Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Acme Packet Net-Net 6.4.0 with Voxox SIP Trunk Service – Issue 1.0

Abstract

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.3, Avaya Aura® Communication Manager Release 6.3, and the Acme Packet Net-Net 6.4.0 with the Voxox SIP Trunk service.

The Voxox service offer referenced within these Application Notes is designed for business customers with an Avaya SIP trunk solution. The service provides local and/or long distance PSTN calling via standards-based SIP trunks directly, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

Voxox is a member of the DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

©2013 Avaya Inc. All Rights Reserved.

Table of Contents

©2013 Avaya Inc. All Rights Reserved.

©2013 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Aura® Session Manager Release 6.3, Avaya Aura® Communication Manager Release 6.3, and Acme Packet Net-Net 3800[1] with the Voxox SIP Trunk service. The Voxox SIP Trunk Service provides local and/or long-distance calls (with PSTN endpoints) via standards-based SIP trunks.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Voxox SIP Trunk Service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and Acme Packet Session Border Controller (SBC).

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

2.1. Interoperability Compliance Testing

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- Response to SIP OPTIONS queries
- Incoming PSTN calls to various phone types including Avaya H.323 and SIP telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323 and SIP telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator can place calls from the local computer or control a remote phone. Both of these modes were tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Each protocol version of Avaya one-X® Communicator was also tested.
- Various call types including: local, long distance, international, outbound toll-free,
- Local directory assistance (411)
- Codec G.711MU and G.729A
- T.38 Fax
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors

---

[1] Although an Acme Net-Net 3800 was used in the reference configuration, the 4250 and 4500 platforms are also supported.

©2013 Avaya Inc. All Rights Reserved.

- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and mobility (extension to cellular – EC500)

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls (911) are supported but were not tested as part of the compliance test.
- Operator (0) and operator assisted (0 + 10 digits) calls are not supported by Voxox.
- Network Call Redirection using the SIP REFER method or a 302 response with redirection is not supported by Voxox.

2.2. Test Results

Interoperability testing of Voxox SIP Trunk Service was completed with successful results for all test cases. The following limitations are noted for the sample configuration described in these Application Notes.

- **SIP Invite without SDP**: Voxox requires re-Invites to contain Session Description Protocol (SDP) information. Thus, the Acme Packet SBC must be used to insert SDP information in re-Invites from Communication Manager that do not include SDP, i.e., "shuffle" Invites, and also to strip the SDP offered in the ACK method. See **Section 7.6** for information on configuring Acme Packet SBC SIP Interface to insert SDP for re-Invites.

- **Multiple codec offerings in 200 OK**: During an inbound call, Voxox sends an SDP offer with multiple codecs in the 200 OK to a "shuffle" re-Invite from Communication Manager. As stated previously, SDP information is inserted by Acme Packet SBC when Communication Manager sends a "shuffle" re-Invite, and strips the SDP information Communication Manager sends in the ACK. When Voxox sends multiple codec offerings in the 200OK to a "shuffle" re-Invite, the priority order specified in the SDP offer may differ from the original Invite. For example, a responding offer by Voxox may include G.711MU, and G.729A in that order, to a re-Invite with an offer of only G.729A. This change in codec priority will cause Communication Manager to select the preferred codec in the ACK message. This information is never sent back to Voxox, as it is deleted by the SBC, causing a mismatch in codecs and no audio between callers. To circumvent this mismatch, a codec policy was created in Acme Packet SBC (see **Section 7.3**) to rearrange the 200 OK SDP offer to match the priority order specified in Communication Manager Codec Set. This codec policy was then applied to the external facing realm as shown in **Section 7.4**.

Note - These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

©2013 Avaya Inc. All Rights Reserved.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com

For technical support on Voxox service offer, visit online support at http://www.voxox.com/contact

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya customer-premises equipment (CPE) location connected via a T1 Internet connection to Voxox SIP Trunk service. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Acme Packet SBC provides NAT functionality and SIP header manipulation. The Acme Packet SBC receives traffic from the Voxox service on port 5060 and sends traffic to the Voxox service on port 5060, using UDP protocol for network transport. The Voxox service provided Direct Inward Dial (DID) 11 digit numbers. These DID numbers can be mapped by Avaya Aura® Session Manager or Avaya Aura® Communication Manager to Avaya telephone extensions.

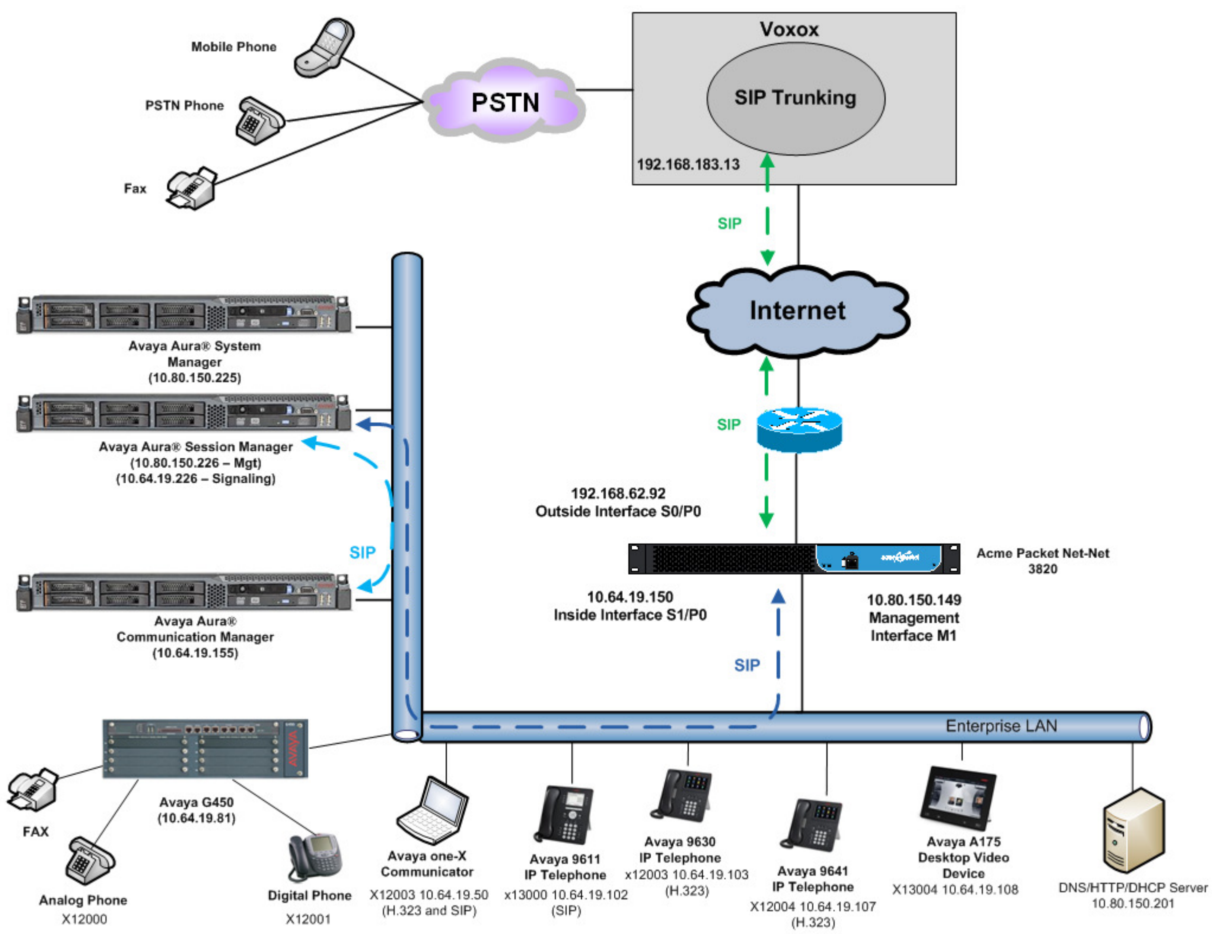


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment:	Software:
HP ProLiant DL360 G7	Avaya Aura® Communication Manager Release 6.3 SP0
HP ProLiant DL360 G7	Avaya Aura® System Manager 6.3 SP2
HP ProLiant DL360 G7	Avaya Aura® Session Manager 6.3 SP2
G450 Gateway	33.13.0
Acme Packet 3820 Net-Net Session Director	SCX6.4.0 MR-2 Patch 1
Avaya 96X0-Series Telephones (H.323)	R 3.2
Avaya 96X1- Series Telephones (SIP)	R6.2.2.17
Avaya 96X1- Series Telephones (H323)	R6.2313
Avaya one-X® Communicator (SIP and H.323)	6.1.8.06-SP8-40314
Avaya Flare® Experience for Windows	1.1.2.11
Avaya Desktop Video Device	Flare 1.1.3
Avaya 6400-Series Digital Telephones	N/A
Okidata Analog Fax	N/A

Table 1: Equipment and Software Used in the Sample Configuration

©2013 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager Release 6.3

This section illustrates an example configuration allowing SIP signaling via the "Processor Ethernet" of Communication Manager to Session Manager. In configurations that use an Avaya G650 Media Gateway, it is also possible to use an Avaya C-LAN in the Avaya G650 Media Gateway for SIP signaling to Session Manager.

Note - The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in these Application Notes.

5.1. Verify Licensed Features

Communication Manager license file controls customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

On **Page 2** of the ***display system-parameters customer-options*** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Voxox SIP Trunk service offer and any other SIP applications. Each call from a non-SIP endpoint to the Voxox SIP Trunk service uses one SIP trunk for the duration of the call. Each call from a SIP endpoint to the Voxox SIP Trunk service uses two SIP trunks for the duration of the call.

```
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: 36000 3
                   Maximum Video Capable IP Softphones: 18000 1
                       Maximum Administered SIP Trunks: 12000 52
  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   2
           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
```


©2013 Avaya Inc. All Rights Reserved.

On **Page 3** of the ***display system-parameters customer-options*** form, verify that **ARS** is enabled.

```
display system-parameters customer-options                          Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
  A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                 ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

On **Page 4** of the ***display system-parameters customer-options*** form, verify that the **Enhanced EC500**, **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging or send-only SDP attributes will be required verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

```
display system-parameters customer-options                          Page   4 of  11
                                OPTIONAL FEATURES
   Emergency Access to Attendant? y                              IP Stations? y
           Enable 'dadmin' Login? y
           Enhanced Conferencing? y                        ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                     Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? n
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                  Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                       IP Trunks? y

           IP Attendant Consoles? y
```


©2013 Avaya Inc. All Rights Reserved.

On **Page 5** of the ***display system-parameters customer-options*** form, verify that the **Private Networking** and **Processor Ethernet** features are enabled.

```
display system-parameters customer-options                Page   5 of  11
                                OPTIONAL FEATURES

                Multinational Locations? n            Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n      Station as Virtual Extension? y
                     Multiple Locations? n
                                             System Management Data Transfer? n
          Personal Station Access (PSA)? y              Tenant Partitioning? y
                       PNC Duplication? n         Terminal Trans. Init. (TTI)? y
                  Port Network Support? y              Time of Day Routing? y
                       Posted Messages? y      TN2501 VAL Maximum Capacity? y
                                                      Uniform Dialing Plan? y
                    Private Networking? y     Usage Allocation Enhancements? y
               Processor and System MSP? y
                    Processor Ethernet? y               Wideband Switching? y
                                                                  Wireless? n
                         Remote Office? y
          Restrict Call Forward Off Net? y
                 Secondary Data Module? y
```

5.2. Dial Plan

In the reference configuration, the Avaya CPE environment uses five digit local extensions such as 12xxx, 14xxx or 20xxx. Trunk Access Codes (TAC) are 3 digits in length and begin with *. The Feature Access Code (FAC) to access Auto Route Selection (ARS) is the single digit 9. The FAC to access Auto Alternate Routing (AAR) is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used.

The dial plan is modified with the ***change dialplan analysis*** command as shown below.

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

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   1            5   ext
   2            5   ext
   8            1   fac
   9            1   fac
   *            3   dac
   #            3   dac
```


©2013 Avaya Inc. All Rights Reserved.

5.3. Node Names

Node names are mappings of names to IP addresses that can be used in various screens. The following ***change node-names ip*** output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is "**SM63**" with IP address "**10.64.19.226**". The node name and IP address for the Processor Ethernet "**procr**" is "**10.64.19.155**".

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
SM63                10.64.19.226
default             0.0.0.0
procr               10.64.19.155
procr6              ::
```

5.4. Processor Ethernet Configuration on HP Common Server

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: 10.64.19.155

           Subnet Mask: /24
```


©2013 Avaya Inc. All Rights Reserved.

5.5. Network Regions for Gateway, Telephones

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1. To provide testing flexibility, network region 2 was associated with other components used specifically for the Voxox SIP Trunk testing.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that **Media Gateway 1** is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (“**10.64.19.155”**), and that the gateway IP address is “**10.64.19.81**”. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```
change media-gateway 1                                          Page   1 of   2
                             MEDIA GATEWAY 1

                    Type: g450
                    Name: G450-1
               Serial No: 08IS38199678
            Encrypt Link? y                   Enable CF? n
          Network Region: 1                    Location: 1
                                              Site Data:
           Recovery Rule: 1

              Registered?  y
   FW Version/HW Vintage: 33 .13 .0  /1
        MGP IPV4 Address: 10.64.19.81
        MGP IPV6 Address:
   Controller IP Address: 10.64.19.155
             MAC Address: 00:1b:4f:03:52:18
```

The following screen shows **Page 2** for **Media Gateway 1**. The gateway has an **S8300** in slot V1 (unused), an **MM712** media module supporting Avaya digital phones in slot V2, an **MM711** supporting analog devices in slot V3, and the capability to provide announcements and music on hold via “**gateway-announcements**” in logical slot V9.

```
change media-gateway 1                                          Page   2 of   2
                             MEDIA GATEWAY 1

                                 Type: g450

Slot   Module Type            Name                     DSP Type  FW/HW version
 V1:   S8300                  ICC MM                   MP80      110  3
 V2:   MM712                  DCP MM
 V3:   MM711                  ANA MM
 V4:
 V5:
 V6:
 V7:
 V8:                                                 Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```


©2013 Avaya Inc. All Rights Reserved.

IP telephones can be assigned a network region based on an IP address mapping. The network region can also associate the IP telephone to a location for location-based routing decisions. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the "gatekeeper" (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. For example, the IP address 10.64.19.109 would be mapped to network region 1, based on the configuration in bold below. In production environments, different sites will typically be on different networks, and ranges of IP addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

```
change ip-network-map                                          Page   1 of  63
                               IP ADDRESS MAPPING

                                               Subnet Network     Emergency
 IP Address                                    Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 10.64.19.100                            /      1      n
   TO: 10.64.19.120
```

The following screen shows IP Network Region 2 configuration. In the shared test environment, network region 2 is used to allow unique behaviors for the Voxox SIP Trunk test environment. In this example, codec set 2 will be used for calls within region 2. The **Authoritative Domain** is set to the enterprise SIP domain "**avayalab.com**" used in the Avaya Interoperability Lab test environment. Session Manager also uses this domain to determined routes for calls based on the domain information of the calls and for SIP phone registration.

```
change ip-network-region 2                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avayalab.com
    Name: SIP TRUNK               Stub Network Region: n
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
```


©2013 Avaya Inc. All Rights Reserved.

The following screen shows the inter-network region connection configuration for region 2. The first bold row shows that network region 2 is directly connected to network region 1, and that codec set 2 will also be used for any connections between region 2 and region 1. For configurations where multiple remote gateways are used, each gateway will typically be configured for a different region, and this screen can be used to specify unique codec or call admission control parameters for the pairs of regions. If a different codec should be used for inter-region connectivity than for intra-region connectivity, a different codec set can be entered in the **codec set** column for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 1, **Page 4** will also show codec set 2 for region 2 to region 1 connectivity.

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

 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    2     y    NoLimit                                             n       t
 2    2                                                                all
 3
 4
```

The following screen shows IP Network Region 1 configuration. In this example, codec set 1 will be used for calls within region 1 due to the **Codec Set** parameter on **Page 1**, but codec set 2 will be used for connections between region 1 and region 2 as noted previously.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avayalab.com
    Name: Enterprise            Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```


©2013 Avaya Inc. All Rights Reserved.

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 2, and that codec set 2 will be used for any connections between region 2 and region 1.

