Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet 3820 Net-Net® Session Director 6.2.0 with CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager, and Acme Packet 3820 Net-Net Session Director 6.2.0 with various Avaya endpoints.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solutions and Interoperability Test Lab, utilizing CenturyLink SIP Trunk Services.

©2012 Avaya Inc. All Rights Reserved.

Table of Contents

1. Introduction 4
2. General Test Approach and Test Results 4
   2.1. Interoperability Compliance Testing 4
   2.2. Test Results 5
   2.3. Support 5
3. Reference Configuration 6
4. Equipment and Software Validated 7
5. Configure Avaya Aura® Communication Manager 7
   5.1. Licensing and Capacity 8
   5.2. System Features 9
   5.3. IP Node Names 10
   5.4. Codecs 10
   5.5. IP Interface for procr 11
   5.6. IP Network Region 11
   5.7. Signaling Group 13
   5.8. Trunk Group 15
   5.9. Inbound Routing 17
   5.10. Calling Party Information 18
   5.11. Outbound Routing 19
   5.12. Saving Communication Manager Configuration Changes 22
6. Configure Avaya Aura® Session Manager 23
   6.1. Avaya Aura® System Manager Login and Navigation 23
   6.2. Specify SIP Domain 25
   6.3. Add Location 25
   6.4. Add SIP Entities 28
   6.5. Add Entity Links 33
   6.6. Add Routing Policies 35
   6.7. Add Dial Patterns 36
   6.8. Verify Avaya Aura® Session Manager Instance 39
7. Configure Acme Packet 3820 Net-Net® Session Director 41
   7.1. Acme Packet Command Line Interface Summary 43
   7.2. System Configuration 44
   7.3. Physical and Network Interfaces 45
   7.4. Realm 47
   7.5. SIP Configuration 49
   7.6. SIP Interface 50
   7.7. Session Agent 51
   7.8. Session Agent Group 54
   7.9. SIP Manipulation 55
   7.10. Steering Pools 58

©2012 Avaya Inc. All Rights Reserved.

7.11. Local Policy 58
8. CenturyLink SIP Trunk Service Configuration 60
9. Verification and Troubleshooting 60
9.1. Verification 60
9.2. Troubleshooting 62
10. Conclusion 62
11. Additional References 63
Appendix A: Acme Packet 3820 Configuration File 64

©2012 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Acme Packet 3820 Net-Net Session Director 6.2.0 (Acme Packet 3820) integration with CenturyLink SIP Trunk (Legacy Qwest) version 7.3.5R6.

In the sample configuration, the Acme Packet 3820 is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Acme Packet 3820 performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the CenturyLink SIP Trunk access method.

Communication Manager and Session Manager are connected using two Communication Manager SIP trunk groups. One trunk group is used for internal SIP traffic including SIP phones and Avaya Aura® Messaging, while the other is used for external SIP traffic. Session Manager then has one connection to Acme Packet 3820 for CenturyLink SIP traffic.

CenturyLink SIP Trunk is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

CenturyLink SIP Trunk will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE). SIP Trunk will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager, Session Manager and the Session Border Controller to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

CenturyLink SIP Trunk Service passed compliance testing.

2.1. Interoperability Compliance Testing

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

©2012 Avaya Inc. All Rights Reserved.

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client).
- Avaya one-X Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Each supported protocol was tested.
- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, emergency calls (911) and local directory assistance (411).
- Codecs G.729A, G.729AB and G.711MU.
- DTMF transmission using RFC 2833.
- T.38 Fax
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).

Items not supported or not tested included the following:

- Inbound toll-free is supported but was not tested as part of the compliance test.
- Network Call Redirection using the SIP REFER method or a 302 response is not supported by CenturyLink.

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink SIP Trunk solution. It is listed here simply as an observation.

2.3. Support

For technical support on the CenturyLink SIP Trunk Service, contact CenturyLink using the Customer Support links at www.centurylink.com

©2012 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the CenturyLink SIP Trunks to East and West servers. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Acme Packet 3820 provides NAT functionality and SIP header manipulation. The Acme Packet 3820 receives traffic from CenturyLink SIP Trunk on port 5060 and sends traffic to the CenturyLink SIP Trunk using destination port 5060, using the UDP protocol. 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 cannot be routed by the PSTN.

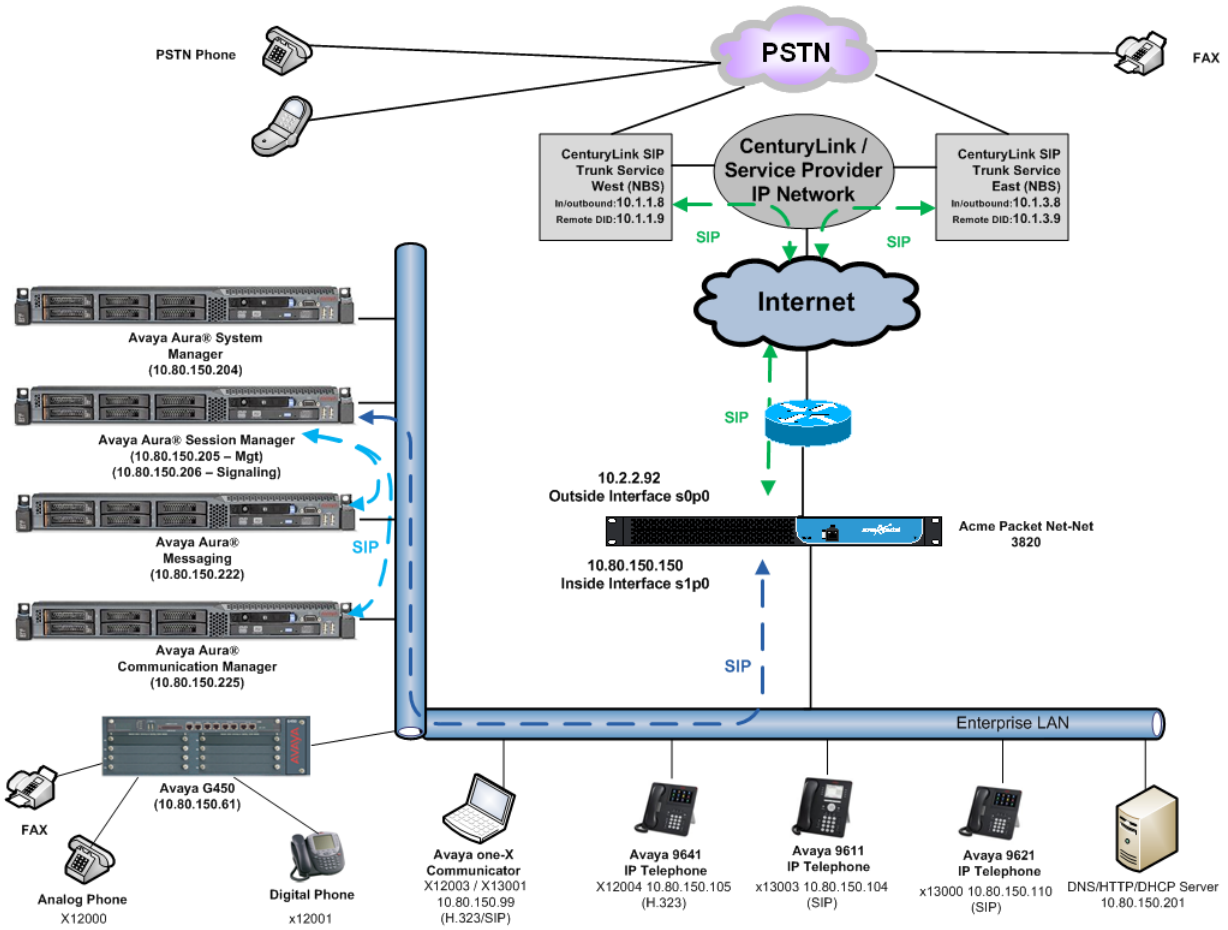

Figure 1: Avaya Interoperability Test Lab Configuration

©2012 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager	R016x.00.1.510.1-19303 (SP 5)
Avaya Aura® Messaging	R016x.00.1.510.1-004_0302 (SP 3)
Avaya Aura® System Manager	6.1.0.0.7345-6.1.5.115
Avaya Aura® Session Manager	6.1.4.0.614005
Acme Packet 3820 Net-Net 3820	6.2.0
Avaya G430	31.18.1
Avaya 9641 IP Telephone (H.323)	Avaya one-X Deskphone Edition 6.0.1
Avaya 9621 IP Telephone (SIP)	Avaya one-X Deskphone SIP Edition 6.0.1
Avaya 9611 IP Telephone (SIP)	Avaya one-X Deskphone SIP Edition 6.0.1
Avaya one-X Communicator (H.323 and SIP)	6.1.0.12
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink (Legacy Qwest) SIP Trunking Solution Components	
Component	Release
NBS	07.03.05 R006

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing.

Note: **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 CenturyLink SIP Trunk Service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from CenturyLink. It is assumed the general installation of Communication Manager, Avaya G430 Media Gateway and Session Manager has been previously completed and is not discussed here.

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

©2012 Avaya Inc. All Rights Reserved.

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** licenses are available and **275** 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 3
             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 275
  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
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

Figure 2: System Parameters Customer Options Page 2

©2012 Avaya Inc. All Rights Reserved.

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**.

```
change 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
```

Figure 3: System Parameters Feature Page 1

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 types of calls.

```
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

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

Figure 4: System Parameters Feature Page 9

©2012 Avaya Inc. All Rights Reserved.

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 Communication Manager (**procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
SM                  10.80.150.206
default             0.0.0.0
procr               10.80.150.225
procr6              ::
```

Figure 5: Node Names IP

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. The CenturyLink SIP Trunk Service supports G.729A, G.729AB and G.711MU. During compliance testing each of the supported codecs were tested independently by changing the order of preference to list the codec being tested as the first choice. The true order of preference is defined by the end customer. In the example below, **G.729A** and **G.711MU** were entered in the **Audio Codec** column of the table. 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.729A           n          2        20
 2: G.711MU          n          2        20
 3:
```

Figure 6: IP Codec Set 2 Page 1

©2012 Avaya Inc. All Rights Reserved.

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-standard        0
    Modem            off                  0
    TDD/TTY          US                   3
```

Figure 7: IP Codec Set 2 Page 2

5.5. IP Interface for procr

The **add ip-interface procr** or **change ip-interface procr** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

```
change ip-interface procr                                       Page   1 of   2
                                  IP INTERFACES


                  Type: PROCR
                                                     Target socket load: 1700

      Enable Interface? y                          Allow H.323 Endpoints? y
                                                    Allow H.248 Gateways? y
        Network Region: 1                            Gatekeeper Priority: 5


                                IPV4 PARAMETERS
             Node Name: procr                    IP Address: 10.80.150.225


           Subnet Mask: /24
```

Figure 8: IP Interface procr

5.6. 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. IP network region 1 is the default IP network region and encompasses the rest of the enterprise. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Location** field to match the enterprise location for this SIP trunk.

©2012 Avaya Inc. All Rights Reserved.

- 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. To enable shuffling, 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: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Figure 9: IP Network Region 2 Page 1

©2012 Avaya Inc. All Rights Reserved.

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

```
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
 3
 4
```

Figure 10: IP Network Region 2 Page 4

5.7. 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 **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). 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). This is necessary so the SM can distinguish this trunk from the trunk used for other enterprise SIP traffic. Port **5081**was used for compliance testing.
- Set the **Peer Detection Enabled** field to **n**.
- Set the **Peer Server** to **Others**. When the Peer Server is detected or set to SM, Communication Manager precedes a + sign to the From, Contact and P-Asserted Identity headers. The addition of the + sign impacted interoperability with CenturyLink.
- 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 **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**.
- 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.

©2012 Avaya Inc. All Rights Reserved.

- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```
change signaling-group 2                                        Page   1 of   1
                                SIGNALING GROUP

 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                            SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? n  Peer Server: Others



   Near-end Node Name: procr                 Far-end Node Name: SM
 Near-end Listen Port: 5081                Far-end Listen Port: 5081
                                        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
```

Figure 11: Signaling Group 2

©2012 Avaya Inc. All Rights Reserved.

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**. For the compliance test, trunk group 2 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 2                                                Page   1 of  21
                                 TRUNK GROUP

Group Number: 2                     Group Type: sip           CDR Reports: y
  Group Name: SIP SP 2                     COR: 1        TN: 1        TAC: *02
   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: 2
                                                       Number of Members: 10
```

Figure 12: Trunk Group 2 Page 1

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

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

TRUNK PARAMETERS

     Unicode Name: auto

                                          Redirect On OPTIM Failure: 5000

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

 Disconnect Supervision - In? y  Out? y
```

Figure 13: Trunk Group 2 Page 2

©2012 Avaya Inc. All Rights Reserved.

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end.

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. Set **Modify Tandem Calling Number** to **tandem-cpn-form**. Default values were used for all other fields.

