a. Enter **address → 205.168.62.35**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → UDP**
    d. Enter **allow-anonymous → all**
    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 → Enterprise**
4. Enter **sip-port**
    a. Enter **address → 10.64.91.115**

   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 session-agent level.

7.8.1. Outside Session-Agent (1)

Create a session-agent for the outside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 64.34.45.227**
3. Enter **ip-address → 64.34.45.227**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP**
8. Enter **realm-id →OneStream**
9. Enter **description →**
10. Enter **ping-method → OPTIONS**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid →**
14. Enter **out-manipulationid →**
15. Enter **done**
16. Enter **exit**

7.8.2. Outside Session-Agent (2)

Create a session-agent for the outside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 64.47.118.70**
3. Enter **ip-address → 64.47.118.70**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**

7. Enter **transport-method → UDP**
8. Enter **realm-id →OneStream**
9. Enter **description →**
10. Enter **ping-method → OPTIONS**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid →**
14. Enter **out-manipulationid →**
15. Enter **done**
16. Enter **exit**

7.8.3. Outside Session-Agent Group

Session agents can be configured in a session agent group (SAG), so multiple session agents can be assigned to a route policy for fail-over or load balancing purposes. For compliance testing OneStream had two session agents assigned. Both of them were used for DIDs and were allocated for both inbound and outbound traffic. Both session agents allocated for inbound and outbound traffic were added to the SAG below.

Create a session-agent group for the outside network.

1. Enter group-name → **OneStream-Group**
2. Enter **description →**
3. Enter **port → 5060**
4. Enter **state → enabled**
5. Enter **app-protocol → SIP**
6. Enter **strategy → Hunt**
7. Enter **dest → 64.34.xx.xx ; 64.47.xx.xx**
8. Enter **trunk-group →**
9. Enter **sag-recursion → enabled**
10. Enter **stop-sag-recurse → 401,407**
11. Enter **home-realm-id→ Enterprise**
12. Enter **egress-relam-id→ Enterprise**
13. Enter **done**
14. Enter **exit**

7.9. Local Policies

Local policies allow SIP requests from the **INTERNAL** realm to be routed to the service provider session agent in the **EXTERNAL** realm (and vice-versa).

7.9.1. Enterprise to OneStream

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 → Enterprise**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → SAG:OneStream-Group**
    b. Enter **realm → OneStream**
    c. Enter **terminate-recursion → disabled**
    d. Enter **app-protocol → SIP**
    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

7.9.2. OneStream to Enterprise

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

1. Enter **session-router → local-policy**
2. Enter **from-address** → *
3. Enter **to-address → ***
4. Enter **source-realm → OneStream**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 10.64.90.109**
    b. Enter **realm → Enterprise**
    c. Enter **terminate-recursion → disabled**
    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 manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 7.3**, it was defined that the set of sip-manipulations named **NatIP** would be performed on outbound traffic in the **outside** realm and **AddDomain** would be performed on outbound traffic in **inside** realm.

The key SIP manipulation (sip-manipulation) fields are:

- **name:** The name of this set of SIP header rules.
- **header-rule**
  - **name:** The name of this individual header rule.
  - **header-name:** The SIP header to be modified.
  - **action:** The action to be performed on the header.
  - **comparison-type:** The type of comparison performed when determining a match.
  - **msg-type:** The type of message to which this rule applies.
  - **element-rule**
    - **name:** The name of this individual element rule.
    - **type:** Defines the particular element in the header to be modified.
    - **action:** The action to be performed on the element.
    - **match-val-type:** Element matching criteria on the data type (if any) in order to perform the defined action.
    - **comparison-type:** The type of comparison performed when determining a match.
    - **match-value:** Element matching criteria on the data value (if any) in order to perform the defined action.
    - **new-value:** New value for the element (if any).

In the configuration file in **Appendix A**, the **NatIP** sip manipulation has many modifications (or header-rules) defined. These header manipulations were added to hide the private IP address and enterprise domain name which appear in the "To", "From", "Request-URI", Diversion" and "PAI" SIP headers for outbound calls.