```
change ip-network-region 1                                      Page   4 of  20

 Source Region: 1     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    1                                                                all
 2    2     y    NoLimit                                             n       t
```

5.6. IP Codec Sets

The following screen shows the configuration for codec set 2, the codec set configured to be used for calls within region 2 and for calls between region 1 and region 2. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, calls to and from the PSTN via the SIP trunks would use G.729A, since G.729A is the preferred codec by both Voxox and the Avaya ip-codec-set. A codec policy is also applied to the Acme Packet SBC (**Section 7.4**) that matches the preference order of this codec set.

```
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:
```

The following screen shows **Page 2** of the form. Configure the Fax **Mode** field to "**t.38-standard**". Set the Fax **Redundancy** field to "**0**", and the **ECM** field to "**y**".

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

                    Mode                    Redundancy
    FAX             t.38-standard            0             ECM: y
    Modem           off                      0
    TDD/TTY         US                       3
    Clear-channel   n                        0
```

The following screen shows the configuration for codec set 1. This configuration for codec set 1 is used for analog, digital, H.323, SIP phones and other connections within region 1.

©2013 Avaya Inc. All Rights Reserved.

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

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.722.2           n         1        20
 2: G.722-64K                   2        20
 3: G.711MU           n         2        20
 4: G.729A            n         2        20
```

5.7. SIP Signaling Group

This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of "**sip**", a **Near-end Node Name** of "**procr**", and a **Far-end Node Name** of "**SM63**". In the example screens, the **Transport Method** for all signaling groups is "**tls**". The **Peer Detection Enabled** field is set to "**y**" and a peer Session Manager has been previously detected. The **Far-end Domain** is set to "**avayalab.com**" matching the configuration in place prior to adding the Voxox SIP Trunk service configuration. The **Enable Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to "**rtp-payload**", which corresponds to RFC 2833.

The following screen shows signaling group 4. Signaling group 4 will be used for processing PSTN calls to / from Voxox via Session Manager. The **Far-end Network Region** is configured to region 2. Port 5091 has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with Voxox DID numbers to a route policy that uses a SIP entity link to Communication Manager specifying port 5091. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. Other parameters may be left at default values.

```
change signaling-group 4                                       Page   1 of   2
                                SIGNALING GROUP

 Group Number: 4              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                 Far-end Node Name: SM63
 Near-end Listen Port: 5091                Far-end Listen Port: 5091
                                        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
```


©2013 Avaya Inc. All Rights Reserved.

The following screen shows signaling group 3, the signaling group to Session Manager that was in place prior to adding the Voxox SIP Trunk configuration to the shared Avaya Solutions and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Voxox SIP Trunk but will be used to enable SIP phones to use features from Communication Manager. Again, the **Near-end Node Name** is "**procr**" and the **Far-end Node Name** is "**SM63**", the node name of the Session Manager. Unlike the signaling group used for the Voxox SIP Trunk signaling, the **Far-end Network Region** is "**1**".

```
change signaling-group 3                                            Page   1 of   2
                                SIGNALING GROUP

 Group Number: 3              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n

   Near-end Node Name: procr                Far-end Node Name: SM63
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

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
```


©2013 Avaya Inc. All Rights Reserved.

5.8. SIP Trunk Group

This section illustrates the configuration of the SIP Trunk Groups corresponding to the SIP signaling group from the previous section.

The following shows **Page 1** for trunk group 4, which will be used for incoming and outgoing PSTN calls from and to Voxox. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field is set to "**public-ntwrk**" for the trunks that will handle calls with Voxox. The **Direction** has been configured to "**two-way**" to allow incoming and outgoing calls in the sample configuration.

```
change trunk-group 4                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 4                    Group Type: sip           CDR Reports: y
  Group Name: Voxox                       COR: 1        TN: 1        TAC: *04
   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: 4
                                                     Number of Members: 15
```

The following screen shows **Page 2** for trunk group 4. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default 600 to 900. Although not strictly necessary, some SIP products prefer a higher session refresh interval than the Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

```
change trunk-group 4                                            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): 900

 Disconnect Supervision - In? y  Out? y


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


©2013 Avaya Inc. All Rights Reserved.

The following screen shows **Page 3** for trunk group 4. All parameters except those in bold are default values. The **Numbering Format** will use "**private**" numbering, meaning that the private numbering table would be consulted for any mappings of Communication Manager extensions to alternate numbers to be sent to Session Manager.

```
change trunk-group 4                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y


                     Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no

 Show ANSWERED BY on Display? y
```

The following screen shows **Page 4** for trunk group 4. The bold fields have non-default values. Although not strictly necessary, the **Telephone Event Payload Type** has been set to "**101**" to match Voxox configuration. For redirected calls, Voxox does not require a Diversion or History-Info header. Both the **Send Diversion Header** and **Support Request History** are set to "**n**". Set **Convert 180 to 183 for Early Media** to "**y**".

```
change trunk-group 4                                              Page   4 of  21
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? n
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? y
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

The following screen shows **Page 1** for trunk group 3, the bi-directional "tie" trunk group to Session Manager that existed before adding the Voxox SIP Trunk configuration to the shared Avaya Interoperability Lab network. Recall that this trunk is used to enable SIP phones to use features from Communication Manager and to communicate with other Avaya applications, such as Avaya Aura® Messaging, and does not reflect any unique Voxox configuration.

©2013 Avaya Inc. All Rights Reserved.

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

Group Number: 3                    Group Type: sip           CDR Reports: y
  Group Name: To SM Enterprise            COR: 1        TN: 1        TAC: *03
   Direction: two-way       Outgoing Display? n
 Dial Access? n                               Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     Number of Members: 20
```

The following shows **Page 3** for trunk group 3. Note that this tie trunk group uses a "**private**" **Numbering Format**.

```
change trunk-group 3                                            Page   3 of  21
                                TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y
                     Numbering Format: private
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no
```

The following screen shows **Page 4** for trunk group 3. Note that unlike the trunks associated with Voxox calls that have non-default "protocol variations", this trunk group maintains all default values. **Support Request History** must remain set to the default "**y**" to support proper subscriber mailbox identification by Avaya Aura® Messaging.

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

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n

                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```


©2013 Avaya Inc. All Rights Reserved.

5.9. Route Pattern Directing Outbound Calls to Voxox

Route pattern 1 will be used for calls destined for the PSTN via the Voxox SIP Trunk service. 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. The **Numbering Format** "**unk-unk**" means no special numbering format will be included.

If desired, one or more alternate Communication Manager trunks can be listed in the route pattern so that the Look-Ahead Routing (**LAR**) "**next**" setting can route-advance to attempt to complete the call using alternate trunks should there be no response or an error response from the far-end.

```
change route-pattern 1                                              Page   1 of   3
                    Pattern Number: 1      Pattern Name: To PSTN 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: 4    0       1                                                      n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

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


©2013 Avaya Inc. All Rights Reserved.

5.10. Route Pattern for Internal Calls via Session Manager

Route pattern 3 contains trunk group 3, the “private” tie trunk group to Session Manager. The **Numbering Format** “**lev0-pvt**” insures proper numbering format for internal local calls to Session Manager.

```
change route-pattern 3                                          Page   1 of   3
                    Pattern Number: 3      Pattern Name: ToSM Enterprise
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No. Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 3    0                                                              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 y  n            bothept                             lev0-pvt  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
```

5.11. Private Numbering

The ***change private-unknown-numbering*** command may be used to define the format of numbers sent to Voxox in SIP headers such as the “From”, “Contact”, and “PAI” headers. In general, the mappings of internal extensions to Voxox DID numbers may be done in Session Manager (via Digit Conversion in adaptations) or in Communication Manager (via private-numbering form for outbound calls, and incoming call handling treatment form for the inbound trunk group).

In the example abridged output below, a specific Communication Manager extension (10000) is mapped to a DID number that is known to Voxox for this SIP Trunk connection (**1702xxxxxx5**), when the call uses trunk group 4. Alternatively, Communication Manager can send the five digit extension to Session Manager, and Session Manager can adapt the number to the Voxox DID. Both methods were tested successfully.

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

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  10                                           5     Total Administered: 5
 5  12                                           5        Maximum Entries: 540
 5  14                                           5
 5  20                                           5
 5  10000            4          1702xxxxxx5      11
```


©2013 Avaya Inc. All Rights Reserved.

5.12. ARS Routing For Outbound Calls

Although not illustrated in these Application Notes, location-based routing may be configured so that users at different locations that dial the same telephone number can have calls choose different route-patterns. In these Application Notes, the ARS "all locations" table directs ARS calls to specific SIP Trunks to Session Manager.

The following screen shows a specific ARS configuration as an example. If a user dials the ARS access code followed by 13035551234, the call will select route pattern 1. Of course, matching of the dialed string need not be this specific. The ARS configuration shown here is not intended to be prescriptive.

```
change ars analysis 1305551234                              Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    13035551234           11   11    1       fnpa          n
```

The ***list ars route-chosen*** command can be used on a target dialed number to check whether routing will behave as intended. An example is shown below.

```
list ars route-chosen 13035551234
                           ARS ROUTE CHOSEN REPORT
     Location:  1                      Partitioned Group Number:  1

      Dialed            Total        Route    Call      Node
      String          Min    Max    Pattern   Type     Number    Location

 13035551234          11    11       1        fnpa                 all
   Actual Outpulsed Digits by Preference (leading 35 of maximum 42 digit)

 1: 13035551234
```