```
add trunk-group 2                                                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: tandem-cpn-form


 Show ANSWERED BY on Display? y
```

Figure 14: Trunk Group 2 Page 3

On **Page 4**, set the **Network Call Redirection** field to **n**. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. Set the **Support Request History** field to **n**.

Set the **Telephone Event Payload Type** to **100**, the value preferred by CenturyLink.

```
add trunk-group 2                                                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? n
               Telephone Event Payload Type: 100


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

Figure 15: Trunk Group 2 Page 4

©2012 Avaya Inc. All Rights Reserved.

5.9. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by CenturyLink is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group.

Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID. As an example, the following screen illustrates a conversion of DID number **3035557104** to extension **12004**.

```
change inc-call-handling-trmt trunk-group 1                    Page   1 of  30
                        INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 3035557104       10  12004
 public-ntwrk    10 3035557105       10  12005
 public-ntwrk    10 3035557106       10  13000
 public-ntwrk    10 3035557107       10  13001
 public-ntwrk    10 3035557108       10  13002
 public-ntwrk    10 3035557127       10  13003
 public-ntwrk    10 6145555714       10  13004
 public-ntwrk    10 6145555715       10  12000
```

Figure 16: Incoming Call Handling Treatment

©2012 Avaya Inc. All Rights Reserved.

5.10. 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 5.8**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is used to authenticate the caller.

In the bolded row shown in the example abridged output below, a specific Communication Manager extension (x12004) is mapped to a DID number that is known to CenturyLink for this SIP Trunk connection (3035557104), when the call uses trunk group 2.

```
change public-unknown-numbering 5 ext-digits 12000 trunk-group 2Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                             Total
Ext Ext            Trk       CPN              CPN
Len Code           Grp(s)    Prefix           Len
                                                   Total Administered: 22
 5  12000          2         6145555715       10       Maximum Entries: 9999
 5  12001          2         6145555716       10
 5  12004          2         3035557104       10    Note: If an entry applies to
 5  12005          2         3035557105       10    a SIP connection to Avaya
 5  13000          2         3035557106       10    Aura(tm) Session Manager,
 5  13001          2         3035557107       10    the resulting number must
 5  13002          2         3035557108       10    be a complete E.164 number.
 5  13003          2         3035557127       10
 5  13004          2         6145555714       10
```

Figure 17: Public Unknown Numbering

Use the **change tandem-calling-party-num** command, to define the calling party number to send to the PSTN for tandem calls from SIP users.

In the example shown below, calls originating from extension 13001 and routed to trunk group 2 will result in a 10-digit calling number. For **Number Format**, use an applicable format, in this case **pub-unk**.

```
change tandem-calling-party-num                                  Page   1 of   8
                  CALLING PARTY NUMBER CONVERSION
                          FOR TANDEM CALLS
     CPN              Trk                                  Number
 Len Prefix           Grp(s)     Delete  Insert            Format

 5   13001            2          5       3035557107        pub-unk
 5   13002            2          5       3035557108        pub-unk
 5   13003            2          5       3035557127        pub-unk
 5   13004            2          5       6145555714        pub-unk
```

Figure 18: Tandem Calling Party Number

©2012 Avaya Inc. All Rights Reserved.

5.11. 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. 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
```

Figure 19: Dialplan Analysis

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:
```

Figure 20: Feature Access Codes

©2012 Avaya Inc. All Rights Reserved.

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9.

- **Dialed String:** enter the leading digits (e.g., **1303**) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., **11**) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., **11**) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., **1**) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.
- **Call Type: fnpa** the call type for North American 1+10 digit calls. For local 7 or 10 digit calls enter **hnpa**. The call type tells Communication Manager what kind of call is made to help decide how to handle the dialed string and whether or not to include a preceding 1. For more information and a complete list of Communication Manager call types, see **Reference [3]** and **[4]**.

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 1                                          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
    1303                  11   11    1        fnpa         n
    1502                  11   11    1        fnpa         n
    1720                  11   11    1        fnpa         n
    1800                  11   11    1        fnpa         n
    1866                  11   11    1        fnpa         n
    1877                  11   11    1        fnpa         n
    1888                  11   11    1        fnpa         n
    1908                  11   11    1        fnpa         n
    2                     10   10    1        hnpa         n
    3                     10   10    1        hnpa         n
    4                     10   10    1        hnpa         n
    411                   3    3     1        svcl         n
    5                     10   10    1        hnpa         n
    555                   7    7     deny     hnpa         n
    6                     10   10    1        hnpa         n
```

Figure 21: ARS Analysis

©2012 Avaya Inc. All Rights Reserved.

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 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 **2** 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 1 will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: CENTURYLINK SIP TRK
                                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: 2    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
 4: y y y y y n  n            rest                                        none
 5: y y y y y n  n            rest                                        none
 6: y y y y y n  n            rest                                        none
```

Figure 22: Route Pattern 1

©2012 Avaya Inc. All Rights Reserved.

Use the **change ars digit-conversion** command to manipulate the routing of dialed digits that match the DIDs to prevent these calls from going out the PSTN and using unnecessary SIP trunk resources. The example below shows the DID numbers assigned by CenturyLink being converted to 5 digit extensions.

```
change ars digit-conversion 0                                    Page   1 of   2
                        ARS DIGIT CONVERSION TABLE
                                  Location: all                Percent Full: 0

  Matching Pattern     Min   Max   Del   Replacement String   Net  Conv ANI Req

  3035557104           10    10    10    12004                ext   y       n
  3035557105           10    10    10    12005                ext   y       n
  3035557106           10    10    10    10000                ext   y       n
  3035557107           10    10    10    13004                ext   y       n
  3035557108           10    10    10    13002                ext   y       n
  3035557109           10    10    10    13001                ext   y       n
  3035557127           10    10    10    13003                ext   y       n
  6145555686           10    10    10    13000                ext   y       n
  6145555711           10    10    10    13003                ext   y       n
  6145555714           10    10    10    13004                ext   y       n
  6145555715           10    10    10    12000                ext   y       n
```

Figure 23: ARS Digit Conversion

5.12. Saving Communication Manager Configuration Changes

The command **save translation all** can be used to save the configuration.

```
save translation all

                              SAVE TRANSLATION

           Command Completion Status                                Error Code

           Success                                                  0
```

Figure 24: Save Translation All

©2012 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Session Manager

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

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Acme Packet and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager Instance, corresponding to the Session Manager server to be administered in 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 **Log On** (not shown). The screen shown below is then displayed.

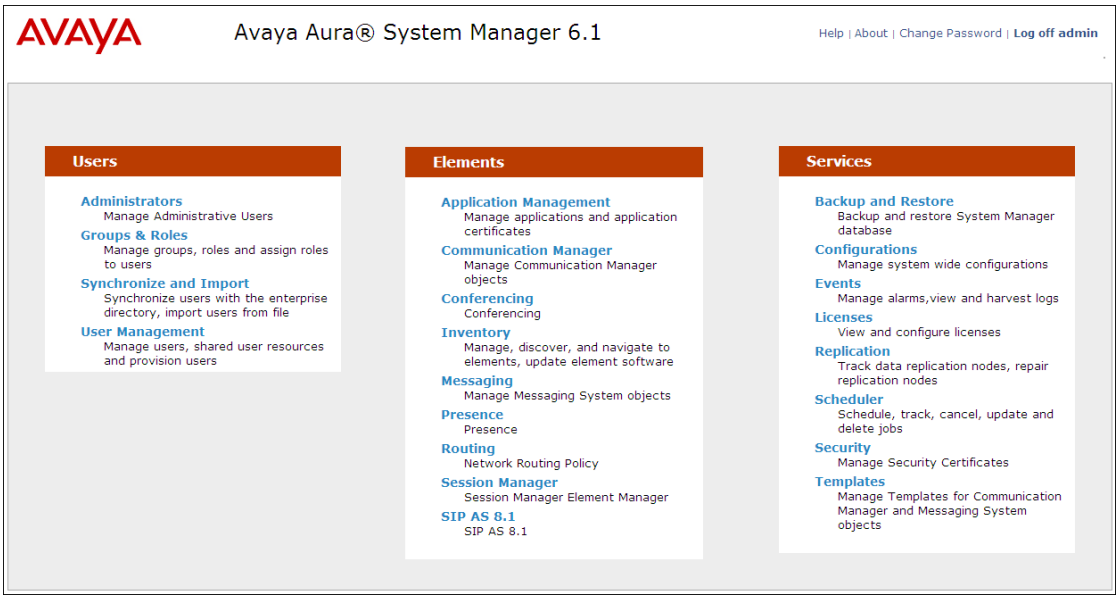

Figure 25: System Manager Main Menu

©2012 Avaya Inc. All Rights Reserved.

Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.

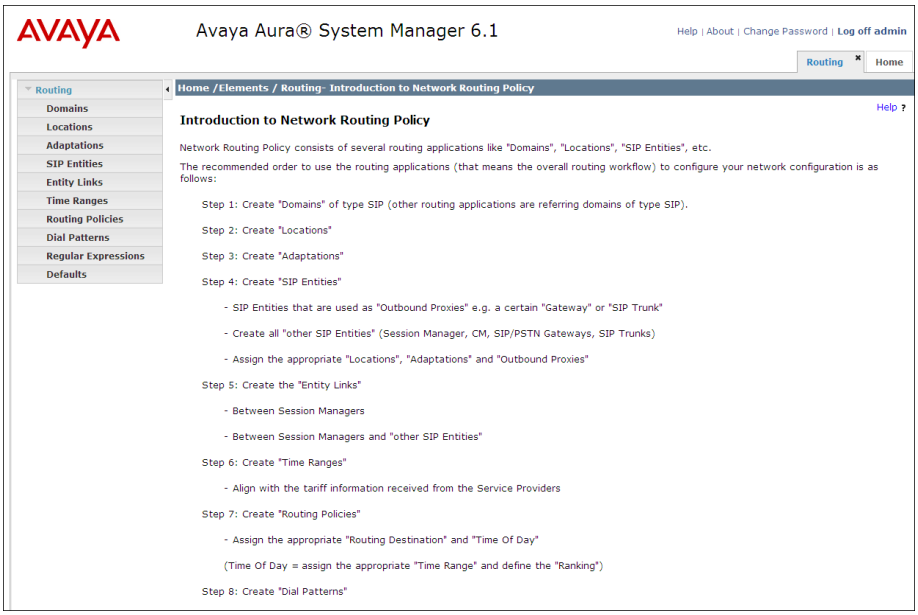

Figure 26: Introduction to Network Routing Policy

©2012 Avaya Inc. All Rights Reserved.

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 (**avayalab.com**). Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, 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 **avayalab.com** domain.

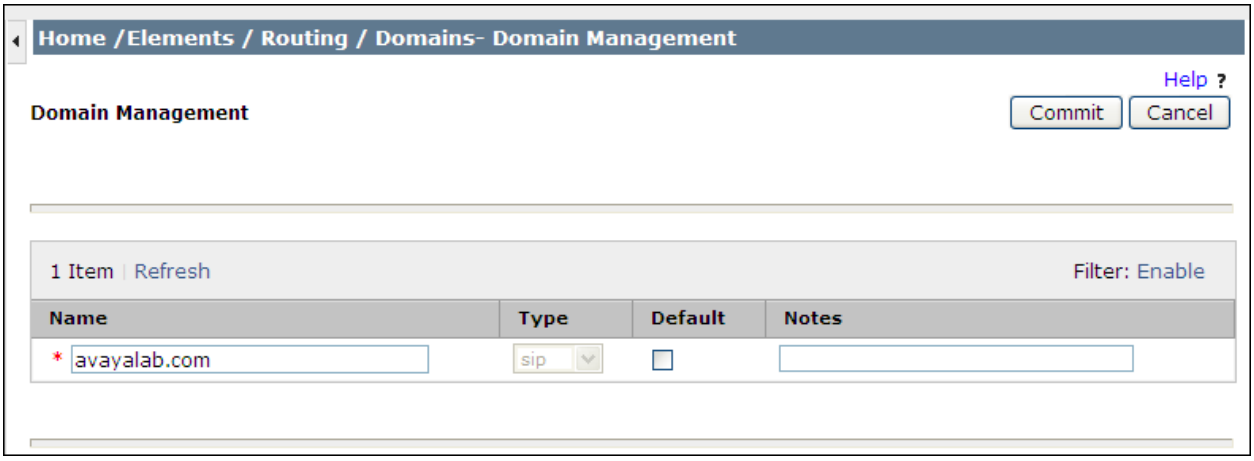

Figure 27: SIP Domain in Session Manager

6.3. Add Location

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

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

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

The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration, Locations are added to SIP Entities (**Section 6.4**), so it was not necessary to add a pattern.

©2012 Avaya Inc. All Rights Reserved.

The screen below shows the addition of **Location_150_SM**, this location will be used for Session Manager. Click **Commit** to save.