Similarly the **AddDomain** sip manipulation was used towards Session Manager to hide the public IP addresses and to add the enterprise domain to the "From" and "PAI" SIP headers.

7.10.1. Sip Manipulation- NatIP

The example below shows the **natFROM, header-rule** in the **NatIP** sip manipulation. It specifies that the "From and To" header in SIP request messages will be manipulated based on the element rule defined. The element rule **natHost** will match any value in the host part of the URI and replace it with the value of **$LOCAL_IP**. The value of **$LOCAL_IP** is the outside IP address of the Acme Packet 3820.

Enter **session-router** → **sip-manipulation**
1. Enter **name** → **NatIP**
2. Enter **header-rule** →

   a. Enter **name** → `natFROM`
   `b.Enter` **header-name** → **From**
   c. Enter **action** → **manipulate**
   d. Enter **comparison-type** → **case-sensitive**
   e. Enter **msg-type** → **request**

f.Enter **element-rule** →

a. Enter **name** → **natHost**
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**

This rule below 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. The element rule **natHost** will match any value in the host part of the URI and replace it with the value of **$ REMOTE_IP**. The value of **$REMOTE_IP** is the IP address of the Service provider, OneStream.

Enter **header-rule** →

a. Enter **name** → **natTO**
b.Enter header-name → To
c. Enter **action** → **manipulate**
d. Enter **comparison-type** → **case-sensitive**
e. Enter **msg-type** → **request**
f.Enter **element-rule** →

    a. Enter **name** → **natHost**
    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**

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

Enter **header-rule** →

a. Enter **name** → **natPAI**
b.Enter header-name → P-Asserted-Identity
c. Enter **action** → **manipulate**
d. Enter **comparison-type** → **case-sensitive**
e. Enter **msg-type** → **any**
f.Enter **element-rule** →

    a. Enter **name** → **natHost**
    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**

Enter **header-rule →**

a. Enter **name →** **remoteAlrtInfo**
b.Enter **header-name →** **Alert-Info**
c. Enter **action →** **delete**
d. Enter **comparison-type →** **case-sensitive**
e. Enter **msg-type →** **any**

Enter **header-rule →**

a. Enter **name →** **removePLoc**
b.Enter **header-name →** **P-Location**
c. Enter **action →** **delete**
d. Enter **comparison-type →** **case-sensitive**
e. Enter **msg-type →** **any**

This rule below replaces the host part of the Diversion 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.

Enter **header-rule →**

a. Enter **name →** **natDiversion**
b.Enter **header-name →** **Diversion**
c. Enter **action →** **manipulate**
d. Enter **comparison-type →** **case-sensitive**
e. Enter **msg-type →** **request**
f.Enter **element-rule →**
 a. Enter **name →** **natHost**
 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**

This rule stores the user part of the Nat Request with the service provider's IP address.

Enter **header-rule →**

a. Enter **name →** **natRequest**
b.Enter **header-name →** **Request-URI**
c. Enter **action →** **manipulate**
d. Enter **comparison-type →** **case-sensitive**
e. Enter **msg-type →** **request**
f.Enter **element-rule →**
 a. Enter **name →** **natHost**
 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**

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

Enter **header-rule** →
a. Enter **name** → **ReferToDomain**t
b.Enter **header-name** → **Refer-To**
c. Enter **action** → **manipulate**
d. Enter **comparison-type** → **case-sensitive**
e. Enter **msg-type** → **request**
f.Enter **element-rule** →
a. Enter **name** → **natHost**
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**

7.10.2. SIP Manipulation- addDomain

The example below shows the **FromDomain header-rule** in the **AddDomain** sip manipulation. It specifies that the "From" header in SIP request messages will be manipulated based on the element rule defined. The element rule **From** will match any value in the host part of the URI and replace it with the value of **avayalab.com**. The value of **avayalab.com** is the domain name used in the enterprise. This value should match the Domain set in Session Manager (**Section 6.2**) and the Communication Manager signaling group Far-end Domain (**Section 5.6**).