5.13. 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
```

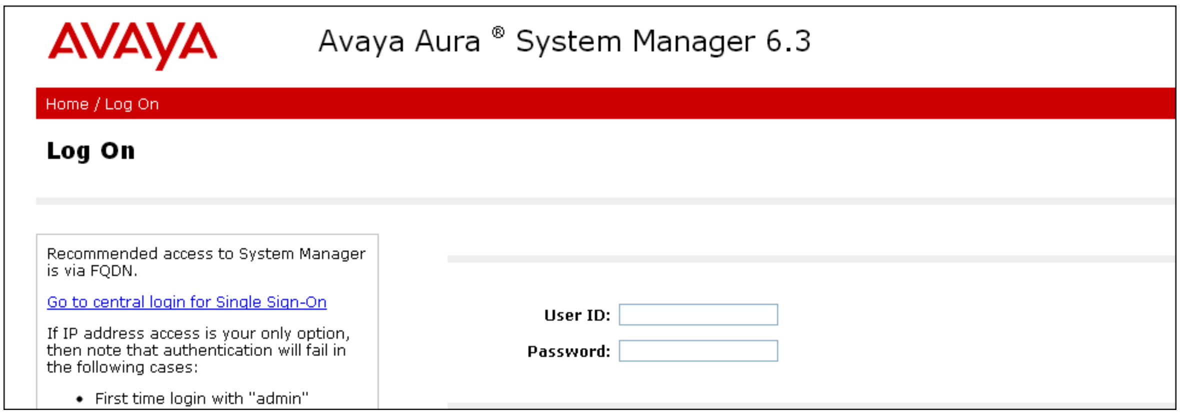

©2013 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Session Manager Release 6.3

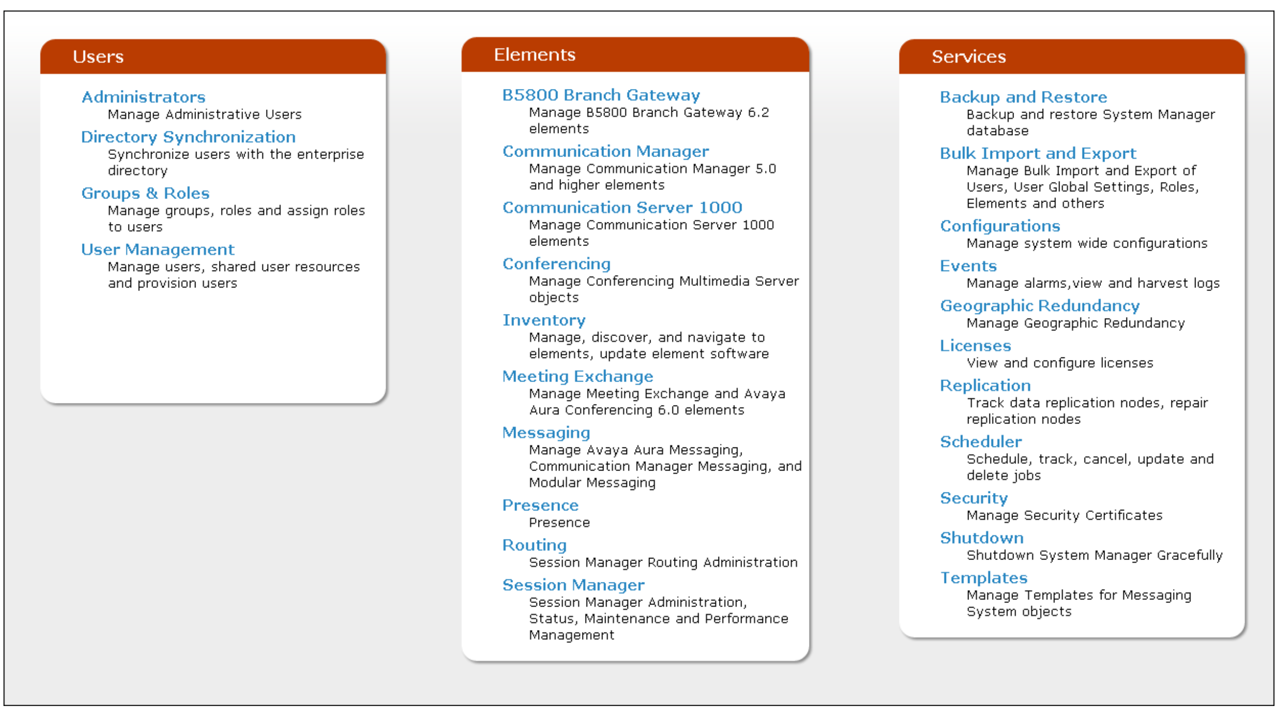
This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between System Manager and Session Manager.

Session Manager is managed via System Manager. Using a web browser, access "https://<ip-addr of System Manager>/SMGR". In the **Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown).



Once logged in, a **Home Screen** is displayed. An abridged **Home Screen** is shown below.



©2013 Avaya Inc. All Rights Reserved.

Under the heading “Elements” in the center, select **Routing**. The right side of the screen, illustrated below, outlines a series of steps. The sub-sections that follow are in the same order as the steps outlined under **Introduction to Network Routing Policy** in the abridged screen shown below.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Scroll down to review additional information as shown below. In these Application Notes, all steps are illustrated with the exception of Step 9, since “Regular Expressions” were not used.

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of the routing application "Dial patterns". That's why this overall routing workflow can be interpreted as

"Dial Pattern driven approach to define Routing Policies"

That means (with regard to steps listed above):

Step 7: "Routing Polices" are defined

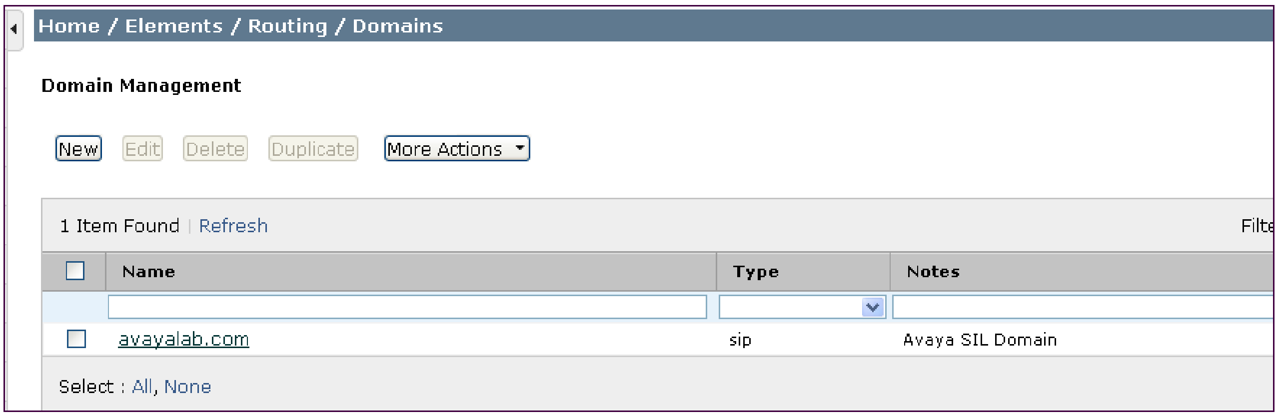
Step 8: "Dial Patterns" are defined and assigned to "Routing Policies" and "Locations" (one step)

Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

6.1. Domains

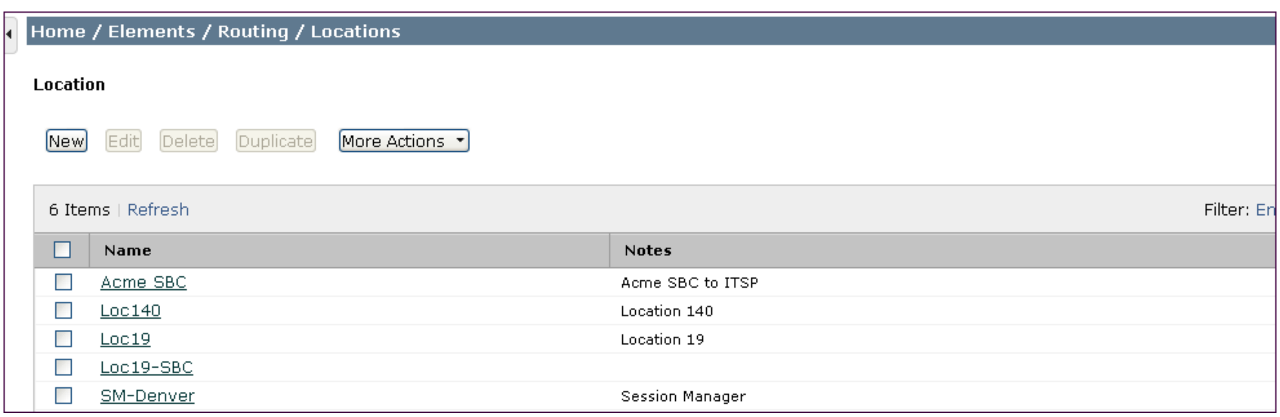
To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button after changes are completed.

The following screen shows a list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among other Avaya interoperability test efforts. The domain "**avayalab.com**" was used for communication with Avaya SIP Telephones and other Avaya systems and applications. The domain "avayalab.com" is not known to the Voxox production service.



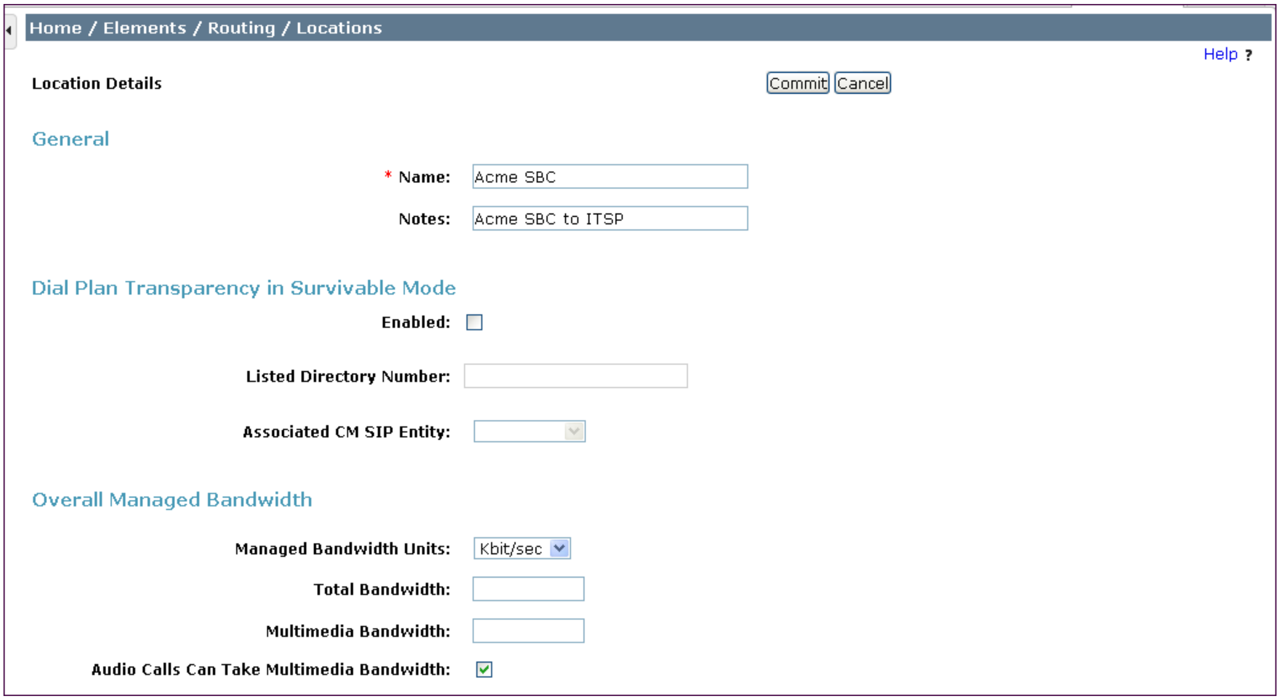
6.2. Locations

To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button (not shown) after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.

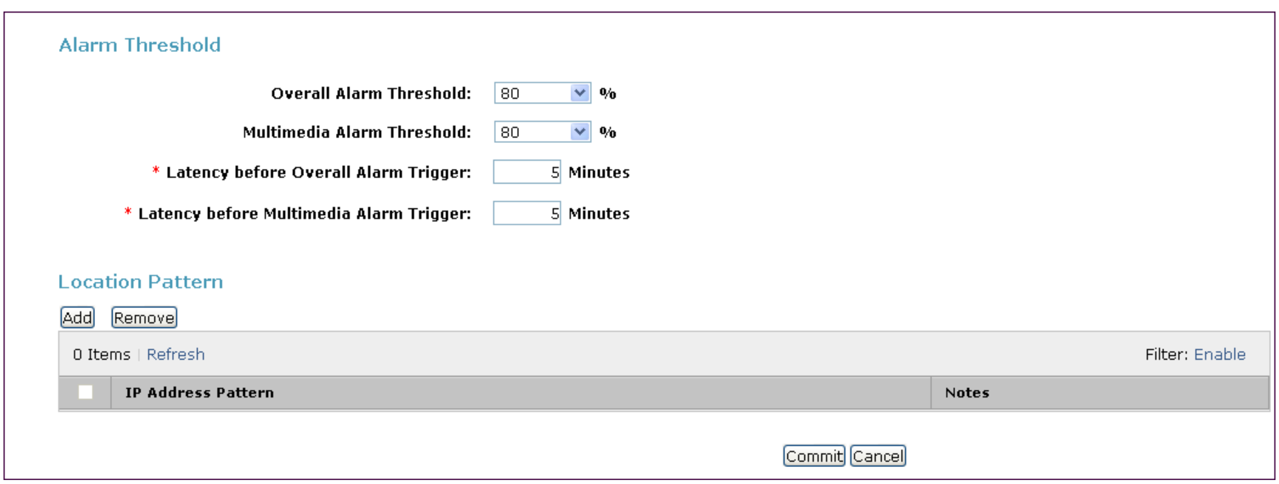


©2013 Avaya Inc. All Rights Reserved.

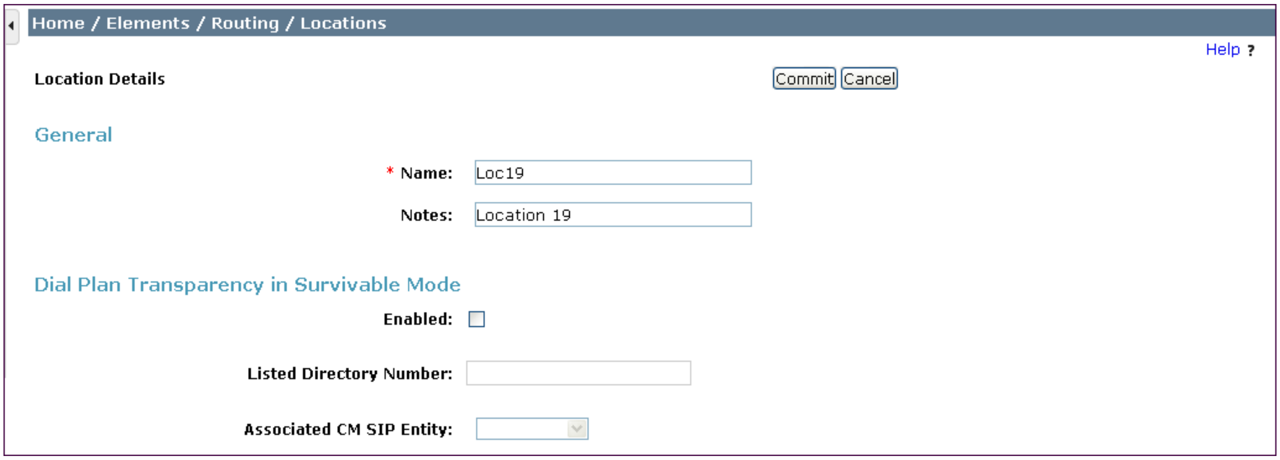
The following screen shows the location details for the location named "**Acme SBC**", corresponding to the Acme Packet SBC relevant to these Application Notes. Later, the location with name "**Acme SBC**" will be assigned to the corresponding Acme Packet SBC SIP Entity.



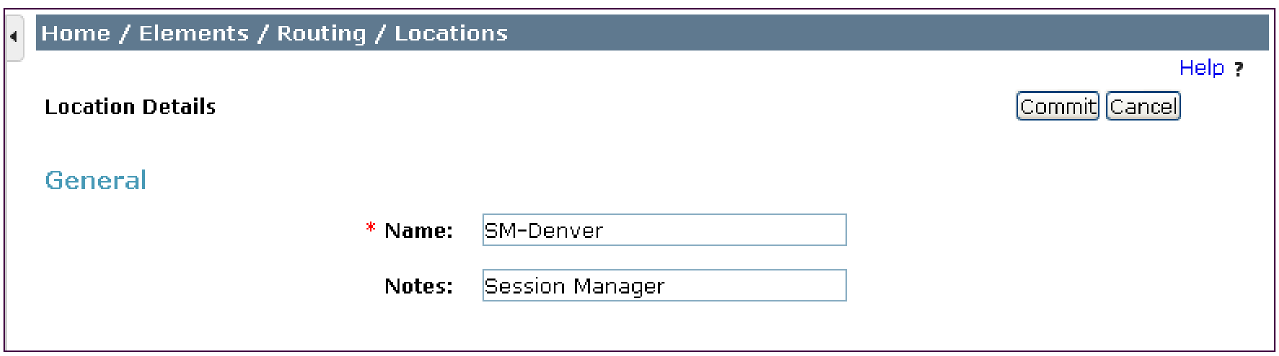
Scrolling down, the **Location Pattern** is used to identify call routing based on IP address. Session Manager matches the IP address of SIP Entities against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the Location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



The following screen shows the location details for the location named “**Loc19**”. Later, this location will be assigned to the corresponding Communication Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.



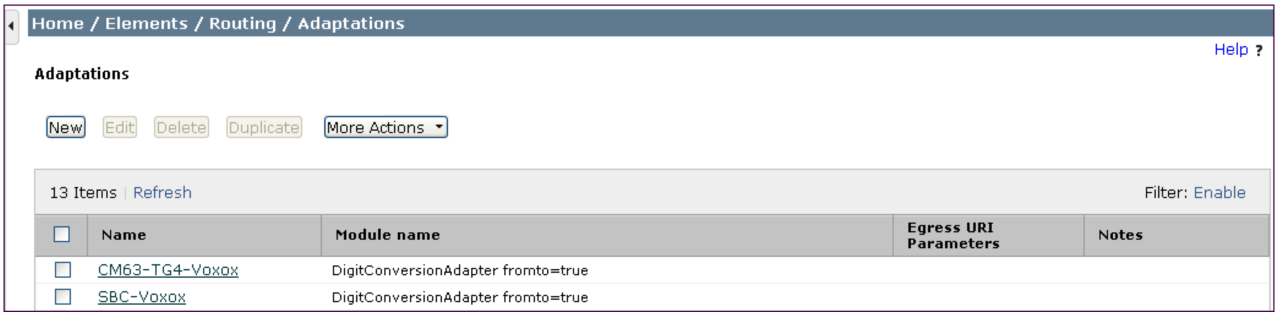
The following screen shows the location details for the location named “**SM-Denver**”, corresponding to Session Manager. This location was created during the installation of Session Manager and was assigned to the Session Manager SIP Entity. In the sample configuration, other location parameters (not shown) retained the default values.



©2013 Avaya Inc. All Rights Reserved.

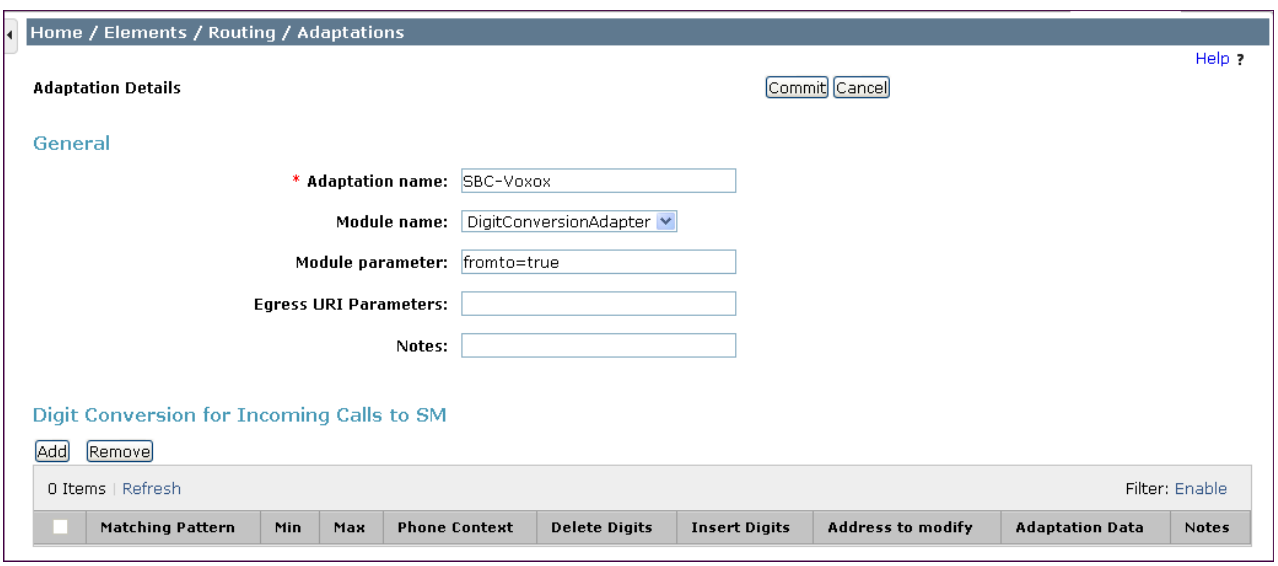
6.3. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed (not shown).



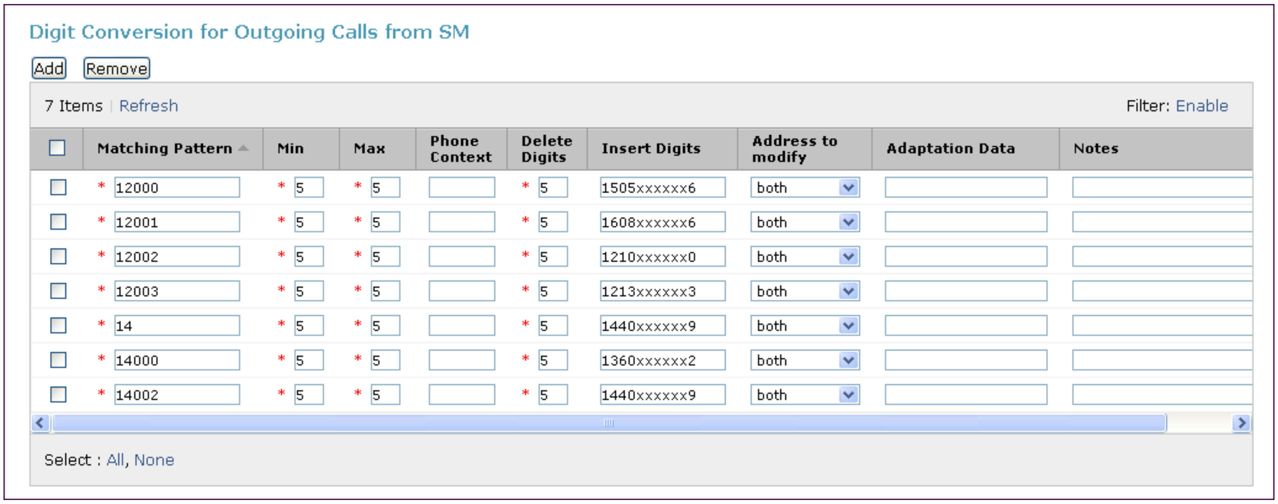
The adapter named "**SBC-Voxox**" shown below will later be assigned to the SIP Entity for the Acme Packet SBC, specifying that all communication from Session Manager to the Acme Packet SBCs will use this adapter.

This adaptation uses the "**DigitConversionAdapter**" module and specifies the "**fromto=true**" parameter. This parameter adapts the From and To headers along with the Request-Line and PAI headers.



©2013 Avaya Inc. All Rights Reserved.

Scrolling down to the **Digit Conversion for Outgoing Calls from SM** section, the following screen shows the extension numbers used on Communication Manager that are being converted to the 11 digit DID numbers assigned by Voxox. Since this adapter will be assigned to the SIP Entity sending calls to Acme Packet SBC for routing to the PSTN, the settings for **Digit Conversion for Outgoing Calls from SM** correspond with outgoing calls from Communication Manager to the PSTN using the Voxox SIP Trunk service. In general, digit conversion such as this, that converts a Communication Manager extension to a corresponding LDN or DID number known to the PSTN, can be performed in Session Manager as shown below. For example, if extension 12000 dials the PSTN, and if Communication Manager sends the extension 12000 to Session Manager as the calling number, Session Manager would convert the calling number to 1505xxxxxx6. Public DID numbers have been masked for security purposes.


Digit Conversion for Outgoing Calls from SM

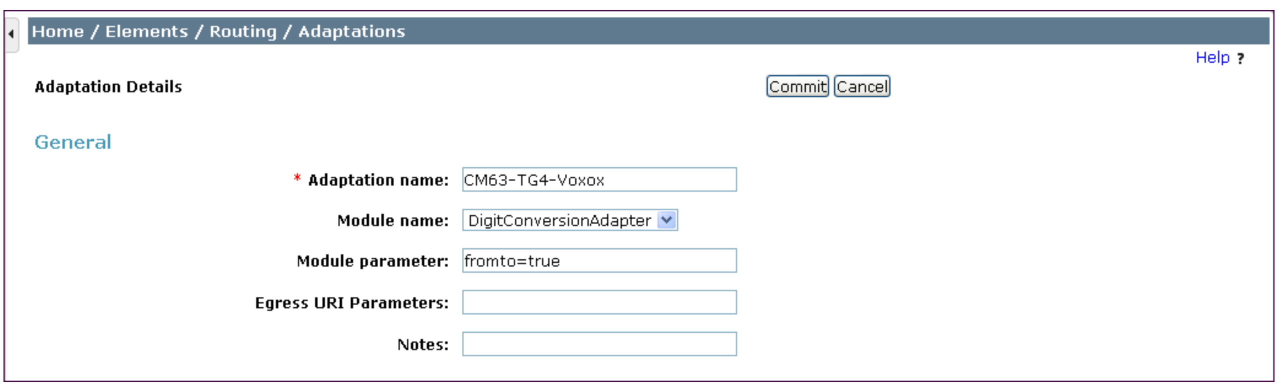
Add Remove

7 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
	* 12000	* 5	* 5		* 5	1505xxxxxx6	both		
	* 12001	* 5	* 5		* 5	1608xxxxxx6	both		
	* 12002	* 5	* 5		* 5	1210xxxxxx0	both		
	* 12003	* 5	* 5		* 5	1213xxxxxx3	both		
	* 14	* 5	* 5		* 5	1440xxxxxx9	both		
	* 14000	* 5	* 5		* 5	1360xxxxxx2	both		
	* 14002	* 5	* 5		* 5	1440xxxxxx9	both		

Select : All, None

The adapter named "**CM63-TG4-Voxox**" shown in the following screen will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Voxox SIP Trunk service. This adaptation also uses the "**DigitConversionAdapter**" and specifies the "**fromto=true**" parameter.