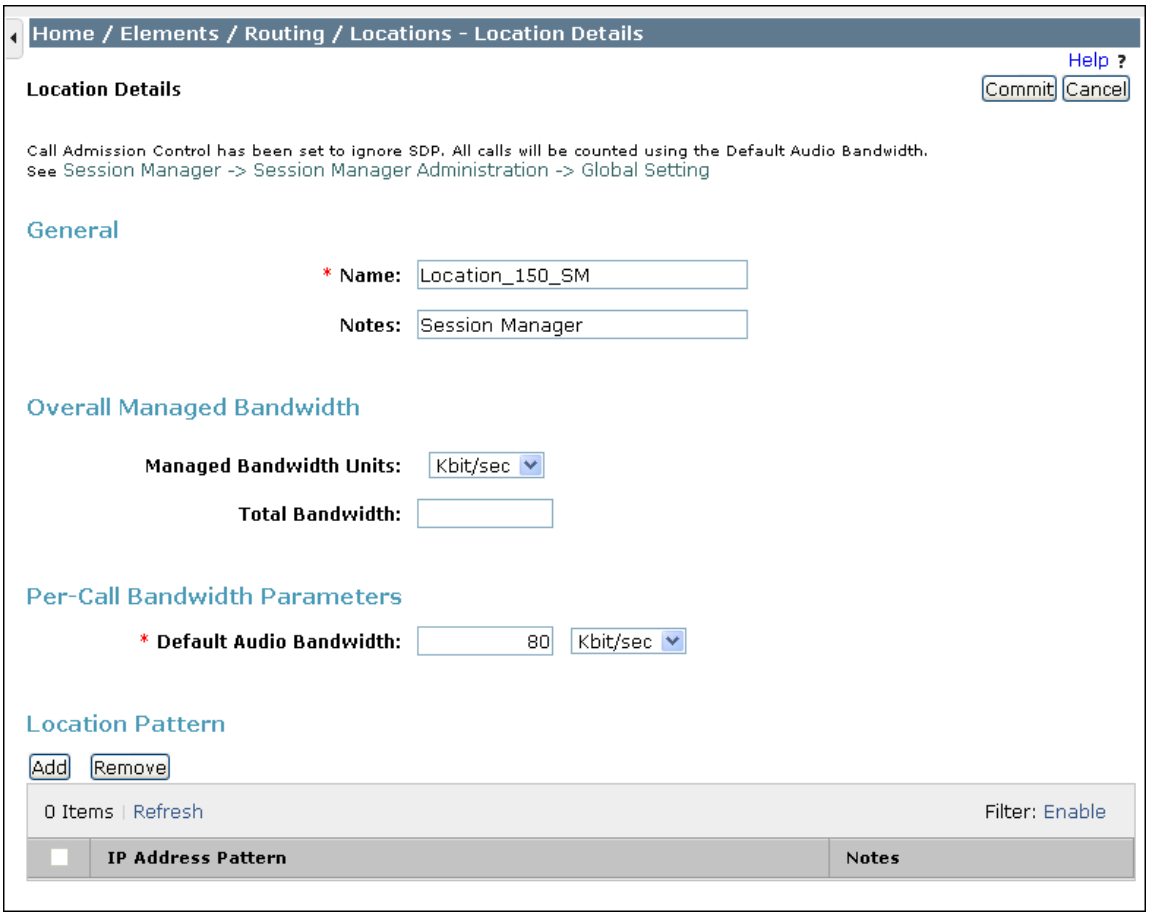

Figure 28: Creating a Location for Session Manager

Note: Call bandwidth management parameters should be set per customer requirement.

©2012 Avaya Inc. All Rights Reserved.

Repeat the preceding procedure to create a separate Location for Communication Manager and Acme Packet 3820. Displayed below is the screen for **Location_150_CM** used for Communication Manager.

Home / Elements / Routing / Locations - Location Details

Help ?

Location Details Commit Cancel

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* **Name:** Location_150_CM

Notes: Communication Manager

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* **Default Audio Bandwidth:** 80 Kbit/sec

Location Pattern

Add Remove

0 Items | Refresh Filter: Enable

	IP Address Pattern	Notes

* **Input Required** Commit Cancel

Figure 29: Creating a Location for Communication Manager

©2012 Avaya Inc. All Rights Reserved.

Below is the screen for **Acme-LOC150** used for Acme Packet 3820.

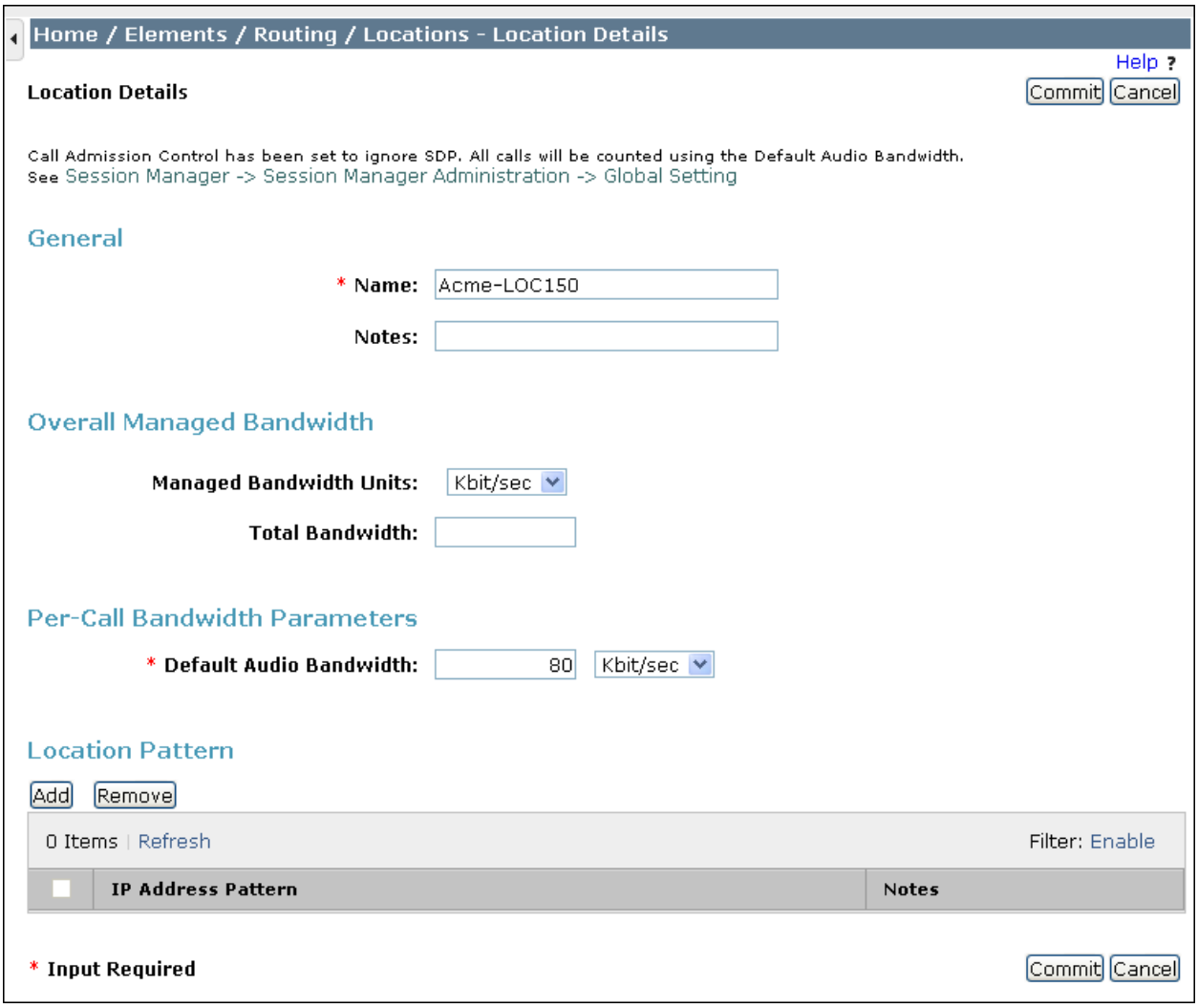

Figure 30: Creating a Location for Acme Packet

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP server connected to it, which includes Communication Manager and Acme Packet 3820. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **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 Acme Packet 3820.

©2012 Avaya Inc. All Rights Reserved.

- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

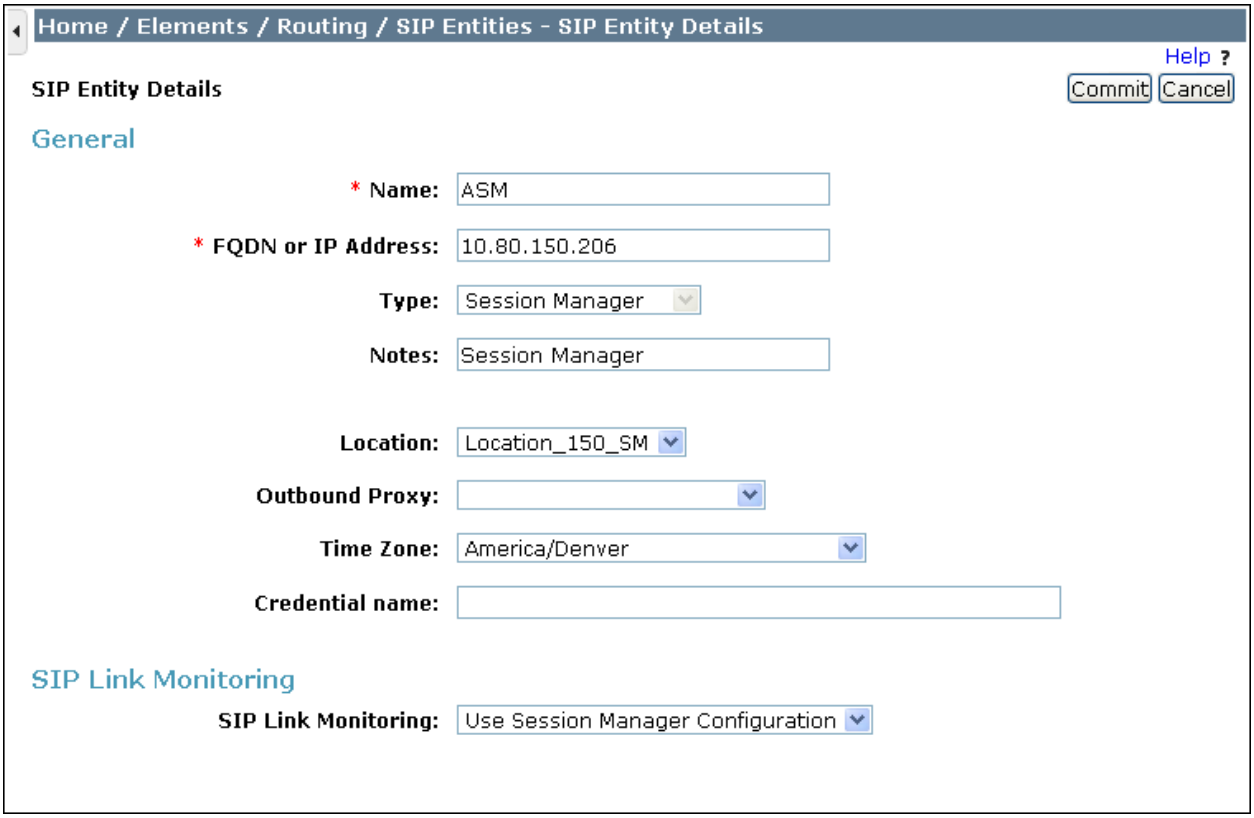

Figure 31: Creating a SIP Entity for Session Manager

©2012 Avaya Inc. All Rights Reserved.

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. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.5**.

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

- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

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

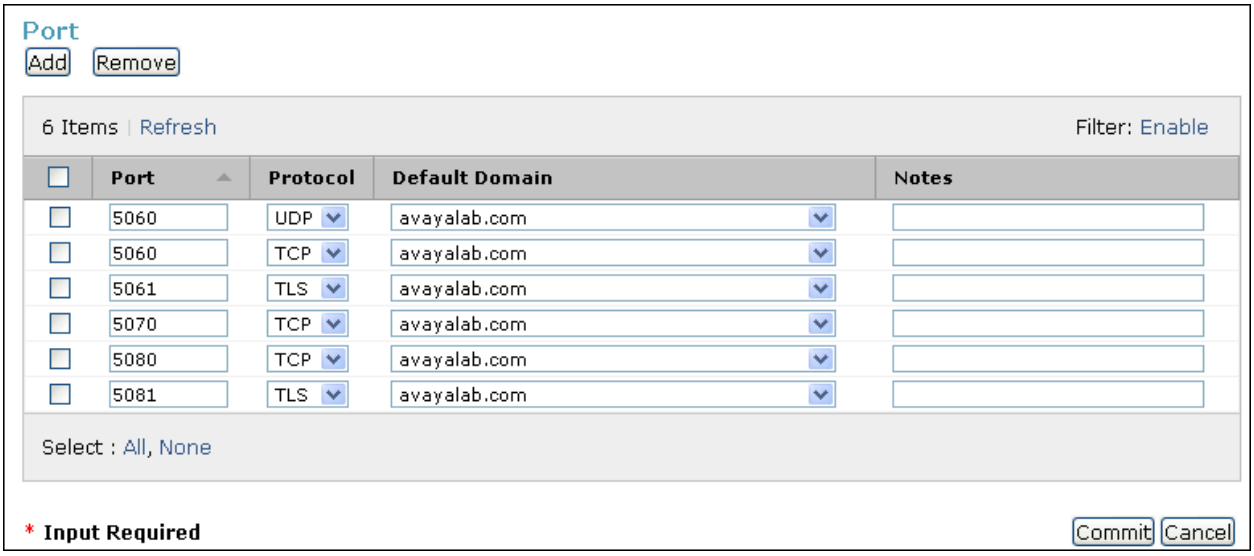

Figure 32: Session Manager Ports

©2012 Avaya Inc. All Rights Reserved.