Enter **session-router** → **sip-manipulation**
1. Enter **name** → **addDomain**
2. Enter **header-rule** →
a. Enter **name** → **FromDomain**
b.Enter **header-name** → **From**
c. Enter **action** → **manipulate**
d. Enter **comparison-type** → **case-sensitive**
e. Enter **msg-type** → **request**
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** → **avayalab.com**

3. Enter **done**
4. Enter **exit**

8. Configure 9600 Series IP Telephones

For the compliance test, the DTMF payload header value for 9600 Series IP Telephones was set to 101 by adding the command **SET DTMF_PAYLOAD_TYPE=101** in the phone 46xxsettings.txt configuration file. Only the 9600 and 1600 SIP Telephones use this setting. The value of 101 is the value used by OneStream. The purpose of this configuration was to avoid a situation where a call between OneStream and the SIP phone could be established with a DTMF payload header value that is different in each direction of the call.

9. OneStream Networks Global SIP Trunking Configuration

OneStream is responsible for the network configuration of the OneStream SIP Trunking service. OneStream will require that the customer provide the public IP address used to reach the Acme 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 Acme 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.

10. 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.

3. Acme Packet 3820:
    - **show running-config –** Displays the current config
    - **show prom-info all –** Displays the all prom information including serial number, hardware revision, manufacturing date, part numbers and more
    - **show sipd sessions all –** Will display all of the active SIP sessions that are currently traversing the SBC, including the To, From, Call-ID.
    - **show support-info -** Outputs all of the system level info, including hardware specifics, licensing info, current call volume, etc.
    - **show health -** For a redundant system will give a status of synchronized processes and an overview of failover history
    - **show sipd invite -** Will display a chart of all recent SIP requests and responses
    - **display-alarms -** Alarm log output of recent and current alarms
    - **show logfile sipmsg.log -** Will output the contents of the sipmsg.log without having to FTP this file off the SBC

11. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Acme Net-Net 3820 Session Border Controller to OneStream SIP Trunking. OneStream SIP Trunking passed compliance testing. Please refer to **Section 2.2** for any exceptions or workarounds.

12. 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 6.2.1, July 2012.
[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, July 2012.
[3] *Administering Avaya Aura® Communication Manager*, Issue 7.0, July 2012, Document Number 03-300509.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation*, Issue 9.0, July 2012, Document Number 555-245-205.
[5] *Upgrading Avaya Aura® System Manager to 6.2*, Release 6.2, July 2012.
[6] *Administering Avaya Aura® System Manager*, Release 6.2, July 2012.
[7] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Document Number 03-603473.
[8] *Administering Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number 03-603324.
[9] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, April 2010, Document Number 16-601443.
[10] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Issue 8, March 2012, Document Number 16-300698.
[11] *Avaya one-X® Deskphone Edition SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
[12] *Avaya one-X® Deskphone SIP 9608, 9611G, 9621G, 9641G Administrator Guide*, Release 6.0.1, May 2011, Document Number 16-603813.
[13] *Administering Avaya one-X® Communicator*, October 2011.
[14] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/
[15] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/
[16] Acme Packet, "Net-Net 4000 S-C6.2.0 ACLI Configuration Guide", 400-0061-62, Nov 2009
[17] Acme Packet, "Net-Net 3800 Series And Net-Net 4500 SSM2 Installation Guide", 400-0114-20, Apr 2010
[18] Acme Packet, "Net-Net 3820 Hardware Installation Guide", 400-0134-10, Mar 2011