Scrolling down, the following screen shows a portion of the "**CM63-TG4-Voxox**" adapter that can be used to convert 11 digit DID numbers assigned by Voxox to the extension number used on Communication Manager. Since this adapter will be assigned to the SIP Entity sending calls to Communication Manager from the PSTN, the settings for **Digit Conversion for Outgoing Calls**

©2013 Avaya Inc. All Rights Reserved.

from SM correspond to incoming calls from the PSTN to Communication Manager. In the example shown below, if a user on the PSTN dials 1210xxxxxx0, Session Manager will convert the number to 12002 before sending the SIP INVITE to Communication Manager. In this case, digit conversion is done after the routing decision has been made based upon the user part of the SIP URI. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. Public DID numbers have been masked for security purposes.

Digit Conversion for Outgoing Calls from SM

Add Remove

6 Items | Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
* 1210xxxxxx0	* 11	* 11		* 11	12002	both		CM - H.323 96x1
* 1213xxxxxx3	* 11	* 11		* 11	12003	both		CM - H323 96x0
* 1360xxxxxx2	* 11	* 11		* 11	14000	both		CM - SIP 96x1
* 1440xxxxxx9	* 11	* 11		* 11	14002	both		CM- Flare
* 1505xxxxxx6	* 11	* 11		* 11	12000	both		CM Analog
* 1608xxxxxx6	* 11	* 11		* 11	12001	both		CM Digital

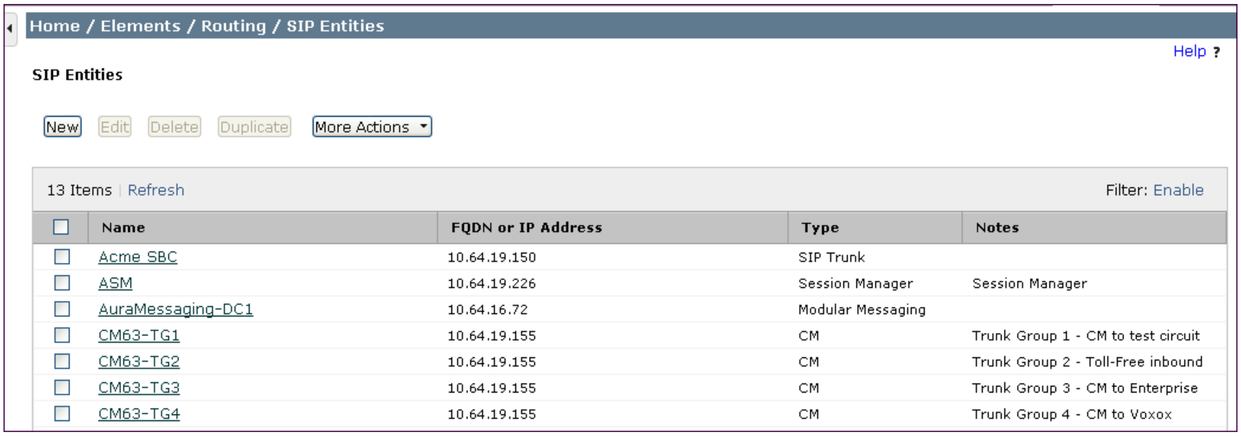
Select : All, None

©2013 Avaya Inc. All Rights Reserved.

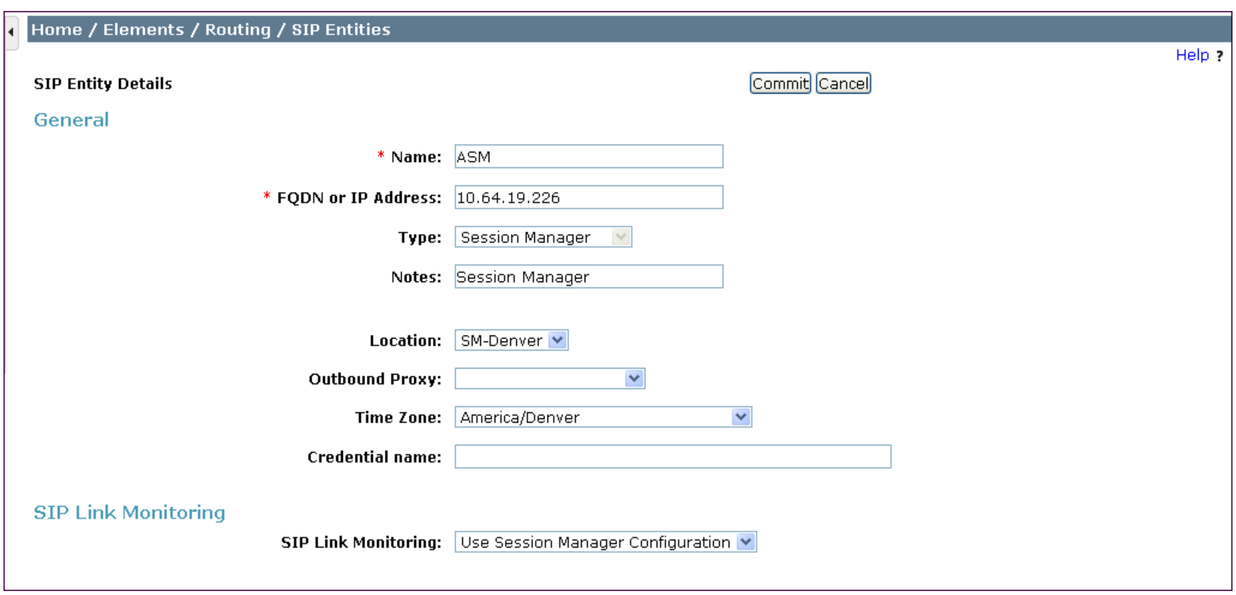
6.4. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. Click the **Commit** button after changes are completed.

The following screen shows the list of configured SIP entities in the shared test environment.

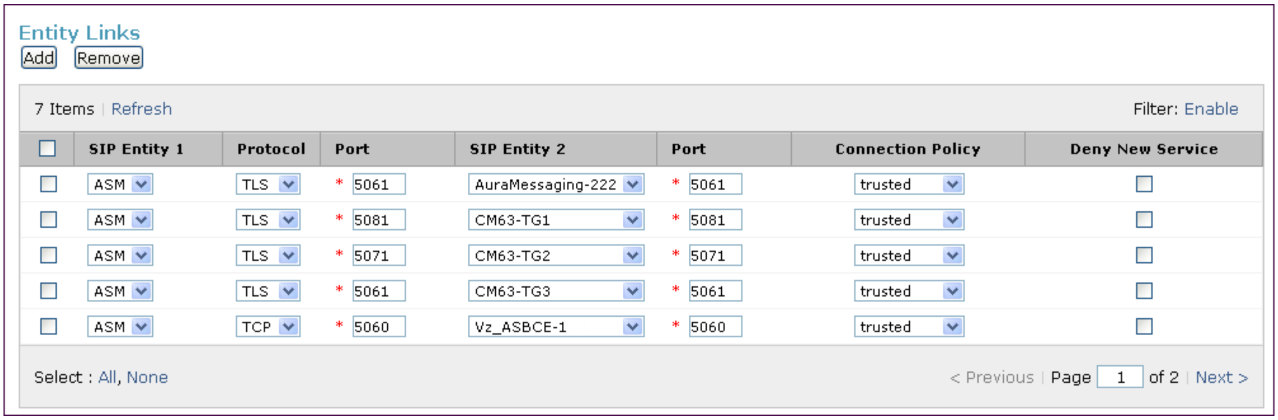


The following screen shows the upper portion of the **SIP Entity Details** corresponding to "**ASM**". The **FQDN or IP Address** field for "**ASM**" is the Session Manager Security Module IP Address (10.64.19.226), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is "Session Manager". Select an appropriate location for the Session Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location "**SM-Denver**". The default **SIP Link Monitoring** parameters may be used. Unless changed elsewhere, links from other SIP entities to this instance of Session Manager will use the default SIP Link Monitoring timers, configurable at the Session Manager level. If desired, these timers may be customized for each entity.



©2013 Avaya Inc. All Rights Reserved.

Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for "**ASM**". The links relevant to these Application Notes are described in the subsequent section.


Entity Links

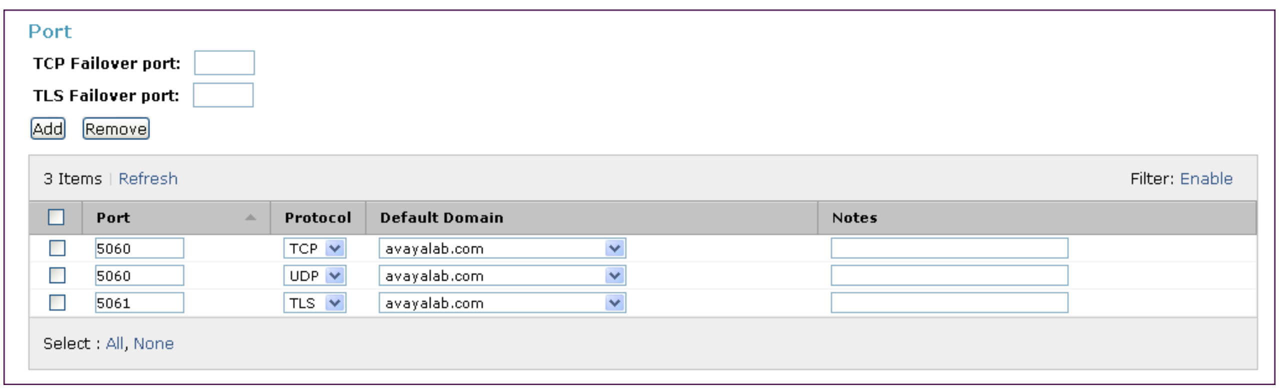
Add Remove

7 Items | Refresh   Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
	ASM	TLS	* 5061	AuraMessaging-222	* 5061	trusted	
	ASM	TLS	* 5081	CM63-TG1	* 5081	trusted	
	ASM	TLS	* 5071	CM63-TG2	* 5071	trusted	
	ASM	TLS	* 5061	CM63-TG3	* 5061	trusted	
	ASM	TCP	* 5060	Vz_ASBCE-1	* 5060	trusted	

Select : All, None   < Previous | Page 1 of 2 | Next >

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, illustrating the configured ports for "**ASM**". 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**.


Port

TCP Failover port:

TLS Failover port:

Add Remove

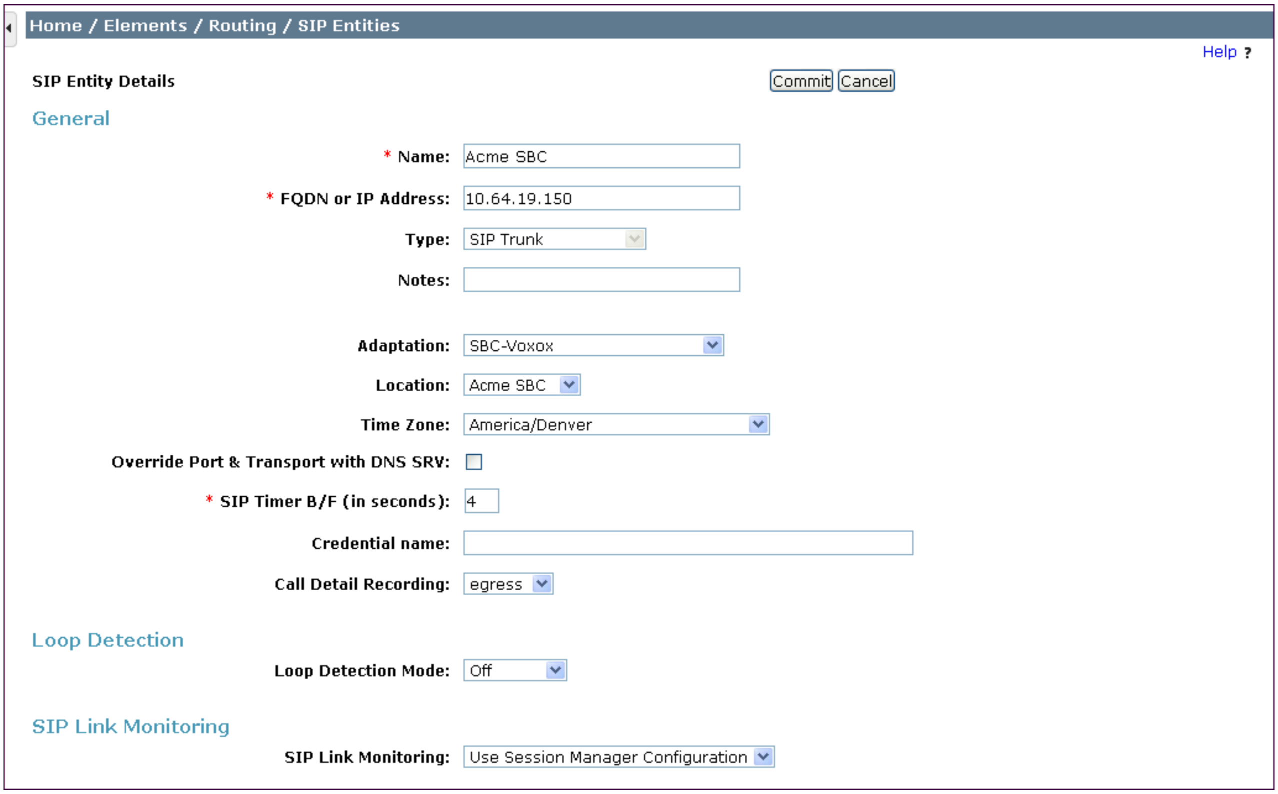
3 Items | Refresh   Filter: Enable

	Port	Protocol	Default Domain	Notes
	5060	TCP	avayalab.com	
	5060	UDP	avayalab.com	
	5061	TLS	avayalab.com	

Select : All, None

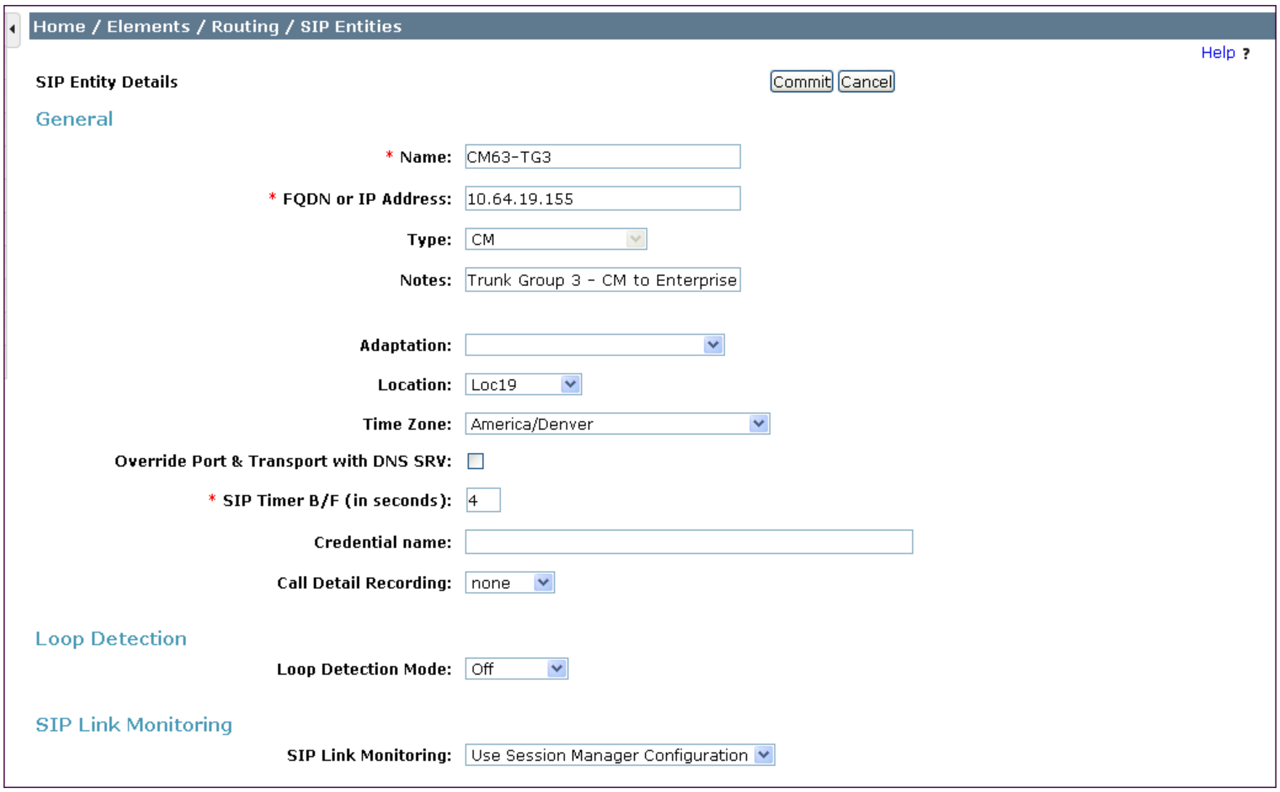
©2013 Avaya Inc. All Rights Reserved.

The following screen shows the upper portion of the **SIP Entity Details** corresponding to "**Acme SBC**". The **FQDN or IP Address** field is configured with the Acme Packet SBC inside IP Address (10.64.19.150). "**SIP Trunk**" is selected from the **Type** drop-down menu for Acme Packet SBC SIP Entities. This Acme Packet SBC has been assigned to **Location** "**Acme SBC**", and the "**SBC-Voxox**" adapter is applied. Other parameters (not shown) retain default values.



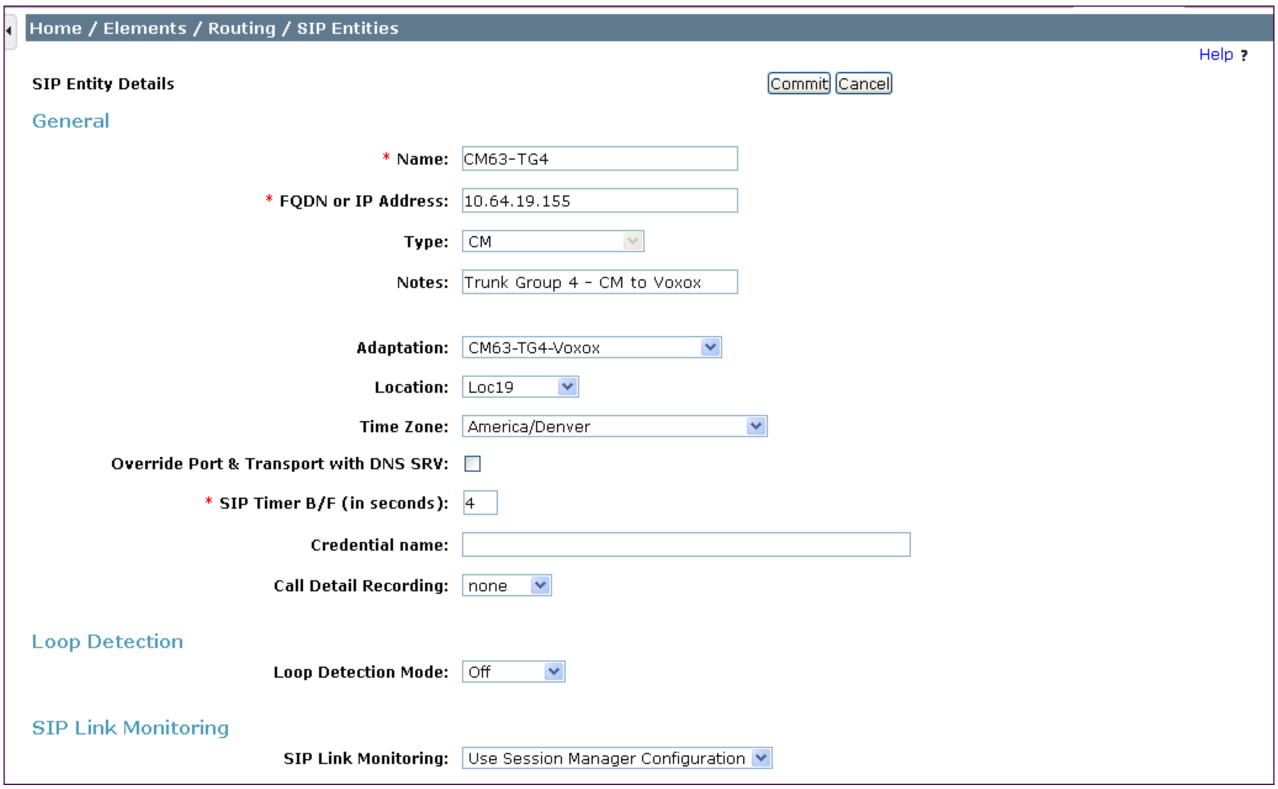
©2013 Avaya Inc. All Rights Reserved.

The following screen shows a portion of the **SIP Entity Details** corresponding to a Communication Manager SIP Entity named "**CM63-TG3**" This is the SIP Entity that was already in place in the shared Avaya Interoperability Test Lab environment, prior to adding the Voxox SIP Trunk configuration. The **FQDN or IP Address** field contains the IP Address of the "processor Ethernet" (10.64.19.155). In systems with Avaya G650 Media Gateways containing C-LAN cards, C-LAN cards may also be used as SIP entities, instead of, or in addition to, the "processor Ethernet". "**CM**" is selected from the **Type** drop-down menu and "**Loc19**" is selected for the **Location**.



©2013 Avaya Inc. All Rights Reserved.

The following screen shows the **SIP Entity Details** for an entity named "**CM63-TG4**". This entity uses the same **FQDN or IP Address** (10.64.19.155) as the prior entity with name "CM63-TG3"; both correspond to Communication Manager Processor Ethernet IP Address. Later, a unique port, 5091, will be used for the Entity Link to "**CM63-TG4**". Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Voxox SIP Trunk from other SIP traffic arriving from the same IP Address of the Session Manager, such as SIP traffic associated with SIP Telephones or other SIP-integrated applications. "**CM**" is selected from the **Type** drop-down menu, "**Loc19**" is selected for the **Location,** and the "**CM63-TG4-Voxox**" adapter is applied.

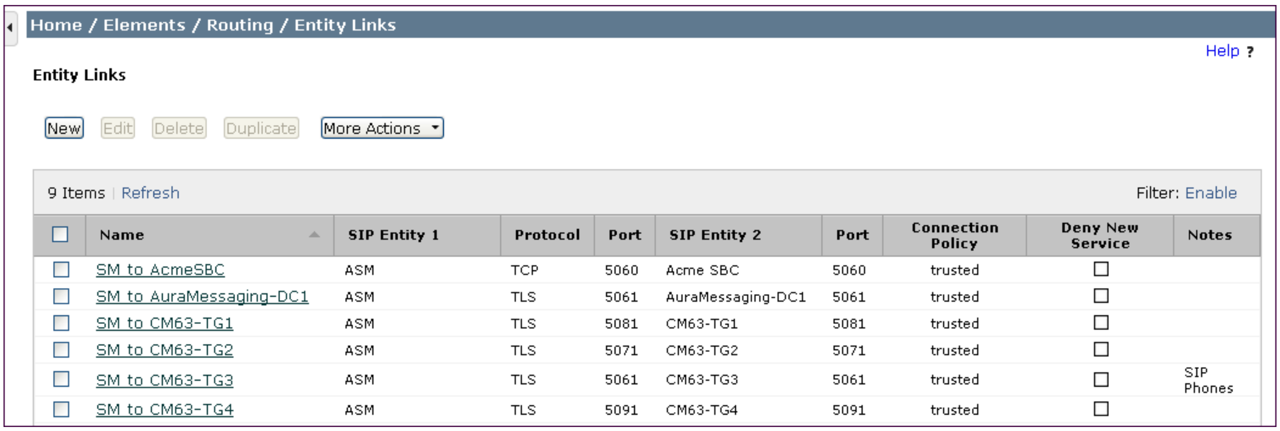


©2013 Avaya Inc. All Rights Reserved.

6.5. Entity Links