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, a new SIP entity is created separate from 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 defined in **Section 5.3** of the procr interface on Communication Manager.

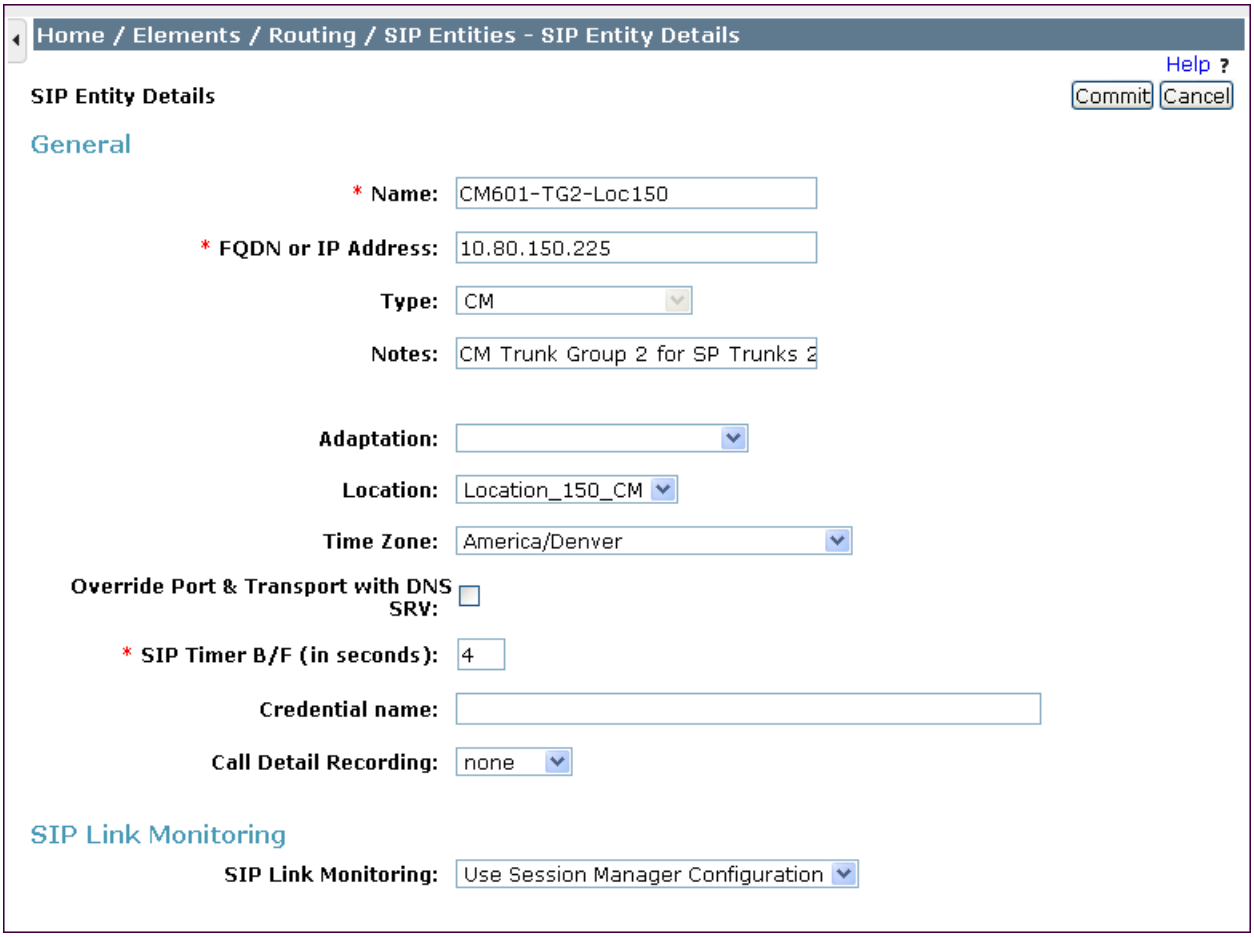

Figure 33: Creating a SIP Entity for Communication Manager Trunk Group 2

©2012 Avaya Inc. All Rights Reserved.

The following screen shows the addition of Acme Packet 3820 SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for Acme Packet 3820 in **Section 6.3**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.

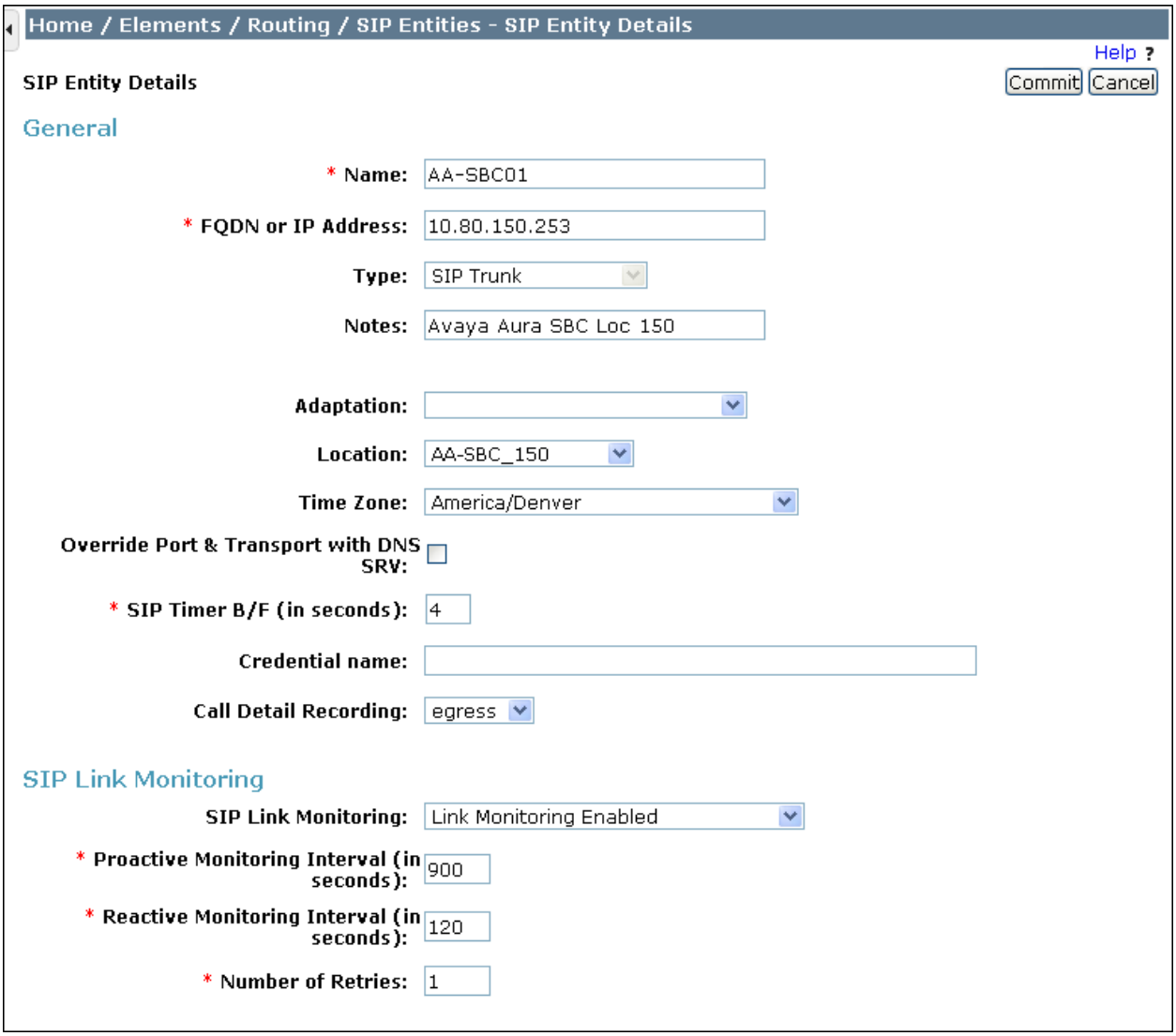

Figure 34: Creating a SIP Entity for Acme Packet

©2012 Avaya Inc. All Rights Reserved.

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and one to Acme Packet 3820. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for 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 Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **Trusted:** Check this box. **Note**: **If this box is not checked, calls from the associated SIP Entity specified in Section 6.4 will be denied**.

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and Acme Packet 3820.

Entity Link to Communication Manager:

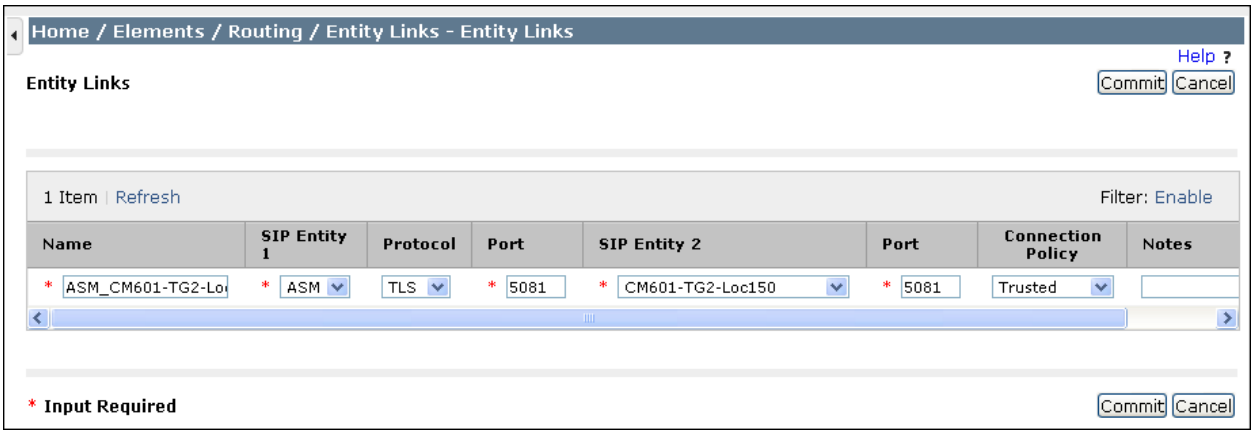

Figure 35: Creating an Entity Link for Communication Manager

©2012 Avaya Inc. All Rights Reserved.

Entity Link to Acme Packet 3820:

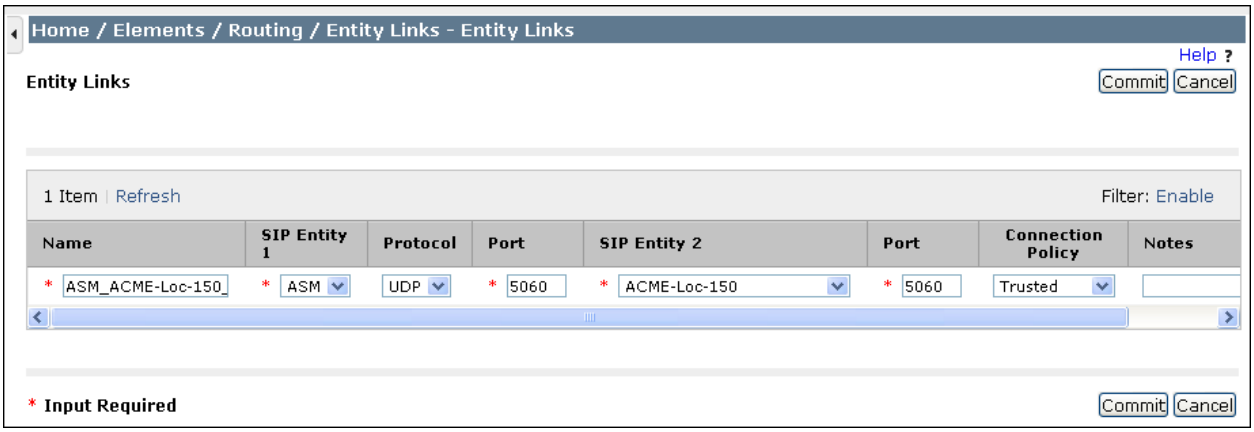

Figure 36: Creating an Entity Link for Acme Packet

©2012 Avaya Inc. All Rights Reserved.

6.6. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two routing policies must be added: one for Communication Manager and one for Acme Packet 3820. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

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

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

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select** (not shown)**.** 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 Acme Packet 3820.