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

Included below is the Acme Packet 3820 configuration used during the compliance testing. The contents of the configuration can be shown by using the ACLI command **show running-config or show config** at the Acme packet 3820**.**

show config
host-routes
dest-network 10.64.90.0
netmask 255.255.255.0
gateway 10.64.91.1
description
last-modified-by admin@135.9.xx.xx
last-modified-date 2012-09-20 16:40:35
host-routes
dest-network 205.168.62.0
netmask 255.255.255.128
gateway 205.168.xx.xx
description
last-modified-by admin@192.168.xx.xx192.168.xx.xx
last-modified-date 2012-09-20 16:45:07
host-routes
dest-network 205.3.3.0
netmask 255.255.255.0
gateway 10.64.91.1
description
last-modified-by admin@192.168.xx.xx192.168.xx.xx
last-modified-date 2012-09-20 16:58:38

local-policy
from-address
*
to-address
*
source-realm
Enterprise
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
last-modified-by admin@192.168.xx.xx192.168.xx.xx

last-modified-date 2012-10-09 16:45:40
policy-attribute
next-hop SAG:OneStream-Group
realm OneStream
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP
state enabled
methods
media-profiles
lookup single
next-key
eloc-str-lkup disabled
eloc-str-match

local-policy
from-address
*
to-address
*
source-realm
OneStream
description
activate-time N/A
deactivate-time N/A
state enabled
policy-priority none
last-modified-by admin@192.168.xx.xx
last-modified-date 2012-10-08 16:22:26
policy-attribute
next-hop 10.64.90.109
realm Enterprise
action none
terminate-recursion disabled
carrier
start-time 0000
end-time 2400
days-of-week U-S
cost 0
app-protocol SIP


```
state                          enabled
methods
media-profiles
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         disabled
min-media-allocation           2000
min-trusted-allocation         4000
deny-allocation                32000
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@192.168.xx.xx
last-modified-date 2010-09-08 19:23:20

network-interface
name **wancom0**
sub-port-id 0
description
hostname
ip-address 192.168.xx.xx
pri-utility-addr
sec-utility-addr
netmask 255.255.255.0
gateway 192.168.xx.xxsec-gateway
gw-heartbeat
state disabled
heartbeat 0
retry-count 0
retry-timeout 1
health-score 0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list
ftp-address
icmp-address
snmp-address
telnet-address
ssh-address
last-modified-by admin@console
last-modified-date 2011-08-22 14:04:52

network-interface
name **s0p0**
sub-port-id 0
description
hostname
ip-address 10.64.91.115
pri-utility-addr
sec-utility-addr
netmask 255.255.255.0
gateway 10.64.91.1
sec-gateway
gw-heartbeat

state disabled
heartbeat 0
retry-count 0
retry-timeout 1
health-score 0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list 10.64.91.115
ftp-address
icmp-address 10.64.91.115
snmp-address
telnet-address
ssh-address
last-modified-by admin@192.168.xx.xx
last-modified-date 2012-09-20 16:09:07

network-interface
name **s0p1**
sub-port-id 0
description
hostname
ip-address 205.168.xx.xx
pri-utility-addr
sec-utility-addr
netmask 255.255.255.128
gateway 205.168.xx.1
sec-gateway
gw-heartbeat
state disabled
heartbeat 0
retry-count 0
retry-timeout 1
health-score 0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
hip-ip-list 205.168.xx.xx
ftp-address
icmp-address 205.168.xx.xx
snmp-address

telnet-address
ssh-address
last-modified-by admin@192.168.xx.xx
last-modified-date 2012-09-20 16:11:18
ntp-config
server 205.3.3.9
last-modified-by admin@192.168.xx.xxlast-modified-date 2010-09-08 19:26:51

phy-interface
name **wancom0**
operation-type Control
port 0
slot 1
virtual-mac
wancom-health-score 50
overload-protection disabled
last-modified-by admin@console
last-modified-date 2010-04-20 12:15:56

phy-interface
name **s0p0**
operation-type Media
port 0
slot 0
virtual-mac
admin-state enabled
auto-negotiation enabled
duplex-mode FULL
speed 100
overload-protection disabled
last-modified-by admin@192.168.xx.xxlast-modified-date 2010-04-20 12:31:37

phy-interface
name **s0p1**
operation-type Media
port 1
slot 0
virtual-mac
admin-state enabled
auto-negotiation enabled
duplex-mode FULL
speed 100
overload-protection disabled
last-modified-by admin@192.168.xx.xx
last-modified-date 2011-08-22 15:54:58

realm-config
identifier **OneStream**
description
addr-prefix 0.0.0.0
network-interfaces
s0p1:0
mm-in-realm enabled
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 NatIP
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
diam-e2-address-realm
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@192.168.xx.xx
last-modified-date 2012-10-09 15:53:44

realm-config
identifier **Enterprise**
description
addr-prefix 0.0.0.0
network-interfaces
s0p0:0
mm-in-realm enabled
mm-in-network enabled
mm-same-ip enabled

mm-in-system 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 addDomain
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
diam-e2-address-realm
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@192.168.xx.xx
last-modified-date           2012-10-09 15:53:29
session-agent
hostname                     10.64.90.109
ip-address                   10.64.90.109
port                         5060
state                        enabled
app-protocol                 SIP
app-type
transport-method             StaticTCP
realm-id                     Enterprise
egress-realm-id
description
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               Proxy
loose-routing                 enabled
send-media-session            enabled
response-map
ping-method                   OPTIONS
ping-interval                 60
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                      enabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                   disabled
in-manipulationid
out-manipulationid
manipulation-string
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@192.168.xx.xx
last-modified-date 2012-10-08 16:19:59

session-agent
hostname **64.34.xx.xx**
ip-address 64.34.xx.xx
port 5060
state enabled
app-protocol SIP
app-type
transport-method UDP
realm-id OneStream
egress-realm-id
description
carriers
allow-next-hop-lp enabled
constraints disabled
max-sessions 0
max-inbound-sessions 0
max-outbound-sessions 0
max-burst-rate 0
max-inbound-burst-rate 0
max-outbound-burst-rate 0
max-sustain-rate 0
max-inbound-sustain-rate 0
max-outbound-sustain-rate 0
min-seizures 5
min-asr 0
time-to-resume 0
ttr-no-response 0
in-service-period 0
burst-rate-window 0
sustain-rate-window 0
req-uri-carrier-mode None
proxy-mode
redirect-action
loose-routing enabled

send-media-session enabled
response-map
ping-method OPTIONS
ping-interval 60
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 enabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me disabled
in-manipulationid
out-manipulationid
manipulation-string
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@192.168.xx.xx
last-modified-date 2012-10-08 15:59:50

session-agent
hostname **64.47.xx.xx**
ip-address 64.47.xx.xx