To view or change Entity Links, select **Routing → Entity Links**. Click on the checkbox corresponding to the name of a link and **Edit** to edit an existing link, or the **New** button to add a link. Click the **Commit** button after changes are completed.

The following screen shows a list of configured links. In the screen below, the links named "**SM to AcmeSBC**" and "**SM to CM63-TG4**" are most relevant to these Application Notes. Each link uses the entity named "**ASM**" as **SIP Entity 1**, and the appropriate entity, such as "**Acme SBC**", for **SIP Entity 2**.



	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
☐	SM to AcmeSBC	ASM	TCP	5060	Acme SBC	5060	trusted	☐	
☐	SM to AuraMessaging-DC1	ASM	TLS	5061	AuraMessaging-DC1	5061	trusted	☐	
☐	SM to CM63-TG1	ASM	TLS	5081	CM63-TG1	5081	trusted	☐	
☐	SM to CM63-TG2	ASM	TLS	5071	CM63-TG2	5071	trusted	☐	
☐	SM to CM63-TG3	ASM	TLS	5061	CM63-TG3	5061	trusted	☐	SIP Phones
☐	SM to CM63-TG4	ASM	TLS	5091	CM63-TG4	5091	trusted	☐	

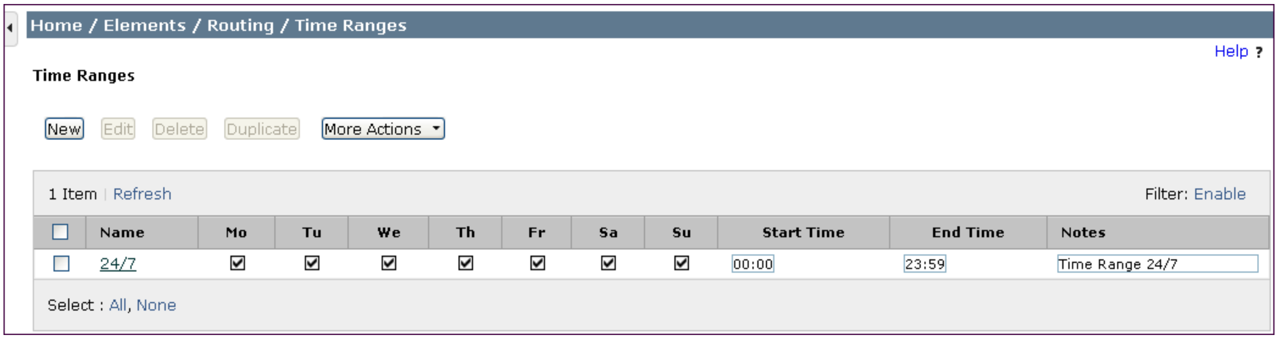
The link named "**SM to CM63-TG3**" links Session Manager "**ASM**" with Communication Manager processor Ethernet. This link existed in the configuration prior to adding the Voxox SIP Trunk related configuration. This link, using port 5061, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Voxox, such as traffic related to SIP Telephones registered to Session Manager.

The link named "**SM to CM63-TG4**" also links Session Manager "**ASM**" with Communication Manager processor Ethernet. However, this link uses port 5091 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Voxox SIP Trunk from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired.

©2013 Avaya Inc. All Rights Reserved.

6.6. Time Ranges

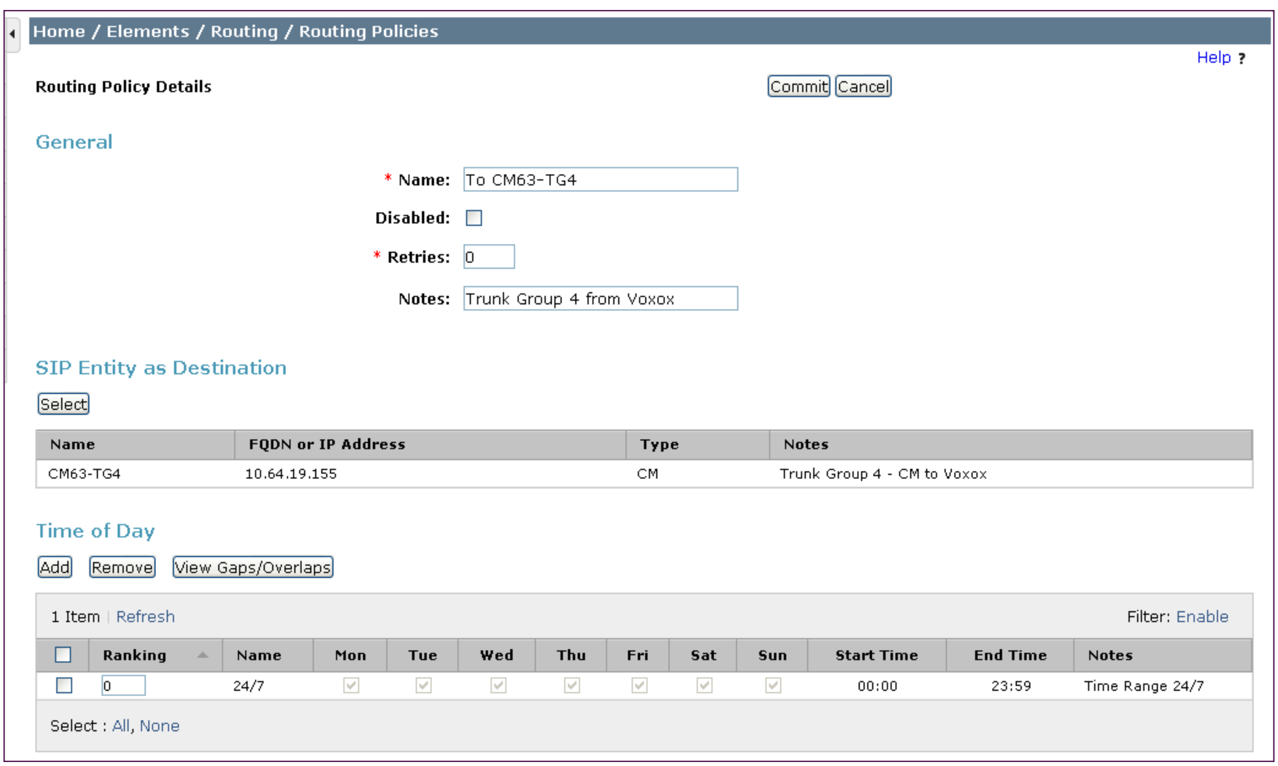
To view or change Time Ranges, select **Routing → Time Ranges**. The Routing Policies shown subsequently will use the "**24/7**" range since time-based routing was not the focus of these Application Notes. Click the **Commit** button (not shown) after changes are completed.



6.7. Routing Policies

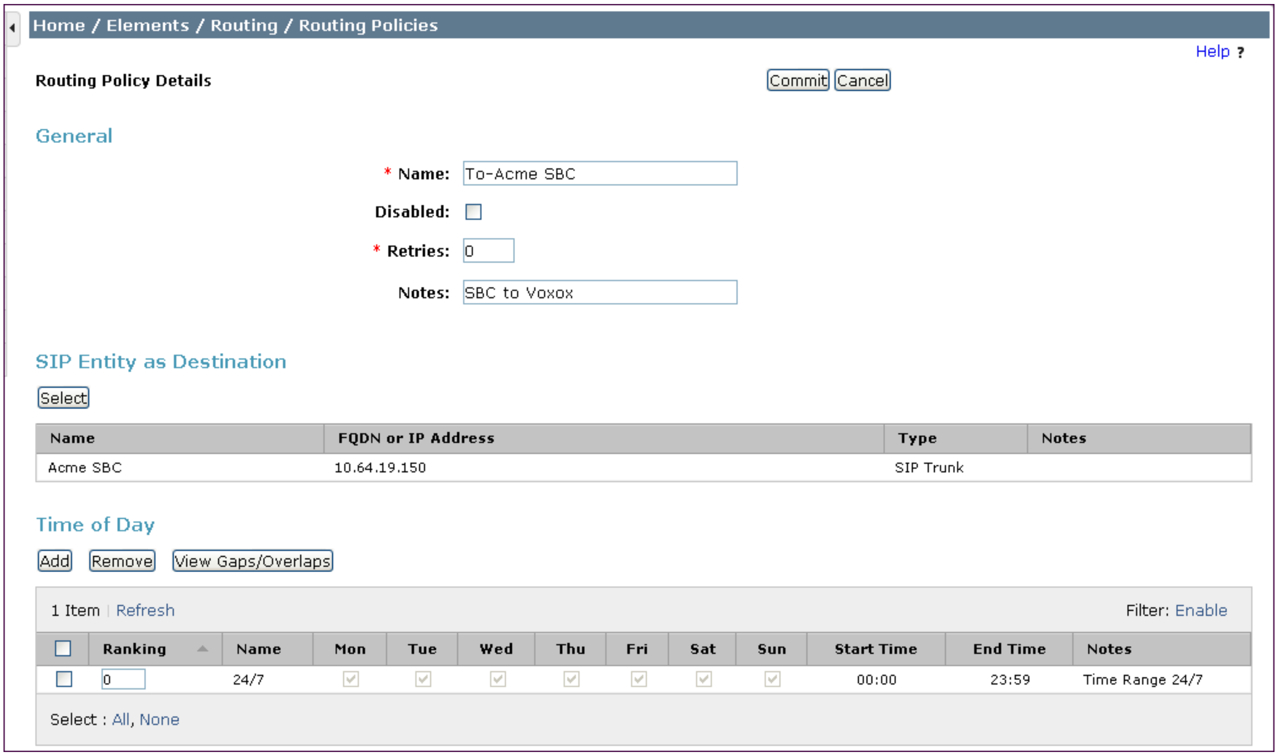
To view or change routing policies, select **Routing → Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. Click the **Commit** button after changes are completed (not shown).

The following screen shows the **Routing Policy Details** for the policy named "**To-CM63-TG4**" associated with incoming PSTN calls from Voxox to Communication Manager. Observe the **SIP Entity as Destination** is the entity named "**CM63-TG4**" that was created in **Section 6.4**.



©2013 Avaya Inc. All Rights Reserved.

The following screen shows the **Routing Policy Details** for the policy named "**To-Acme SBC**" associated with outgoing calls from Communication Manager to the PSTN via Voxox SIP Trunk through Acme Packet SBC. Observe the **SIP Entity as Destination** as the entity named "**Acme SBC**".

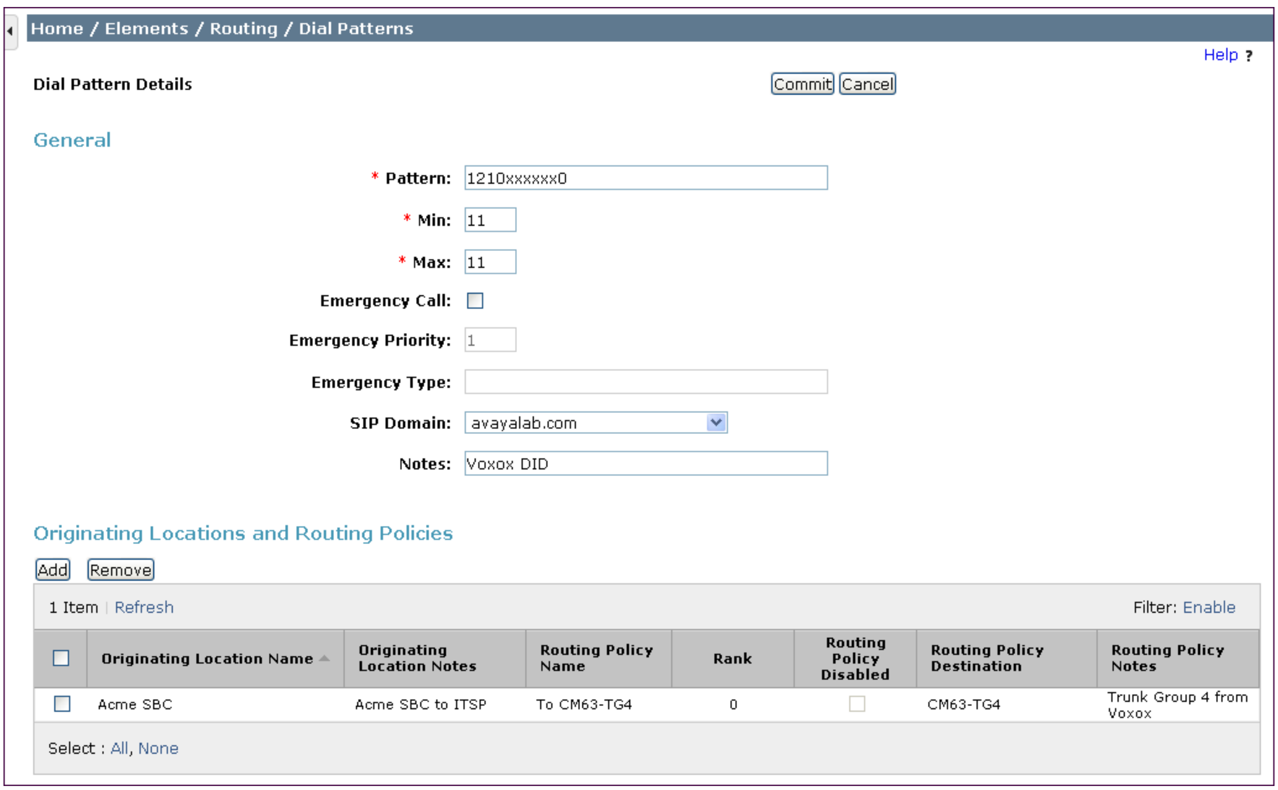


©2013 Avaya Inc. All Rights Reserved.

6.8. Dial Patterns

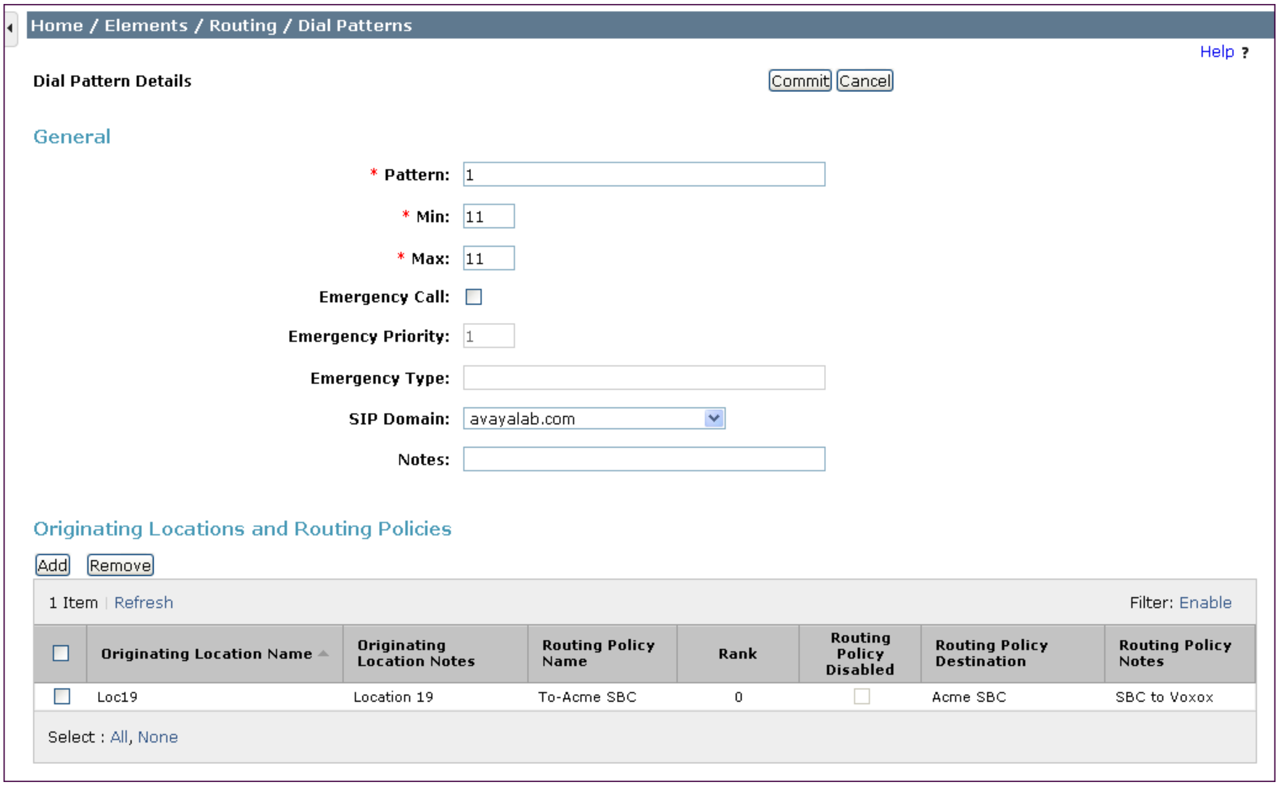
To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click the **Commit** button after changes are completed.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. When a user on the PSTN dials a number assigned to the Voxox SIP Trunk service, such as 1210xxxxxx0, Voxox delivers the number to the enterprise, and the Acme Packet SBC sends the call to Session Manager. The pattern below matches on 1-210-xxx-xxx0 specifically (The DID number has been masked for security purposes). Dial patterns can alternatively match on ranges of number (e.g., a DID block). Under **Originating Locations and Routing Policies**, the routing policy named "**To-CM63-TG4**" is chosen when the call originates from **Originating Location Name** "**Acme SBC**". This sends the call to Communication Manager using port 5091 as described previously.



©2013 Avaya Inc. All Rights Reserved.

The following screen illustrates an example dial pattern used to verify outbound calls from the enterprise to the PSTN. When a Communication Manager user dials a PSTN number such as 9-1303-555-1234, Communication Manager sends the call to Session Manager. Session Manager will match the dial pattern shown below and send the call to the Acme Packet SBC via the **Routing Policy Name "To-Acme SBC"**.



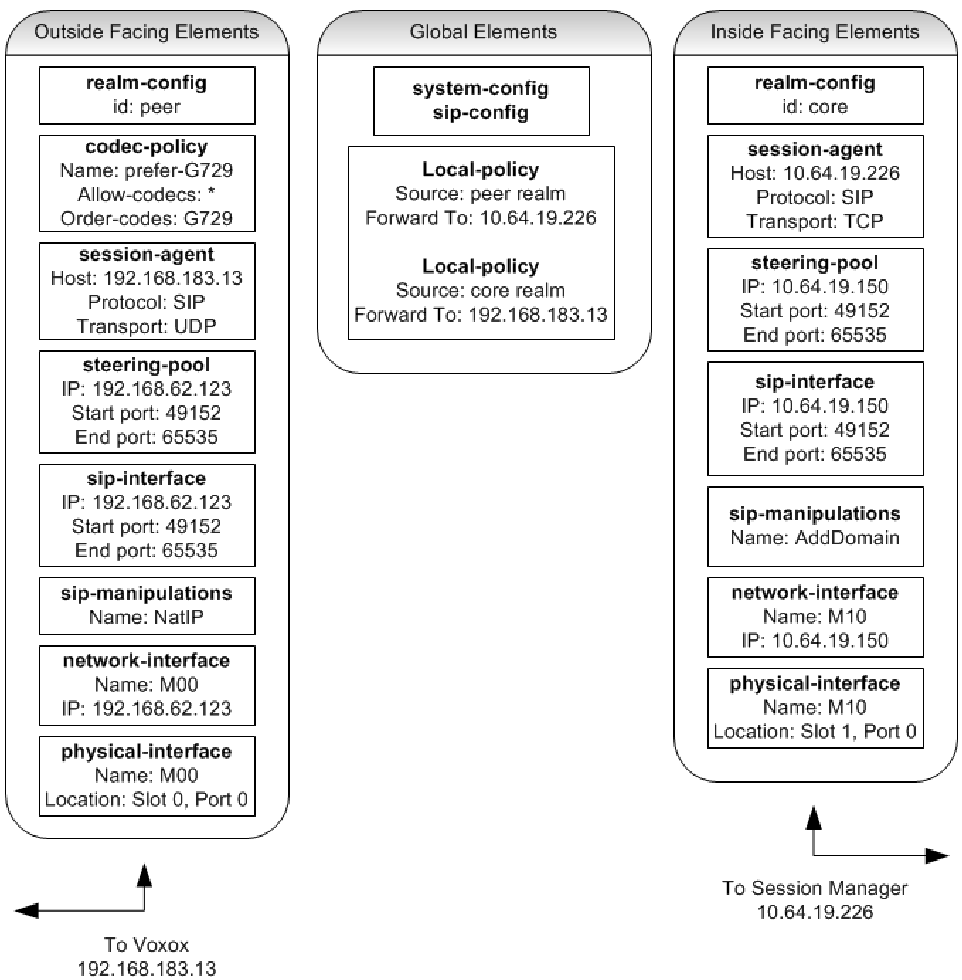
©2013 Avaya Inc. All Rights Reserved.

7. Configure Acme Packet Session Border Controller

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

A pictorial view of this configuration is shown below. It shows the internal components used in the sample configuration. Each of these components is defined in the Acme Packet SBC configuration file contained in **Appendix A**. However, this section does not cover standard Acme Packet SBC 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 Voxox and Session Manager. The remaining fields are generally the default/standard value used by the Acme Packet SBC for that field. For additional details on the administration of the Acme Packet SBC, see **Reference [8]**.



©2013 Avaya Inc. All Rights Reserved.

7.1. Acme Packet Command Line Interface Summary

The Acme Packet SBC 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 SBC 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 SBC 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.

©2013 Avaya Inc. All Rights Reserved.

7.2. Physical and Network Interfaces

In the sample configuration, the Ethernet interface slot 0 / port 0 of the Acme Packet SBC is connected to the external untrusted network. Ethernet slot 1 / port 0 is connected to the internal corporate LAN. A network interface is 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
        speed
        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
        speed
        overload-protection             disabled
        last-modified-by                admin@console
        last-modified-date              2011-11-01 10:00:38
```