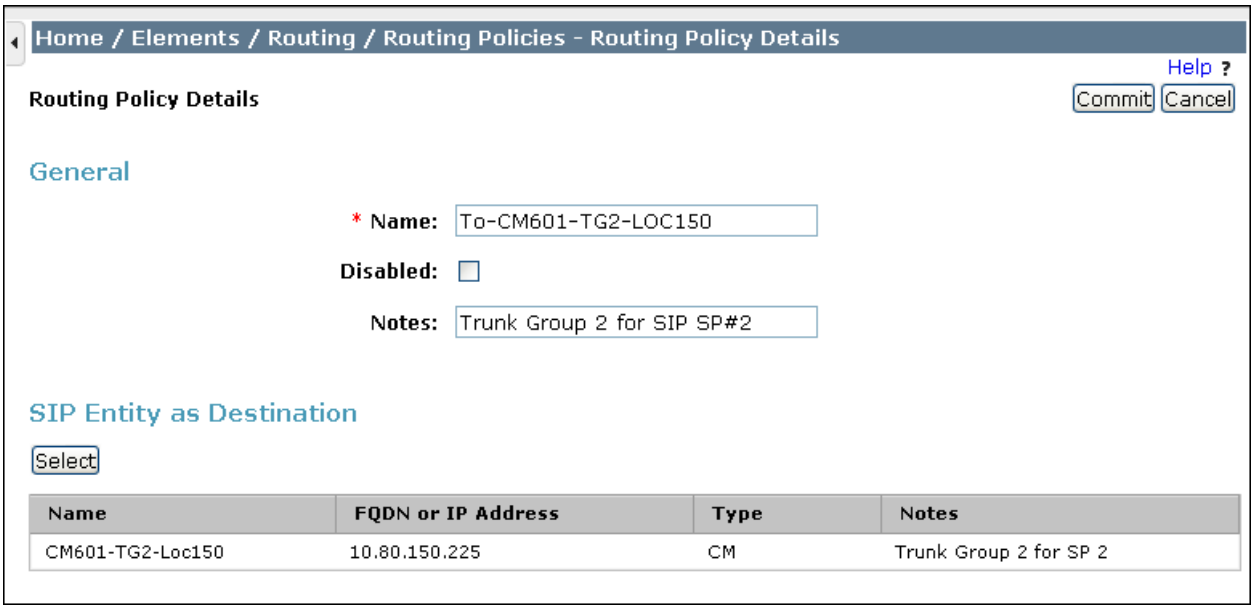

Figure 37: Routing Policy to Communication Manager Trunk Group 2

©2012 Avaya Inc. All Rights Reserved.

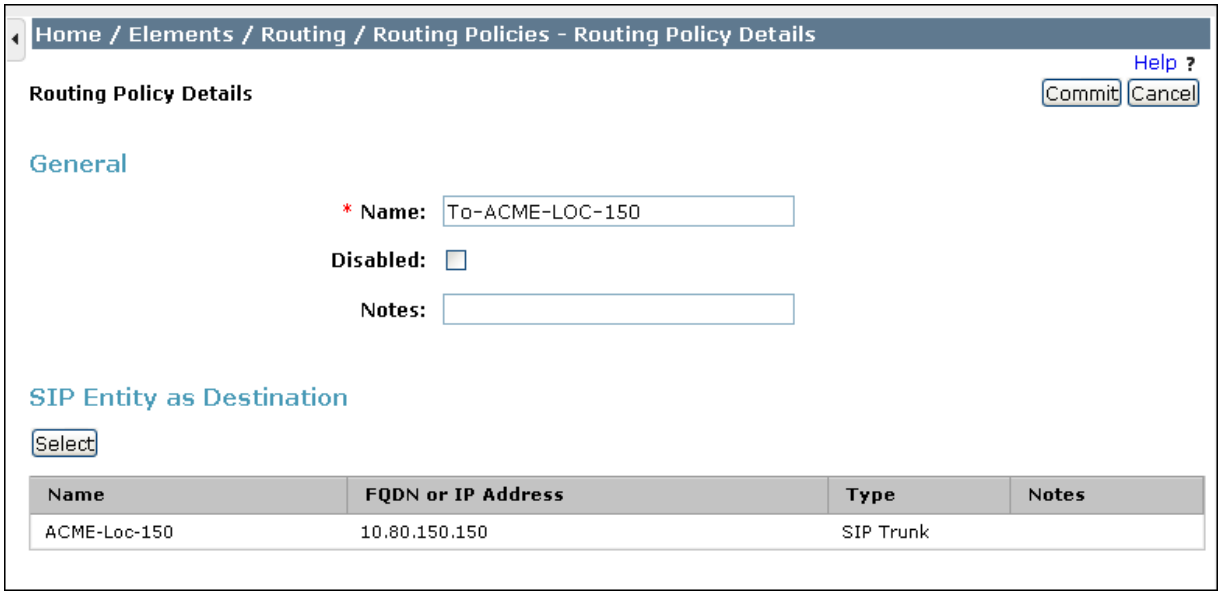

Figure 38: Routing Policy to Acme Packet

6.7. 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 CenturyLink 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 and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

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

©2012 Avaya Inc. All Rights Reserved.

Two examples of the dial patterns used for the compliance test are shown below. This Session Manager is shared between two test environments. The first example shows that **11** digit dialed numbers that begin with **1** originating from **Location_150_CM** uses route policy **To-AMCE-LOC-150**.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Help ?

Dial Pattern Details Commit Cancel

General

* **Pattern:** 1

* **Min:** 11

* **Max:** 11

Emergency Call: ☐

SIP Domain: -ALL-

Notes: 1+ OUTBOUND

Originating Locations and Routing Policies

Add Remove

2 Items | Refresh Filter: Enable

	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
☐	Location_140_CM	Subnet 140	To Sipera	0	☐	Sipera	
☐	Location_150_CM	Communication Manager	To-ACME-LOC-150	0	☐	ACME-Loc-150	

Select : All, None

Figure 39: Outbound Dial Pattern Example

©2012 Avaya Inc. All Rights Reserved.

The second example shows that a **10** digit number starting with **303555** to domain **avayalab.com** and originating from **Acme-LOC150** uses route policy **To-CM601-TG2-LOC150**. This will allow DID numbers assigned to the enterprise from CenturyLink to route to Communication Manager using trunk group 2. CenturyLink did not assign every number that starts with 30355 to the enterprise. So to properly route any number that is not a DID starting with 303555 dialed from Communication Manager, **Location_150_CM** was added to use route policy **To-ACME-LOC-150**.

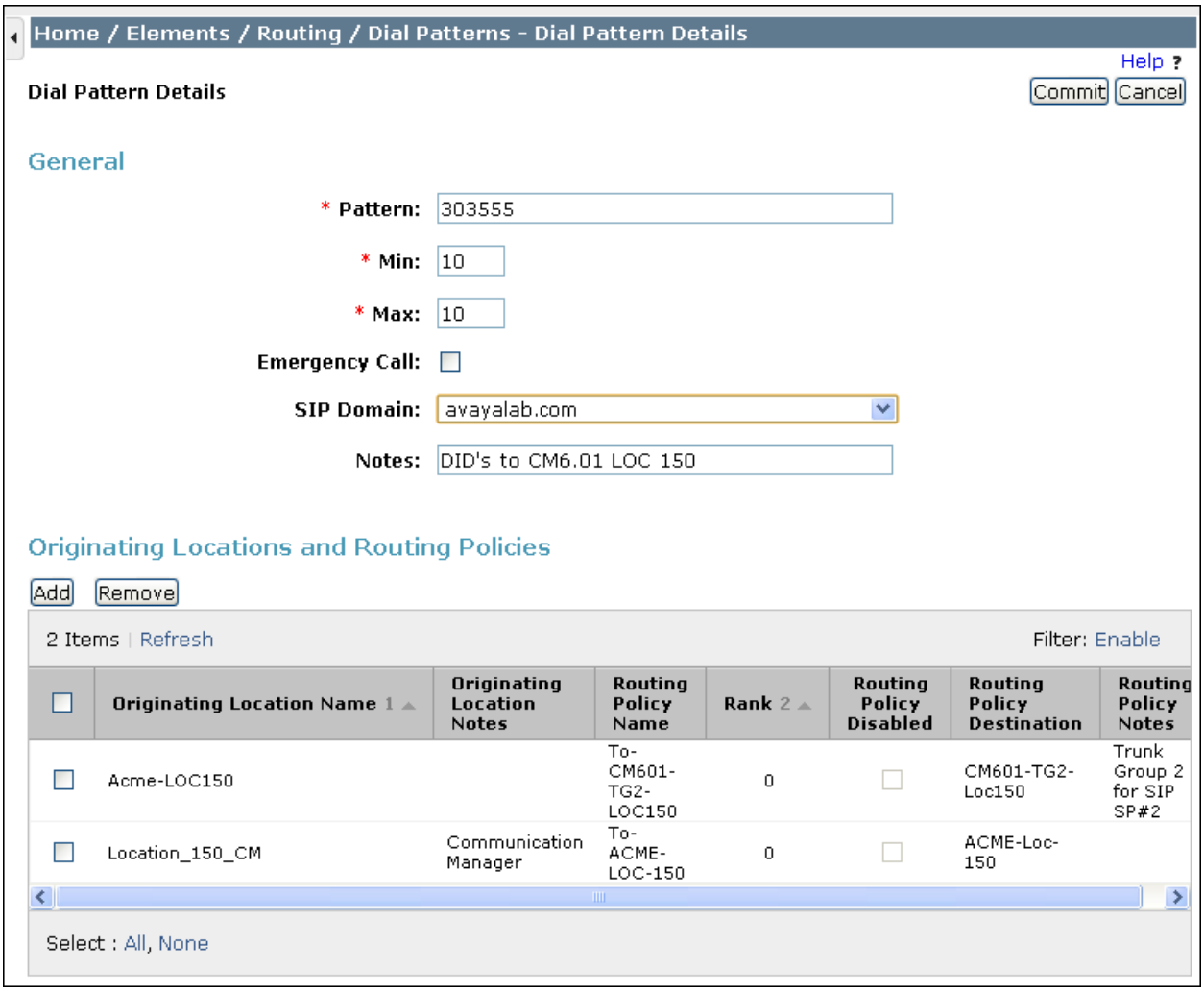

Figure 40: Inbound Dial Pattern Example

©2012 Avaya Inc. All Rights Reserved.

6.8. Verify Avaya Aura® Session Manager Instance

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

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.

Figure 41: Session Manager Administration

©2012 Avaya Inc. All Rights Reserved.

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.

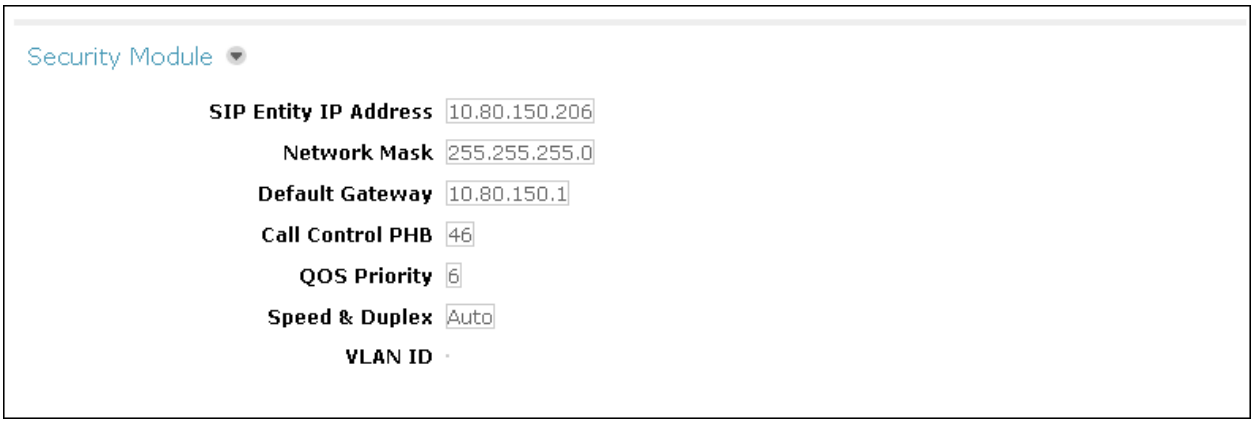

Figure 42: Session Manager Security Module

©2012 Avaya Inc. All Rights Reserved.

7. Configure Acme Packet 3820 Net-Net® Session Director

This section describes the configuration of the Acme Packet 3820 necessary for interoperability with CenturyLink and Session Manager. The Acme Packet 3820 is configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet 3820.

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**.

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 CenturyLink 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 [15].**

©2012 Avaya Inc. All Rights Reserved.