```
port                        5060
state                       enabled
app-protocol                SIP
app-type
transport-method            UDP
realm-id                    OneStream
egress-realm-id
description
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
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@192.168.xx.xx
last-modified-date 2012-10-09 15:45:04

session-group
group-name **OneStream-Group**
description
state enabled
app-protocol SIP
strategy **Hunt**
dest
64.34.xx.xx
64.47.xx.xx
trunk-group
sag-recursion enabled
stop-sag-recurse 401,407
last-modified-by admin@192.168.xx.xxlast-modified-date 2012-10-18 14:33:05
sip-config
state enabled
operation-mode dialog
dialog-transparency enabled

home-realm-id Enterprise
egress-realm-id Enterprise
nat-mode None
registrar-domain
registrar-host
registrar-port 0
register-service-route always
init-timer 500
max-timer 4000
trans-expire 32
invite-expire 180
inactive-dynamic-conn 32
enforcement-profile
pac-method
pac-interval 10
pac-strategy PropDist
pac-load-weight 1
pac-session-weight 1
pac-route-weight 1
pac-callid-lifetime 600
pac-user-lifetime 3600
red-sip-port 1988
red-max-trans 10000
red-sync-start-time 5000
red-sync-comp-time 1000
add-reason-header disabled
sip-message-len 4096
enum-sag-match disabled
extra-method-stats enabled
registration-cache-limit 0
register-use-to-for-lp disabled
options max-udp-length=65535
set-inv-exp-at-100-resp
refer-src-routing disabled
add-ucid-header disabled
proxy-sub-events
pass-gruu-contact disabled
sag-lookup-on-redirect disabled
set-disconnect-time-on-bye disabled
last-modified-by admin@192.168.xx.xx
last-modified-date 2012-10-08 15:34:13