©2013 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 Voxox SIP trunk service resides. In the sample configuration, the IP address "**192.168.62.123**" is assigned to the public interface and "**10.64.19.150**" is 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 SBC 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 SBC will answer ICMP requests on this interface.

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

```
network-interface
       name                           M00
       sub-port-id                    0
       description                    PUBLIC
       hostname
       ip-address                     192.168.62.123
       pri-utility-addr
       sec-utility-addr
       netmask                        255.255.255.128
       gateway                        192.168.62.1
       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                    192.168.62.123
       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
```


©2013 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                      10.64.19.150
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.0
        gateway                         10.64.19.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     10.64.19.150
        ftp-address
        icmp-address                    10.64.19.150
        snmp-address
        telnet-address
        ssh-address
        last-modified-by                admin@10.80.150.38
        last-modified-date              2011-11-01 12:16:22
```

7.3. Codec Policy

In the sample configuration, a codec policy (**codec-policy**) is used to change the preferred codec offered in the SDP information to prevent a codec mismatch during the call setup process. See **Section 2.2** for details. Depending on the order of preference desired by the end customer, either "**prefer-G729**" or "**prefer-PCMU**" will be applied to the peer realm in the next section.

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

- **name:** A descriptive string used to reference the codec policy.
- **allow-codecs:** An asterisk (*) indicates any codec.
- **order-codecs:** Codec(s) listed in the preferred order.