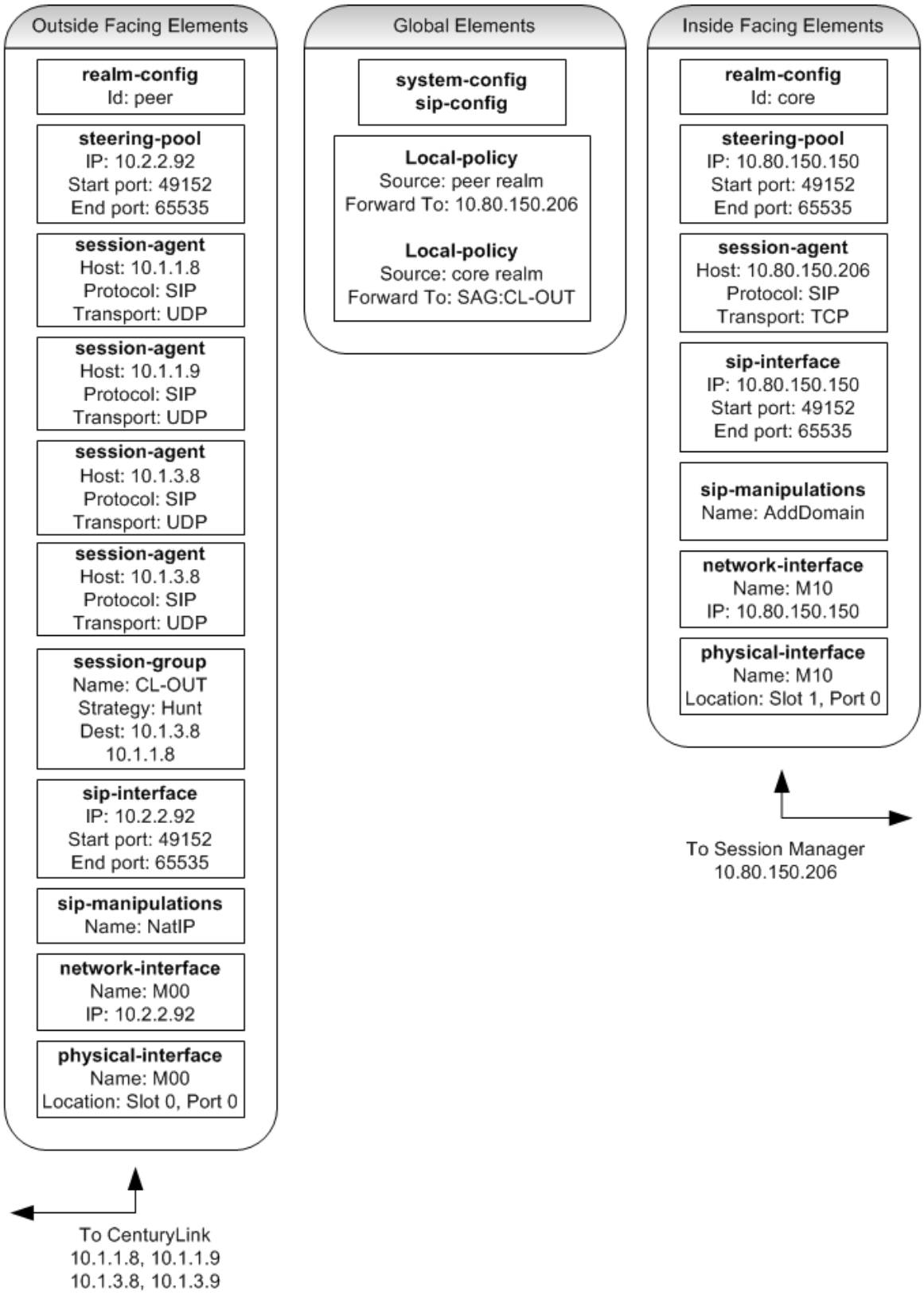

Figure 43: Pictorial View of Configuration

©2012 Avaya Inc. All Rights Reserved.

7.1. Acme Packet Command Line Interface Summary

The Acme Packet 3820 is configured using the Acme Packet Command Line Interface (ACLI). The following are the generic ACLI steps for configuring various elements.

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: 115200
    - 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 M00**).
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.

©2012 Avaya Inc. All Rights Reserved.

7.2. System Configuration

The system configuration defines system-wide parameters for the Acme Packet 3820.

The key system configuration (**system-config**) field is:

- **default-gateway**: The IP address of the default gateway for the management network (10.80.150.0/24) from **Figure 1**. In this case, the default gateway is **10.80.150.1**.

```
system-config
       hostname
       description
       location
       mib-system-contact
       mib-system-name

< text removed for brevity >

       call-trace                      disabled
       internal-trace                  disabled
       log-filter                      all
       default-gateway                 10.80.150.1
       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
```

Figure 44: System Config

©2012 Avaya Inc. All Rights Reserved.

7.3. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface slot 0 / port 0 of the Acme Packet 3820 was connected to the external untrusted network. Ethernet slot 1 / port 0 was connected to the internal corporate LAN. A network interface was defined for each physical interface to assign it a routable IP address.

The key physical interface (**phy-interface**) fields are:

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

```
phy-interface
       name                          M00
       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@console
       last-modified-date            2011-11-01 09:59:56
phy-interface
       name                          M10
       operation-type                Media
       port                          0
       slot                          1
       virtual-mac
       admin-state                   enabled
       auto-negotiation              enabled
       duplex-mode                   FULL
       speed                         100
       overload-protection           disabled
       last-modified-by              admin@console
       last-modified-date            2011-11-01 10:00:38
```

Figure 45: Physical Interface

©2012 Avaya Inc. All Rights Reserved.

The key network interface (**network-interface**) fields are:

- **name:** The name of the physical interface (defined previously) that is associated with this network interface.
- **description:** A descriptive name to help identify the interface.
- **ip-address:** The IP address on the interface connected to the network on which the CenturyLink SIP trunk service resides. In the compliance test, the IP address **10.2.2.92** was assigned to the public interface and **10.80.150.150** was assigned to the private interface.
- **netmask:** Subnet mask for the IP subnet.
- **gateway:** The subnet gateway address.
- **hip-ip-list:** The list of virtual IP addresses assigned to the Acme Packet 3820 on this interface. If a single virtual IP address is used, this value would be the same as the value entered for the **ip-address** field above.
- **icmp-address:** The list of IP addresses to which the Acme Packet 3820 will answer ICMP requests on this interface.

```
network-interface
       name                          M00
       sub-port-id                   0
       description                   PUBLIC
       hostname
       ip-address                    10.2.2.92
       pri-utility-addr
       sec-utility-addr
       netmask                       255.255.255.128
       gateway                       10.2.2.1
       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                   10.2.2.92
       ftp-address
       icmp-address
       snmp-address
       telnet-address
       ssh-address
       last-modified-by              admin@10.80.150.38
       last-modified-date            2011-11-01 12:52:08
```

Figure 46: Network Interface Public

©2012 Avaya Inc. All Rights Reserved.

The settings for the private side network interface are shown below.

```
network-interface
       name                          M10
       sub-port-id                   0
       description                   PRIVATE
       hostname
       ip-address                    10.80.150.150
       pri-utility-addr
       sec-utility-addr
       netmask                       255.255.255.0
       gateway                       10.80.150.1
       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                   10.80.150.150
       ftp-address
       icmp-address                  10.80.150.150
       snmp-address
       telnet-address
       ssh-address
       last-modified-by              admin@10.80.150.38
       last-modified-date            2011-11-01 12:16:22
```

Figure 47: Network Interface Private

7.4. Realm

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

The key realm (**realm-config**) fields are:

- **identifier:** A string used as a realm reference. This will be used in the configuration of other components.
- **network interfaces:** The network interfaces located in this realm.
- **out-manipulationid:** For the **peer** realm **NatIP** was used and for the **core** realm **AddDomain** was used. These names refer to a set of sip-manipulations (defined in **Section 7.9**) 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 (**peer**) of the Acme Packet 3820 as well as to outbound traffic from the private side (**core**) of the Acme Packet 3820.

©2012 Avaya Inc. All Rights Reserved.

```
realm-config
       identifier                      peer
       description
       addr-prefix                     0.0.0.0
       network-interfaces
                                       M00:0
       mm-in-realm                     enabled
       mm-in-network                   enabled
       mm-same-ip                      enabled
       mm-in-system                    enabled

< text removed for brevity >

       out-translationid
       in-manipulationid
       out-manipulationid              NatIP
       manipulation-string
       manipulation-pattern
       class-profile
       average-rate-limit              0

< text removed for brevity >

realm-config
       identifier                      core
       description
       addr-prefix                     0.0.0.0
       network-interfaces
                                       M10:0
       mm-in-realm                     enabled
       mm-in-network                   enabled
       mm-same-ip                      enabled
       mm-in-system                    enabled

< text removed for brevity >

       out-translationid
       in-manipulationid
       out-manipulationid              AddDomain
       manipulation-string
       manipulation-pattern
       class-profile
       average-rate-limit              0

< text removed for brevity >
```

Figure 48: Realm Configuration

©2012 Avaya Inc. All Rights Reserved.

7.5. SIP Configuration

The SIP configuration (**sip-config**) defines the global system-wide SIP parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

The key SIP configuration (**sip-config**) fields are:

- **state: enabled**
- **home-realm-id:** The name of the realm on the private side of the Acme Packet 3820.
- **egress-realm-id:** The name of the realm on the private side of the Acme Packet 3820.
- **options: max-udp=length=0**. This option was used to prevent errors about the packet size being too large.

```
sip-config
       state                          enabled
       operation-mode                 dialog
       dialog-transparency            enabled
       home-realm-id                  core
       egress-realm-id                core
       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

< text removed for brevity >

       options                        max-udp-length=0
       refer-src-routing              disabled
       add-ucid-header                disabled
       proxy-sub-events

< text removed for brevity >
```

Figure 49: SIP Configuration

©2012 Avaya Inc. All Rights Reserved.

7.6. SIP Interface

The SIP interface (**sip-interface**) defines the receiving characteristics of the SIP interfaces on the Acme Packet 3820. Two SIP interfaces were defined; one for each realm.

The key SIP interface (**sip-interface**) fields are:

- **realm-id:** The name of the realm to which this interface is assigned.
- **sipport**
  - **address:** The IP address assigned to this sip-interface.
  - **port:** The port assigned to this sip-interface. Port 5060 is used for both UDP and TCP.
  - **transport-protocol:** The transport method used for this interface.
  - **allow-anonymous:** Defines from whom SIP requests will be allowed. On the peer side, the value of **agents-only** is used. Thus, SIP requests will only be accepted from session agents (as defined in **Section 7.7**) on this interface. On the core side, the value of **all** is used. Thus, SIP requests will be accepted from anyone on this interface.

```
sip-interface
       state                          enabled
       realm-id                       peer
       description
       sip-port
              address                         10.2.2.92
              port                            5060
              transport-protocol              UDP
              tls-profile
              allow-anonymous                 agents-only
              ims-aka-profile
       carriers
       trans-expire                   0
       invite-expire                  0

< text removed for brevity >

sip-interface
       state                          enabled
       realm-id                       core
       description
       sip-port
              address                         10.80.150.150
              port                            5060
              transport-protocol              UDP
              tls-profile
              allow-anonymous                 all
              ims-aka-profile
       carriers
       trans-expire                   0
       invite-expire                  0

< text removed for brevity >
```

Figure 50: SIP Interface

©2012 Avaya Inc. All Rights Reserved.

7.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet 3820 such as Session Manager and CenturyLink SIP Trunk service.

The key session agent (**session-agent**) fields are:

- **hostname:** Fully qualified domain name or IP address of this SIP peer.
- **ip-address**: The IP address of this SIP peer.
- **port:** The port used by the peer for SIP traffic.
- **app-protocol: SIP**
- **transport-method:** UDP
- **realm-id:** The realm id where this peer resides.
- **description:** A descriptive name for the peer.
- **ping-method**: **OPTIONS;hops=70** This setting defines that the SIP OPTIONS message will be sent to the peer to verify that the SIP connection is functional. In addition, this parameter causes the Acme Packet 3820 to set the SIP "Max-Forward" field to 70 in outbound SIP OPTIONS pings generated by the Acme Packet 3820 to this session agent.
- **ping-interval:** Specifies the interval (in seconds) between each ping attempt.

The settings for the session agent used for CenturyLink East Inbound/Outbound peer:

```
session-agent
       hostname                        10.1.1.8
       ip-address                      10.1.1.8
       port                            5060
       state                           enabled
       app-protocol                    SIP
       app-type
       transport-method                UDP
       realm-id                        peer
       egress-realm-id
       description
       carriers
       allow-next-hop-lp               enabled
       constraints                     disabled
       max-sessions                    0

< text removed for brevity >

       response-map
       ping-method                     OPTIONS;hops=70
       ping-interval                   60

< text removed for brevity >
```

Figure 51: Session Agent for CenturyLink East

©2012 Avaya Inc. All Rights Reserved.