sip-interface
state enabled
realm-id **OneStream**

```
description
sip-port
address                   205.168.xx.xx
port                      5060
transport-protocol        UDP
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@192.168.xx.xx
last-modified-date 2012-10-08 15:42:00

sip-interface
state enabled
realm-id **Enterprise**
description
sip-port
address 10.64.91.115
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@192.168.xx.xx
last-modified-date 2012-10-08 15:52:43

sip-manipulation
name **addDomain**
description
split-headers
join-headers
header-rule
name FromDomain
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 avayalab.com
header-rule
name PaiDomain
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 avayalab.com
last-modified-by admin@192.168.xx.xx
last-modified-date 2012-10-08 17:20:03

sip-manipulation
name **NatIP**
description
split-headers
join-headers
header-rule
name natFROM
header-name From
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name natHost
parameter-name
type uri-host
action replace
match-val-type any
comparison-type case-sensitive
match-value
new-value $LOCAL_IP
header-rule
name natTO
header-name To
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name natHost
parameter-name
type uri-host
action replace
match-val-type any
comparison-type case-sensitive
match-value


```
new-value              $REMOTE_IP
header-rule
name                   natPAI
header-name            P-Asserted-Identity
action                 manipulate
comparison-type        case-sensitive
msg-type               any
methods
match-value
new-value
element-rule
name                   natHost
parameter-name
type                   uri-host
action                 replace
match-val-type         any
comparison-type        case-sensitive
match-value
new-value              $LOCAL_IP
header-rule
name                   remoteAlrtInfo
header-name            Alert-Info
action                 delete
comparison-type        case-sensitive
msg-type               any
methods
match-value
new-value
header-rule
name                   removePLoc
header-name            P-Location
action                 delete
comparison-type        case-sensitive
msg-type               any
methods
match-value
new-value
header-rule
name                   natDiversion
header-name            Diversion
action                 manipulate
comparison-type        case-sensitive
msg-type               request
methods
match-value
```

new-value
element-rule
name natHost
parameter-name
type uri-host
action replace
match-val-type any
comparison-type case-sensitive
match-value
new-value $REMOTE_IP
header-rule
name natRequest
header-name Request-URI
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name natHost
parameter-name
type uri-host
action replace
match-val-type any
comparison-type case-sensitive
match-value
new-value $REMOTE_IP
header-rule
name ReferToDomain
header-name Refer-To
action manipulate
comparison-type case-sensitive
msg-type request
methods
match-value
new-value
element-rule
name NatHost
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@135.9. xx.xxlast-modified-date 2012-10-18 14:45:29

steering-pool
ip-address 205.168.xx.xx
start-port 16384
end-port 40000
realm-id OneStream
network-interface s0p1:0
last-modified-by admin@192.168.xx.xxlast-modified-date 2012-10-09 14:48:48
steering-pool
ip-address 10.64.91.115
start-port 16384
end-port 40000
realm-id Enterprise
network-interface s0p0:0
last-modified-by admin@135.9. xx.xx
last-modified-date 2012-10-09 16:11:43
system-config
hostname Enterprise-Acme
description
location
mib-system-contact
mib-system-name
mib-system-location
snmp-enabled enabled
enable-snmp-auth-traps disabled
enable-snmp-syslog-notify disabled
enable-snmp-monitor-traps disabled
enable-env-monitor-traps disabled
snmp-syslog-his-table-length 1
snmp-syslog-level WARNING
system-log-level WARNING
process-log-level NOTICE
process-log-ip-address 0.0.0.0
process-log-port 0
collect
sample-interval 5
push-interval 15
boot-state disabled
start-time now
end-time never
red-collect-state disabled
red-max-trans 1000
red-sync-start-time 5000

```
red-sync-comp-time            1000
push-success-trap-state       disabled
call-trace                    disabled
internal-trace                disabled
log-filter                    all
default-gateway               205.168.xx.1
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@192.168.xx.xx
last-modified-date            2012-09-20 16:12:07
task done
ACME_SP#
```