```
codec-policy
        name                            prefer-G729
        allow-codecs                    *
        order-codecs                    G729
        last-modified-by                admin@10.80.150.50
        last-modified-date              2013-09-06 13:56:14
codec-policy
        name                            prefer-PCMU
        allow-codecs                    *
        order-codecs                    PCMU
        last-modified-by                admin@10.80.150.50
        last-modified-date              2013-09-09 17:00:17
```


©2013 Avaya Inc. All Rights Reserved.

7.4. Realm

A realm represents a group of related Acme Packet SBC components. Two realms are defined in the sample configuration. The **peer** realm is defined for the external network and the **core** realm is 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**" is used and for the **core** realm "**AddDomain**" is used. These names refer to a set of sip-manipulations (defined in **Section 7.7**) that are performed on outbound traffic from the Acme Packet SBC. 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 SBC as well as to outbound traffic from the private side (**core**) of the Acme Packet SBC.
- **codec-policy:** For the **peer** realm "**prefer-G729**" is used. This refers to the codec-policy, previously defined in **Section 7.3**, which will arrange the offered codecs to prefer G.729. During compliance testing, G.711MU was tested by changing this field to "**prefer-PCMU**" along with changing the order of preference to G.711MU as the first codec choice in the Communication Manager IP Codec Set in **Section 5.6**.

The peer realm:

```
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 >

        dyn-refer-term                  disabled
        codec-policy                    prefer-G729
        codec-manip-in-realm            disabled

< text removed for brevity >
```


©2013 Avaya Inc. All Rights Reserved.

The core realm:

```
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 >
```

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

©2013 Avaya Inc. All Rights Reserved.

```
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 >
```


©2013 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 SBC. 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.
- **sip-port**
    - **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.
- **add-sdp-invite:** for the **peer** realm, "**reinvite**" is selected. This allows the Acme Packet SBC to insert SDP information in re-Invites from Communication Manager. See **Section 2.2** for details.

The settings for the sip-interface for Voxox SIP Trunk:

```
sip-interface
        state                           enabled
        realm-id                        peer
        description
        sip-port
                address                         192.168.62.123
                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 >

        add-sdp-invite                  reinvite
        add-sdp-profiles

< text removed for brevity >
```

©2013 Avaya Inc. All Rights Reserved.

The settings for the sip-interface for Session Manager:

```
sip-interface
        state                           enabled
        realm-id                        core
        description
        sip-port
                address                         10.64.19.150
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0

< text removed for brevity >
```

7.7. Session Agent

A session agent defines the characteristics of a signaling peer to the Acme Packet SBC such as Session Manager and Voxox 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 SBC to set the SIP "Max-Forward" field to 70 in outbound SIP OPTIONS pings generated by the Acme Packet SBC to this session agent.
- **ping-interval:** Specifies the interval (in seconds) between each ping attempt.

©2013 Avaya Inc. All Rights Reserved.

The settings for the session agent used for Voxox SIP Trunk:

```
session-agent
      hostname                       192.168.183.13
      ip-address                     192.168.183.13
      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 >
```

The settings for the session agent used for Session Manager:

```
session-agent
      hostname                       10.64.19.226
      ip-address                     10.64.19.226
      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 >
```


©2013 Avaya Inc. All Rights Reserved.

7.8. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages (if necessary) for interoperability. In **Section 7.4**, it is defined that the set of sip-manipulations named "**NatIP**" is performed on outbound traffic in the **peer** realm, and "**AddDomain**" is 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 hide the private IP address and enterprise domain name which appear in the "To", "From", "Request-URI", and "PAI" SIP headers for outbound calls.

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

©2013 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 SBC.

```
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 >
```


©2013 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 6.1**) 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 >
```

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

7.9. Steering Pools

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

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

- **ip-address:** The address of the interface on the Acme Packet SBC.
- **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                      192.168.62.123
        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                      10.64.19.150
        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
```

7.10. 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.

©2013 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 **10.80.150.226** (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 IP address **192.168.183.13**.

```
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@10.80.150.50
        last-modified-date            2013-08-19 16:50:24
        policy-attribute
                next-hop                      10.54.19.226
                realm                         core
                action                        none

< text removed for brevity >

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@10.80.150.50
        last-modified-date            2013-08-19 18:18:54
        policy-attribute
                next-hop                      192.168.183.13
                realm                         peer
                action                        none


< text removed for brevity >
```

8. Verification Steps

This section provides example verifications of the Avaya configuration with Voxox SIP Trunk service.

8.1. Avaya Aura® Communication Manager Verifications

This section illustrates verifications from Communication Manager.

8.1.1 Example Incoming Call from PSTN via Voxox SIP Trunk

Incoming PSTN calls arrive from Voxox at Acme Packet SBC, which sends the call to Session Manager. Session Manager sends the call to Communication Manager. On Communication Manager, the incoming call arrives via signaling group 4 and trunk group 4.

The following edited Communication Manager ***list trace tac*** trace output shows a call incoming on trunk group 4. The PSTN telephone dialed 1210-xxx-xxx0. Session Manager mapped the number received from Voxox to the extension of a Communication Manager telephone (x12002). Extension 12002 is an IP Telephone with IP address 10.64.19.103 in Region 1. The RTP media path is “ip-direct” from the IP Telephone (10.64.19.109) to the “inside” of the Acme Packet SBC (10.64.19.150) in Region 2.

```
list trace tac *04                                                  Page   1
                                LIST TRACE
time            data

12:22:41 TRACE STARTED 09/18/2013 CM Release String cold-03.0.124.0-20850
/* Incoming call arrives to Communication Manager for extension 12002 */
12:22:45 SIP<INVITE sip:12002@avayalab.com:5060 SIP/2.0
12:22:45     active trunk-group 4 member 1    cid 0x156
/* Communication Manager sends 183 with SDP as a result of TG 4 configuration */
12:22:45 SIP>SIP/2.0 183 Session Progress
/* Communication Manager dials the extension 12002 */
12:22:45     dial 12002
12:22:45     ring station      12002 cid 0x156
12:22:45     G711MU ss:off ps:20
             rgn:1 [10.64.19.103]:2404
             rgn:1 [10.64.19.81]:2060
/* G450 Gateway at 10.80.19.81, ringback tone heard by caller */
12:22:45     G729 ss:off ps:20
             rgn:2 [10.64.19.150]:49156
             rgn:1 [10.64.19.81]:2052
12:22:46 SIP<PRACK sip:12002@10.64.19.155:5091;transport=tls SIP/2.0
12:22:46 SIP>SIP/2.0 200 OK
/* User Answers call, Communication Manager sends 200 OK */
12:22:48 SIP>SIP/2.0 200 OK
12:22:48     active station      12002 cid 0x156

<Continued on Next Page>
```


©2013 Avaya Inc. All Rights Reserved.

```
/* Communication Manager receives ACK to 200 OK */
12:22:48 SIP<ACK sip:12002@10.64.19.155:5091;transport=tls SIP/2.0
/* Communication Manager shuffles the call from the gateway to direct media * /
12:22:48 SIP>INVITE sip:13035551234@10.64.19.150:5060;transport=tcp;
12:22:48 SIP>gsid=295d1310-208d-11e3-9f05-9c8e992b0a68 SIP/2.0
12:22:48     G729A ss:off ps:20
             rgn:2 [10.64.19.150]:49156
             rgn:1 [10.64.19.103]:2404
12:22:48     G729 ss:off ps:20
             rgn:1 [10.64.19.103]:2404
             rgn:2 [10.64.19.150]:49156
12:22:49 SIP>ACK sip:13035551234@10.64.19.150:5060;transport=tcp;gsi
12:22:49 SIP>d=295d1310-208d-11e3-9f05-9c8e992b0a68 SIP/2.0
/* Communiction Manager Extension terminates the call */
12:22:51 SIP>BYE sip:13035551234@10.64.19.150:5060;transport=tcp;gsi
12:22:51 SIP>d=295d1310-208d-11e3-9f05-9c8e992b0a68 SIP/2.0
12:22:51     idle station      12002 cid 0x156
```

The following screen shows **Page 2** of the output of the ***status trunk*** command pertaining to this same call. Note the signaling using port 5091 between Communication Manager and Session Manager. Note the media is "**ip-direct**" from the IP Telephone (10.64.19.103) to the inside IP address of Acme Packet SBC (10.64.19.150) using codec G.729.

```
status trunk 4/1                                              Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                               Port
   Near-end:  10.64.19.155                           : 5091
    Far-end:  10.64.19.226                           : 5091
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                               Port
   Near-end:  10.64.19.103                           : 2404
    Far-end:  10.64.19.150                           : 49160

 Video Near:
  Video Far:
 Video Port:
  Video Near-end Codec:               Video Far-end Codec:
```

The following screen shows **Page 3** of the output of the ***status trunk*** command pertaining to this same call. Here it can be observed that G.729a codec is used.