The settings for the session agent used for CenturyLink East Remote DID peer:

```
session-agent
       hostname                        10.1.1.9
       ip-address                      10.1.1.9
       port                            5060
       state                           enabled
       app-protocol                    SIP
       app-type
       transport-method                UDP
       realm-id                        peer
       egress-realm-id
       description
       carriers
       allow-next-hop-lp               enabled
       constraints                     disabled
       max-sessions                    0

< text removed for brevity >

       response-map
       ping-method                     OPTIONS;hops=70
       ping-interval                   60

< text removed for brevity >
```

Figure 52: Session Agent for CenturyLink East Remote DID

The settings for the session agent used for CenturyLink West Inbound/Outbound peer:

```
session-agent
       hostname                        10.1.3.8
       ip-address                      10.1.3.8
       port                            5060
       state                           enabled
       app-protocol                    SIP
       app-type
       transport-method                UDP
       realm-id                        peer
       egress-realm-id
       description
       carriers
       allow-next-hop-lp               enabled
       constraints                     disabled
       max-sessions                    0

< text removed for brevity >

       response-map
       ping-method                     OPTIONS;hops=70
       ping-interval                   60

< text removed for brevity >
```

Figure 53: Session Agent for CenturyLink West

©2012 Avaya Inc. All Rights Reserved.

The settings for the session agent used for CenturyLink West Remote DID peer:

```
session-agent
       hostname                        10.1.3.9
       ip-address                      10.1.3.9
       port                            5060
       state                           enabled
       app-protocol                    SIP
       app-type
       transport-method                UDP
       realm-id                        peer
       egress-realm-id
       description
       carriers
       allow-next-hop-lp               enabled
       constraints                     disabled
       max-sessions                    0

< text removed for brevity >

       response-map
       ping-method                     OPTIONS;hops=70
       ping-interval                   60

< text removed for brevity >
```

Figure 54: Session Agent for CenturyLink West Remote DID

The settings for the session agent used for Session Manager:

```
session-agent
       hostname                        10.80.150.206
       ip-address                      10.80.150.206
       port                            5060
       state                           enabled
       app-protocol                    SIP
       app-type
       transport-method                UDP
       realm-id                        core
       egress-realm-id
       description
       carriers
       allow-next-hop-lp               enabled
       constraints                     disabled
       max-sessions                    0

< text removed for brevity >

       response-map
       ping-method                     OPTIONS;hops=70
       ping-interval                   60

< text removed for brevity >
```

Figure 55: Session Agent for Session Manager

©2012 Avaya Inc. All Rights Reserved.

7.8. 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 CenturyLink had four session agents assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound traffic. Only the two session agents allocated for outbound traffic were added to the SAG.

The key session agent group (**session-group**) fields are:

- **group-name:** A descriptive string used to reference the session agent group.
- **state**: **enabled**
- **app-protocol: SIP**
- **strategy: Hunt** This strategy will route to the secondary session agent only if the primary fails. An alternative is to use a strategy of **RoundRobin.** This strategy will alternatively select between session agents.
- **dest:** The list of session agents to be added to the group. For compliance testing **10.1.3.8** and **10.1.1.8** were used.
- **sag-recursion: enabled** This allows Acme Packet 3820 to select a different session agent in the SAG if a failure occurs to the first session agent.

```
session-group
       group-name                      CL-OUT
       description
       state                           enabled
       app-protocol                    SIP
       strategy                        Hunt
       dest
                                       10.1.1.8
                                       10.1.3.8
       trunk-group
       sag-recursion                   enabled
       stop-sag-recurse                401,407
       last-modified-by                admin@10.80.150.38
       last-modified-date              2011-11-04 13:35:59
```

Figure 56: Session Agent Group

©2012 Avaya Inc. All Rights Reserved.

7.9. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 7.4**, it was defined that the set of sip-manipulations named **NatIP** would be performed on outbound traffic in the **peer** realm and **AddDomain** would be performed on outbound traffic in **core** 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.

©2012 Avaya Inc. All Rights Reserved.

The example below shows the **natFROM header-rule** in the **NatIP** sip manipulation. It specifies that the "From" 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.

```
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

< text removed for brevity >
```

Figure 57: SIP Manipulation NatIP

©2012 Avaya Inc. All Rights Reserved.

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 5.7**).

```
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

< text removed for brevity >
```

Figure 58: SIP Manipulation AddDomain

For the complete configuration of these rules refer to **Appendix A**.

©2012 Avaya Inc. All Rights Reserved.

7.10. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools were defined; one for each realm.

The key steering pool (**steering-pool**) fields are:

- **ip-address**: The address of the interface on the Acme Packet 3820.
- **start-port**: An even number of the port that begins the range.
- **end-port**: An odd number of the port that ends the range.
- **realm-id**: The realm to which this steering pool is assigned

```
steering-pool
       ip-address                      10.2.2.92
       start-port                      49152
       end-port                        65535
       realm-id                        peer
       network-interface
       last-modified-by                admin@console
       last-modified-date              2011-11-01 10:36:17
steering-pool
       ip-address                      10.80.150.150
       start-port                      49152
       end-port                        65535
       realm-id                        core
       network-interface
       last-modified-by                admin@console
       last-modified-date              2011-11-01 10:36:39
```

Figure 59: Steering Pool

7.11. Local Policy

Local policy controls the routing of SIP calls from one realm to another.

The key local policy (**local-policy**) fields are:

- **from-address:** A policy filter indicating the originating IP address to which this policy applies. An asterisk (*) indicates any IP address.
- **to-address:** A policy filter indicating the terminating IP address to which this policy applies. An asterisk (*) indicates any IP address.
- **source-realm:** A policy filter indicating the matching realm in order for the policy rules to be applied.
- **policy-attribute:**
    - **next-hop:** The IP address where the message should be sent when the policy rules match.
    - **realm:** The realm associated with the next-hop IP address.

©2012 Avaya Inc. All Rights Reserved.

In this case, the first policy provides a simple routing rule indicating that messages originating from the **peer** realm are to be sent to the **core** realm via IP address **10.80.150.206** (Session Manager at the enterprise). The second policy indicates that messages originating from the **core** realm are to be sent to the **peer** realm via the session agent group **CL-OUT** created in **Section 7.8**.

```
local-policy
       from-address
                                        *
       to-address
                                        *
       source-realm
                                        peer
       description
       activate-time                    N/A

< text removed for brevity >

       policy-attribute
              next-hop                          10.80.150.206
              realm                             core
              action                            none

< text removed for brevity >

local-policy
       from-address
                                        *
       to-address
                                        *
       source-realm
                                        core
       description
       activate-time                    N/A

< text removed for brevity >

       policy-attribute
              next-hop                          SAG:CL-OUT
              realm                             peer

< text removed for brevity >
```

Figure 60: Local Policy

©2012 Avaya Inc. All Rights Reserved.

8. CenturyLink SIP Trunk Service Configuration

To use CenturyLink SIP Trunk Service, a customer must request the service from CenturyLink using their sales processes. This process can be initiated by contacting CenturyLink via the corporate web site at www.centurylink.com and requesting information via the online sales links or telephone numbers

9. Verification and Troubleshooting

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.

9.1. Verification

The following steps may be used to verify the configuration:

1. Verify the call routing administration on Session Manager by logging in to System Manager and executing the Call Routing Test. Expand **Elements → Session Manager → System Tools → Call Routing Test**. Populate the field for the call parameters of interest. For example, the following screen shows a call routing test for an outbound call to PSTN via CenturyLink. Under **Routing Decisions**, observe the call will rout via Acme Packet 3820 to CenturyLink. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

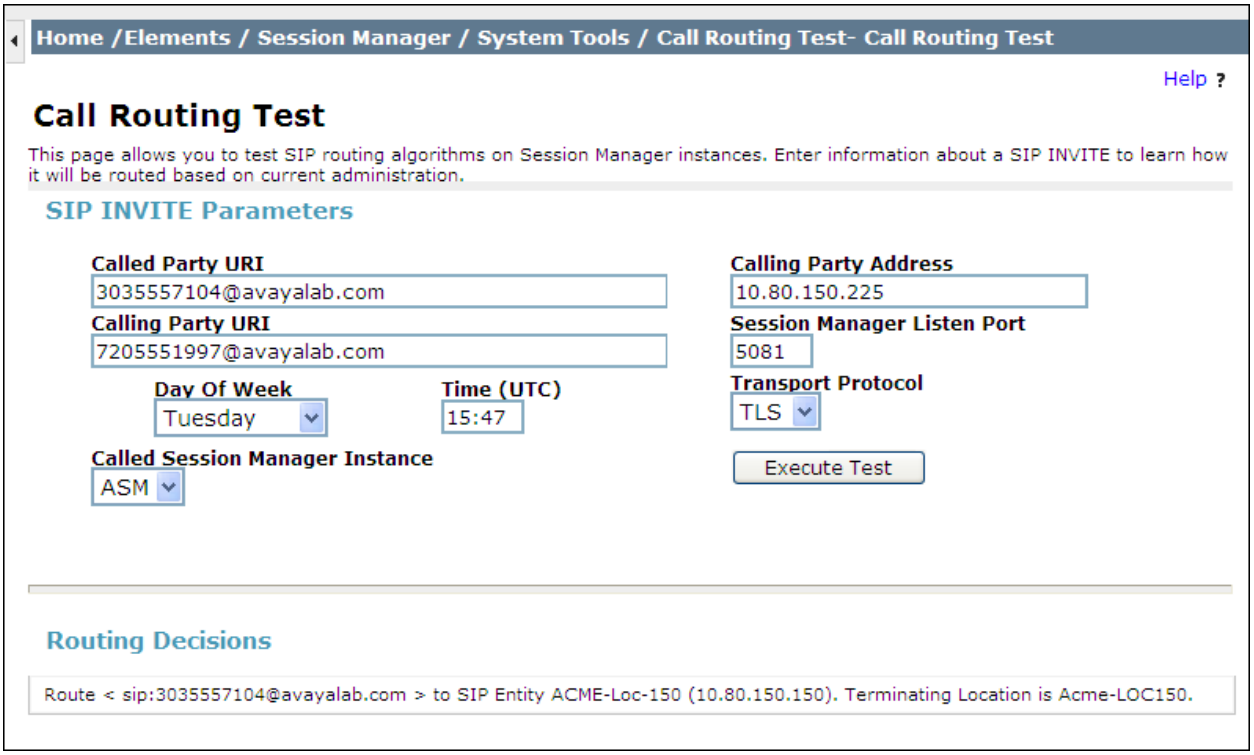

Figure 61: Call Routing Test

©2012 Avaya Inc. All Rights Reserved.

2. 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.
3. 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.
4. Verify that the user on the PSTN can end an active call by hanging up.
5. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Use the SAT interface on Communication Manager to verify status of SIP trunks. Specifically use the **status trunk n** command to verify the active call has ended. Where **n** is the trunk group number used for CenturyLink SIP Trunk Service defined in **Section 5.8**.

Below is an example of an active call.

```
status trunk 2

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/active  no   S00000
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

Figure 62: Status Trunk 2 - Active

Verify the port returns to **in-service/idle** after the call has ended.

```
status trunk 2

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
```

Figure 63: Status Trunk 2 - Idle

©2012 Avaya Inc. All Rights Reserved.

9.2. Troubleshooting

1. Communication Manager:
    - **list trace station** <extension number> - Traces calls to and from a specific station.
    - **list trace tac** <trunk access code number> - Trace 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.

2. Session Manager: **traceSM -x –uni** – Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Acme Packet 3820 Net-Net Session Director, Avaya Aura® Session Manager, and Avaya Aura® Communication Manager Evolution Server to the CenturyLink SIP Trunk (Legacy Qwest) Service. The CenturyLink SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The CenturyLink SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

©2012 Avaya Inc. All Rights Reserved.

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com. Acme Packet product documentation is available at http://www.acmepacket.com. A support account may be required to access the Acme Packet documentation.

[1] *Installing and Configuring Avaya Aura® System Platform, Release 6.0.3, February 2011.*

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

[3] *Administering Avaya Aura® Communication Manager,* June2010, Document Number 03-300509.

[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* June 2010, Document Number 555-245-205.

[5] *Installing and Upgrading Avaya Aura® System Manager 6.1 GA Version,* November 2010.

[6] *Installing and Configuring Avaya Aura® Session Manager,* April 2011, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager,* November 2010, Document Number 03-603324.

[8] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x,* April 2010, Document Number 16-601443.

[9] *4600 Series IP Telephone LAN Administrator Guide,* July 2008, Document Number 555-233-507.

[10] *Avaya one-X Deskphone H.323 Administrator Guide,* May 2011, Document Number 16-300698.

[11] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1,* December 2010, Document Number 16-603838

[12] *Administering Avaya one-X Communicator,* July 2011

[13] *Administrator Guide for Avaya Communication Manager,* February 2007, Issue 3, Document Number 03-300509.

[14] *Feature Description and Implementation for Avaya Communication Manager,* Issue 5, Document Number 555-245-205

[15] *Acme Packet, "Net-Net 4000 S-C6.2.0 ACLI Configuration Guide",* 400-0061-62, Nov 2009

[16] *Acme Packet, "Net-Net 3800 Series And Net-Net 4500 SSM2 Installation Guide",* 400-0114-20, Apr 2010

[17] *Acme Packet, "Net-Net 3820 Hardware Installation Guide",* 400-0134-10, Mar 2011

©2012 Avaya Inc. All Rights Reserved.

Appendix A: Acme Packet 3820 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** at the Acme Packet 3820

```
acmesystem# show running-config
local-policy
      from-address
                                    *
      to-address
                                    *
      source-realm
                                    peer
      description
      activate-time                 N/A
      deactivate-time               N/A
      state                         enabled
      policy-priority               none
      last-modified-by              admin@10.80.150.38
      last-modified-date            2011-11-04 13:08:27
      policy-attribute
            next-hop                      10.80.150.206
            realm                         core
            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
                                    core
      description
      activate-time                 N/A
      deactivate-time               N/A
      state                         enabled
      policy-priority               none
      last-modified-by              admin@10.80.150.38
      last-modified-date            2011-11-03 17:39:11
      policy-attribute
```


©2012 Avaya Inc. All Rights Reserved.

```
            next-hop                        SAG:CL-OUT
            realm                           peer
            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
      syslog-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
```


©2012 Avaya Inc. All Rights Reserved.

```
      last-modified-by                admin@10.80.150.38
      last-modified-date              2011-11-01 12:25:41
network-interface
      name                            M00
      sub-port-id                     0
      description                     PUBLIC
      hostname
      ip-address                      10.2.2.92
      pri-utility-addr
      sec-utility-addr
      netmask                         255.255.255.128
      gateway                         10.2.2.1
      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                     10.2.2.92
      ftp-address
       icmp-address
      snmp-address
      telnet-address
      ssh-address
      last-modified-by                admin@10.80.150.38
      last-modified-date              2011-11-01 12:52:08
network-interface
      name                            M10
      sub-port-id                     0
      description                     PRIVATE
      hostname
      ip-address                      10.80.150.150
      pri-utility-addr
      sec-utility-addr
      netmask                         255.255.255.0
      gateway                         10.80.150.1
      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                     10.80.150.150
      ftp-address
```


©2012 Avaya Inc. All Rights Reserved.

```
            icmp-address                    10.80.150.150
      snmp-address
      telnet-address
      ssh-address
      last-modified-by                  admin@10.80.150.38
      last-modified-date                2011-11-01 12:16:22
phy-interface
      name                              M00
      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@console
      last-modified-date                2011-11-01 09:59:56
phy-interface
      name                              M10
      operation-type                    Media
      port                              0
      slot                              1
      virtual-mac
      admin-state                       enabled
      auto-negotiation                  enabled
      duplex-mode                       FULL
      speed                             100
      overload-protection               disabled
      last-modified-by                  admin@console
      last-modified-date                2011-11-01 10:00:38
realm-config
      identifier                        peer
      description
      addr-prefix                       0.0.0.0
      network-interfaces
                                        M00:0
      mm-in-realm                       enabled
      mm-in-network                     enabled
      mm-same-ip                        enabled
      mm-in-system                      enabled
      bw-cac-non-mm                     disabled
      msm-release                       disabled
      qos-enable                        disabled
      generate-UDP-checksum             disabled
      max-bandwidth                     0
      fallback-bandwidth                0
      max-priority-bandwidth            0
      max-latency                       0
      max-jitter                        0
      max-packet-loss                   0
      observ-window-size                0
      parent-realm
      dns-realm
      media-policy
```


©2012 Avaya Inc. All Rights Reserved.

```
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
cac-failure-threshold           0
untrust-cac-failure-threshold   0
ext-policy-svr
symmetric-latching              disabled
pai-strip                       disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching             none
restriction-mask                32
accounting-enable               enabled
user-cac-mode                   none
user-cac-bandwidth              0
user-cac-sessions               0
icmp-detect-multiplier          0
icmp-advertisement-interval     0
icmp-target-ip
monthly-minutes                 0
net-management-control          disabled
delay-media-update              disabled
refer-call-transfer             disabled
dyn-refer-term                  disabled
codec-policy
codec-manip-in-realm            disabled
constraint-name
call-recording-server-id
xnq-state                       xnq-unknown
hairpin-id                      0
stun-enable                     disabled
stun-server-ip                  0.0.0.0
stun-server-port                3478
stun-changed-ip                 0.0.0.0
stun-changed-port               3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp                      disabled
hide-egress-media-update        disabled
last-modified-by                admin@10.80.150.38
```


©2012 Avaya Inc. All Rights Reserved.

```
      last-modified-date             2011-11-01 13:03:09
realm-config
      identifier                     core
      description
      addr-prefix                    0.0.0.0
      network-interfaces
                                     M10:0
      mm-in-realm                    enabled
      mm-in-network                  enabled
      mm-same-ip                     enabled
      mm-in-system                   enabled
      bw-cac-non-mm                  disabled
      msm-release                    disabled
      qos-enable                     disabled
      generate-UDP-checksum          disabled
      max-bandwidth                  0
      fallback-bandwidth             0
      max-priority-bandwidth         0
      max-latency                    0
      max-jitter                     0
      max-packet-loss                0
      observ-window-size             0
      parent-realm
      dns-realm
      media-policy
      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
      cac-failure-threshold          0
      untrust-cac-failure-threshold  0
      ext-policy-svr
      symmetric-latching             disabled
      pai-strip                      disabled
      trunk-context
      early-media-allow
      enforcement-profile
      additional-prefixes
      restricted-latching            none
      restriction-mask               32
      accounting-enable              enabled
      user-cac-mode                  none
      user-cac-bandwidth             0
      user-cac-sessions              0
      icmp-detect-multiplier         0
```


©2012 Avaya Inc. All Rights Reserved.

```
      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@10.80.150.38
      last-modified-date             2011-11-03 15:52:37
session-agent
      hostname                       10.80.150.206
      ip-address                     10.80.150.206
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       core
      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
```


©2012 Avaya Inc. All Rights Reserved.

```
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action                Proxy
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method                    OPTIONS;hops=70
      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                       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@10.80.150.38
      last-modified-date             2011-11-03 15:51:54
session-agent
      hostname                       10.1.1.8
      ip-address                     10.1.1.8
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       peer
      egress-realm-id
      description
```


©2012 Avaya Inc. All Rights Reserved.

```
carriers
allow-next-hop-lp              enabled
constraints                    disabled
max-sessions                   0
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method                    OPTIONS;hops=70
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                       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
```


©2012 Avaya Inc. All Rights Reserved.

```
      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@10.80.150.38
      last-modified-date             2011-11-01 12:39:40
session-agent
      hostname                       10.1.1.9
      ip-address                     10.1.1.9
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       peer
      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;hops=70
      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                       disabled
      request-uri-headers
      stop-recurse
```


©2012 Avaya Inc. All Rights Reserved.

```
      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@10.80.150.38
      last-modified-date              2011-11-01 12:39:46
session-agent
      hostname                        10.1.3.8
      ip-address                      10.1.3.8
      port                            5060
      state                           enabled
      app-protocol                    SIP
      app-type
      transport-method                UDP
      realm-id                        peer
      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
```


©2012 Avaya Inc. All Rights Reserved.

```
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method                    OPTIONS;hops=70
      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                       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@10.80.150.38
      last-modified-date             2011-11-04 13:30:48
session-agent
      hostname                       10.1.3.9
      ip-address                     10.1.3.9
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               UDP
      realm-id                       peer
      egress-realm-id
```


©2012 Avaya Inc. All Rights Reserved.

```
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;hops=70
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                       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
```


©2012 Avaya Inc. All Rights Reserved.

```
      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@10.80.150.38
      last-modified-date             2011-11-03 17:09:25
session-group
      group-name                     CL-OUT
      description
      state                          enabled
      app-protocol                   SIP
      strategy                       Hunt
      dest
                                     10.1.1.8
                                     10.1.3.8
      trunk-group
      sag-recursion                  enabled
      stop-sag-recurse               401,407
      last-modified-by               admin@10.80.150.38
      last-modified-date             2011-11-21 12:39:05
sip-config
      state                          enabled
      operation-mode                 dialog
      dialog-transparency            enabled
      home-realm-id                  core
      egress-realm-id                core
      nat-mode                       None
      registrar-domain
      registrar-host
      registrar-port                 0
      register-service-route         always
      init-timer                     500
      max-timer                      4000
      trans-expire                   32
      invite-expire                  180
      inactive-dynamic-conn          32
      enforcement-profile
      pac-method
      pac-interval                   10
      pac-strategy                   PropDist
      pac-load-weight                1
      pac-session-weight             1
      pac-route-weight               1
      pac-callid-lifetime            600
      pac-user-lifetime              3600
      red-sip-port                   1988
      red-max-trans                  10000
      red-sync-start-time            5000
      red-sync-comp-time             1000
      add-reason-header              disabled
      sip-message-len                4096
      enum-sag-match                 disabled
      extra-method-stats             disabled
```


©2012 Avaya Inc. All Rights Reserved.

```
      registration-cache-limit       0
      register-use-to-for-lp         disabled
      options                        max-udp-length=0
      refer-src-routing              disabled
      add-ucid-header                disabled
      proxy-sub-events
      pass-gruu-contact              disabled
      sag-lookup-on-redirect         disabled
      last-modified-by               admin@10.80.150.38
      last-modified-date             2011-11-21 17:43:22
sip-interface
      state                          enabled
      realm-id                       peer
      description
      sip-port
            address                        10.2.2.92
            port                           5060
            transport-protocol             UDP
            tls-profile
            allow-anonymous                agent-only
            ims-aka-profile
      carriers
      trans-expire                   0
      invite-expire                  0
      max-redirect-contacts          0
      proxy-mode
      redirect-action
      contact-mode                   none
      nat-traversal                  none
      nat-interval                   30
      tcp-nat-interval               90
      registration-caching           disabled
      min-reg-expire                 300
      registration-interval          3600
      route-to-registrar             disabled
      secured-network                disabled
      teluri-scheme                  disabled
      uri-fqdn-domain
      trust-mode                     all
      max-nat-interval               3600
      nat-int-increment              10
      nat-test-increment             30
      sip-dynamic-hnt                disabled
      stop-recurse                   401,407
      port-map-start                 0
      port-map-end                   0
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      sip-ims-feature                disabled
      operator-identifier
      anonymous-priority             none
      max-incoming-conns             0
      per-src-ip-max-incoming-conns  0
      inactive-conn-timeout          0
```


©2012 Avaya Inc. All Rights Reserved.

```
      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@console
      last-modified-date             2011-11-01 10:44:02
sip-interface
      state                          enabled
      realm-id                       core
      description
      sip-port
            address                        10.80.150.150
            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
```


©2012 Avaya Inc. All Rights Reserved.

```
      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@console
      last-modified-date             2011-11-01 10:44:54
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
```


©2012 Avaya Inc. All Rights Reserved.

```
            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                          removePLoc
      header-name                   P-Location
      action                        delete
      comparison-type               case-sensitive
      msg-type                      any
      methods
      match-value
      new-value
header-rule
      name                          remoteAlrtInfo
      header-name                   Alert-Info
      action                        delete
```


©2012 Avaya Inc. All Rights Reserved.

```
            comparison-type                 case-sensitive
            msg-type                        any
            methods
            match-value
            new-value
      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                            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                       $LOCAL_IP

      last-modified-by                  admin@10.80.150.38
      last-modified-date                2011-11-10 17:38:33
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
```


©2012 Avaya Inc. All Rights Reserved.

```
            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
      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
      last-modified-by              admin@10.80.150.38
      last-modified-date            2011-11-01 17:59:35
steering-pool
      ip-address                    10.2.2.92
      start-port                    49152
      end-port                      65535
      realm-id                      peer
      network-interface
      last-modified-by              admin@console
```


©2012 Avaya Inc. All Rights Reserved.

```
      last-modified-date             2011-11-01 10:36:17
steering-pool
      ip-address                     10.80.150.150
      start-port                     49152
      end-port                       65535
      realm-id                       core
      network-interface
      last-modified-by               admin@console
      last-modified-date             2011-11-01 10:36:39
system-config
      hostname
      description
      location
      mib-system-contact
      mib-system-name
      mib-system-location
      snmp-enabled                   enabled
      enable-snmp-auth-traps         disabled
      enable-snmp-syslog-notify      disabled
      enable-snmp-monitor-traps      disabled
      enable-env-monitor-traps       disabled
      snmp-syslog-his-table-length   1
      snmp-syslog-level              WARNING
      system-log-level               WARNING
      process-log-level              NOTICE
      process-log-ip-address         0.0.0.0
      process-log-port               0
      collect
            sample-interval                5
            push-interval                  15
            boot-state                     disabled
            start-time                     now
            end-time                       never
            red-collect-state              disabled
            red-max-trans                  1000
            red-sync-start-time            5000
            red-sync-comp-time             1000
            push-success-trap-state        disabled
      call-trace                     disabled
      internal-trace                 disabled
      log-filter                     all
      default-gateway                10.80.150.1
      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
```


©2012 Avaya Inc. All Rights Reserved.

```
      cleanup-time-of-day            00:00
      last-modified-by               admin@console
      last-modified-date             2011-11-01 10:30:52
task done
acmesystem#
```


©2012 Avaya Inc. All Rights Reserved.

©2012 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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