```
status trunk 4/1                                              Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00031
T00031:TX:10.64.19.150:49160/g729/20ms
S00025:RX:10.64.19.103:2404/g729a/20ms
```

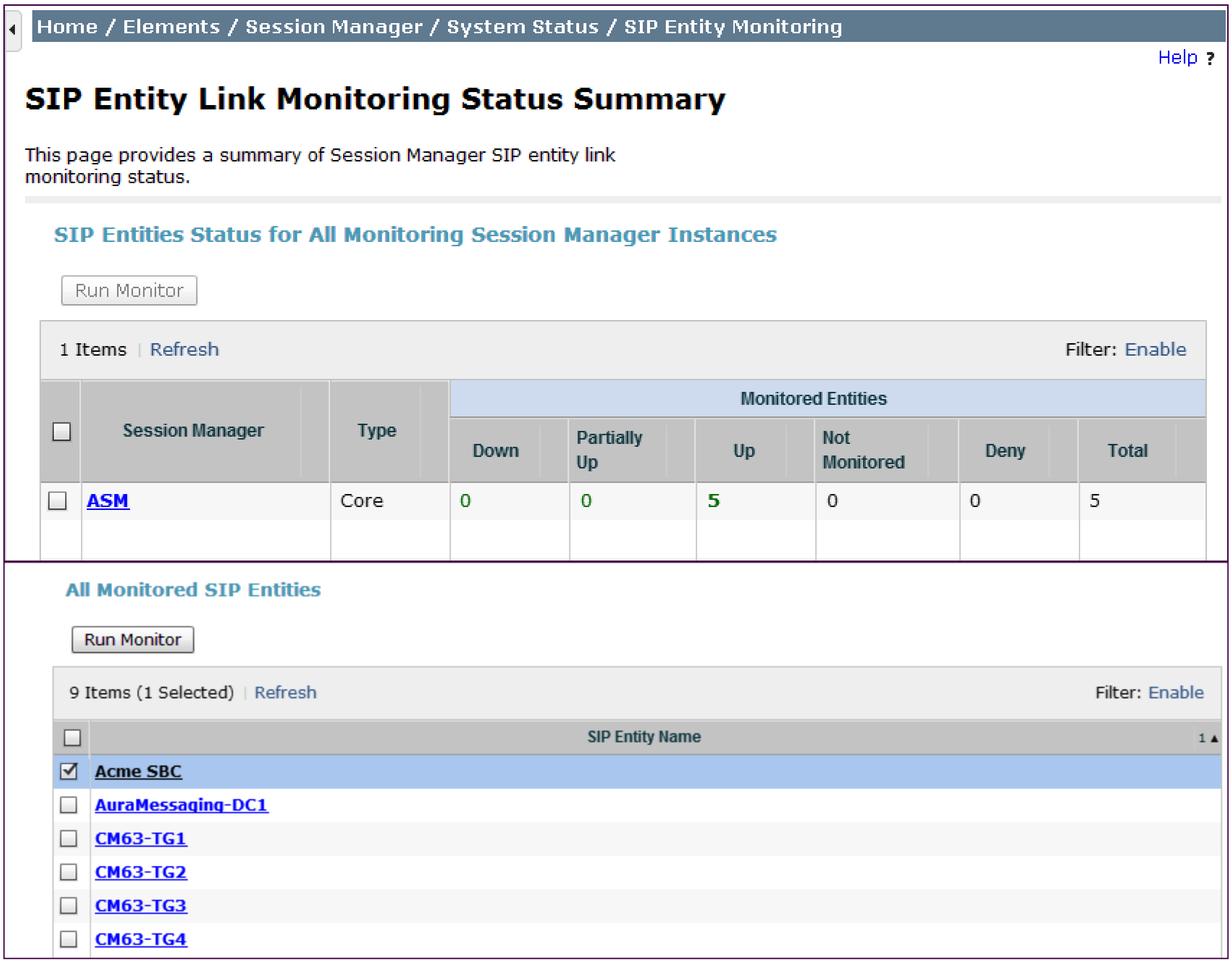

©2013 Avaya Inc. All Rights Reserved.

8.2. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

This section contains verification steps that may be performed using System Manager for Session Manager.

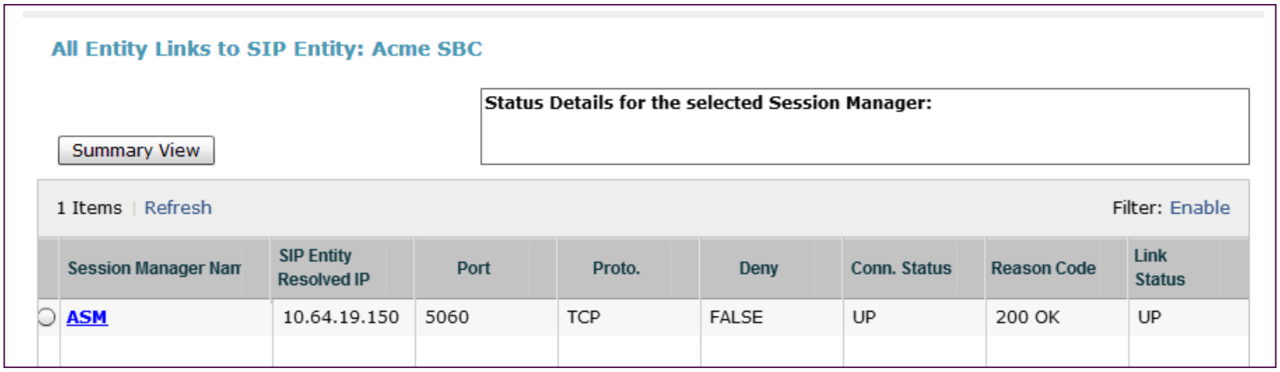
8.2.1 Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**, as shown below.



©2013 Avaya Inc. All Rights Reserved.

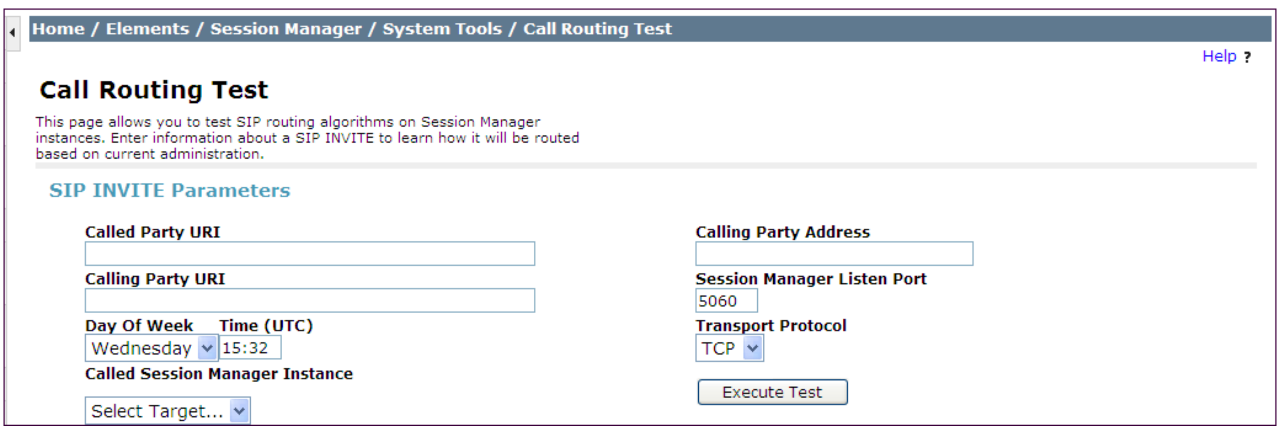
From the list of monitored entities, select an entity of interest, such as "**Acme SBC**". Under normal operating conditions, the **Link Status** should be "**UP**" as shown in the example screen below.



Session Manager Nam	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
ASM	10.64.19.150	5060	TCP	FALSE	UP	200 OK	UP

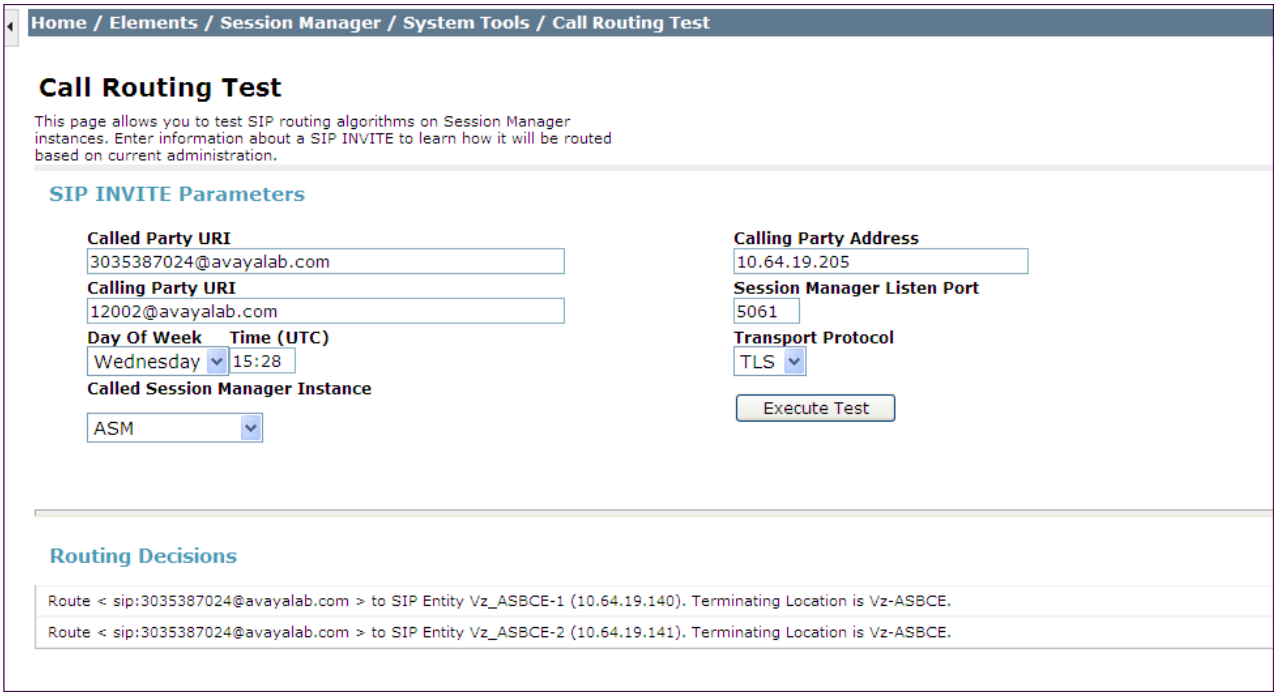
8.2.2 Call Routing Test

The **Call Routing Test** verifies the routing for a particular source and destination. To run the routing test, expand **Elements → Session Manager → System Tools → Call Routing Test**. A screen such as the following is displayed.

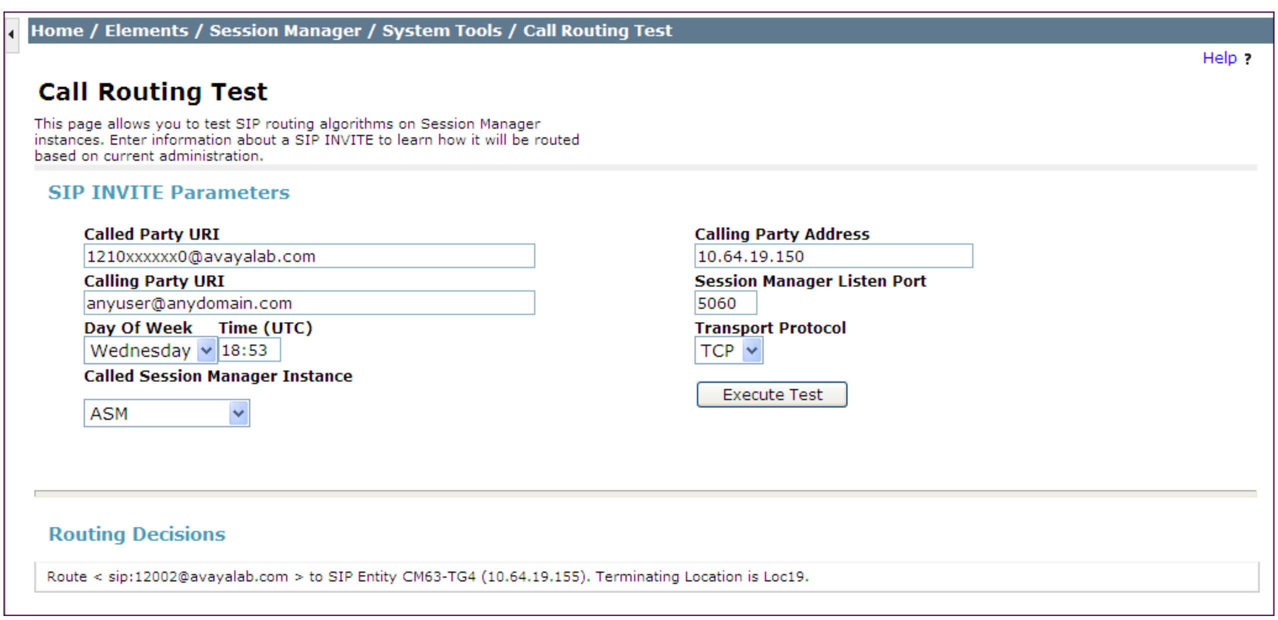


©2013 Avaya Inc. All Rights Reserved.

Populate the fields for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to the PSTN via Voxox. Under **Routing Decisions**, observe that the call will route via an Acme Packet SBC on the path to Voxox. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



Another example shows an inbound call to one of Voxox assigned DID numbers. Observe that the DID number 1210xxxxxx0 has been converted to Communication Manager extension 12002 under **Routing Decisions** and will be routed to Communication Manager.



©2013 Avaya Inc. All Rights Reserved.

9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Acme Packet Net-Net 3800[2] can be configured to interoperate successfully with Voxox SIP Trunk service. This solution allows Avaya Aura® Communication Manager and Avaya Aura® Session Manager users access to the PSTN using a Voxox public SIP trunk service connection.

10. 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] *Implementing Avaya Aura® Communication Manager*, Doc ID 03-603558, Release 6.3
[2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, Release 6.3
[3] *Implementing Avaya Aura® Session Manager*, Release 6.3
[4] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3
[5] *Upgrading Avaya Aura® Session Manager,* Release 6.3
[6] *Maintaining and Troubleshooting Avaya Aura® Session Manager,* Release 6.3
[7] *Implementing Avaya Aura® System Manager*, Release 6.3
[8] *Acme Packet, "S-Cx6.4.0 ACLI Configuration Guide",* 400-0061-64, Aug 2013
[9] *Acme Packet, "BCP, SIP Trunking Configuration for Enterprise",* 520-0046-00, Nov 2011
[10] *Acme Packet, "Net-Net 3820 Hardware Installation Guide",* 400-0134-10, Mar 2011
[11] *RFC 3261, SIP: Session Initiation Protocol. http://www.ietf.org/*

[2] Although an Acme Net-Net 3800 was used in the reference configuration, the 4250 and 4500 platforms are also supported.

©2013 Avaya Inc. All Rights Reserved.

Appendix A: Acme Packet Configuration File

Included below is the Acme Packet SBC 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 SBC.

```
ACMESYSTEM# show running-config
codec-policy
      name                          prefer-G729
      allow-codecs                  *
      order-codecs                  G729
      last-modified-by              admin@10.80.150.50
      last-modified-date            2013-09-06 13:56:14
codec-policy
        name                        prefer-PCMU
        allow-codecs                *
        order-codecs                PCMU
        last-modified-by            admin@10.80.150.50
        last-modified-date          2013-09-09 17:00:17
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@10.80.150.50
      last-modified-date            2013-08-19 18:18:54
      policy-attribute
            next-hop                      10.64.19.226
            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
```


©2013 Avaya Inc. All Rights Reserved.

```
                               *
      source-realm
                               core
      description
      activate-time            N/A
      deactivate-time          N/A
      state                    enabled
      policy-priority          none
      last-modified-by         admin@10.80.150.50
      last-modified-date       2013-08-19 16:50:24
      policy-attribute
            next-hop                 192.168.183.13
            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
      trap-on-demote-to-untrusted    disabled
      syslog-on-demote-to-untrusted  disabled
```


©2013 Avaya Inc. All Rights Reserved.

```
      anonymous-sdp                  disabled
      arp-msg-bandwidth              32000
      fragment-msg-bandwidth         0
      rfc2833-timestamp              disabled
      default-2833-duration          100
      rfc2833-end-pkts-only-for-non-sig enabled
      translate-non-rfc2833-event    disabled
      media-supervision-traps        disabled
      dnsalg-server-failover         disabled
      last-modified-by               admin@10.80.150.50
      last-modified-date             2013-08-23 12:39:34
network-interface
      name                           M00
      sub-port-id                    0
      description                    PUBLIC
      hostname
      ip-address                     192.168.62.123
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.128
      gateway                        192.168.62.1
      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                    192.168.62.123
      ftp-address
        icmp-address                   192.168.62.123
      snmp-address
      telnet-address
      ssh-address
      signaling-mtu                  0
      last-modified-by               admin@10.80.150.50
      last-modified-date             2012-06-06 14:40:39
network-interface
      name                           M10
      sub-port-id                    0
      description                    PRIVATE
      hostname
      ip-address                     10.64.19.150
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.0
      gateway                        10.64.19.1
      sec-gateway
      gw-heartbeat
            state                          disabled
            heartbeat                      0
            retry-count                    0
```


©2013 Avaya Inc. All Rights Reserved.

```
            retry-timeout                  1
            health-score                   0
      dns-ip-primary                10.80.150.201
      dns-ip-backup1
      dns-ip-backup2
      dns-domain                    avayalab.com
      dns-timeout                   11
        hip-ip-list                   10.64.19.150
                                      10.64.19.151
      ftp-address
        icmp-address                  10.64.19.150
                                      10.64.19.151
      snmp-address
      telnet-address
      ssh-address
      signaling-mtu                 0
      last-modified-by              admin@10.80.150.50
      last-modified-date            2013-09-11 19:14:05
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
```


©2013 Avaya Inc. All Rights Reserved.

```
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
srtp-msm-passthrough            disabled
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
max-endpoints-per-nat           0
nat-invalid-message-threshold   0
wait-time-for-invalid-register  0
deny-period                     30
cac-failure-threshold           0
untrust-cac-failure-threshold   0
ext-policy-svr
diam-e2-address-realm
symmetric-latching              disabled
pai-strip                       disabled
trunk-context
early-media-allow
enforcement-profile
additional-prefixes
restricted-latching             none
restriction-mask                32
accounting-enable               enabled
user-cac-mode                   none
user-cac-bandwidth              0
user-cac-sessions               0
icmp-detect-multiplier          0
icmp-advertisement-interval     0
icmp-target-ip
monthly-minutes                 0
net-management-control          disabled
delay-media-update              disabled
refer-call-transfer             disabled
refer-notify-provisional        none
dyn-refer-term                  disabled
codec-policy                    prefer-G729
codec-manip-in-realm            disabled
```


©2013 Avaya Inc. All Rights Reserved.

```
        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
        tcp-media-profile
        subscription-id-type            END_USER_NONE
        alt-family-realm
        pref-network-type               none
        last-modified-by                admin@10.80.150.50
        last-modified-date              2013-09-10 14:29:44
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
        srtp-msm-passthrough            disabled
        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
```


©2013 Avaya Inc. All Rights Reserved.

```
      maximum-signal-threshold       0
      untrusted-signal-threshold     0
      nat-trust-threshold            0
      max-endpoints-per-nat          0
      nat-invalid-message-threshold  0
      wait-time-for-invalid-register 0
      deny-period                    30
      cac-failure-threshold          0
      untrust-cac-failure-threshold  0
      ext-policy-svr
      diam-e2-address-realm
      symmetric-latching             disabled
      pai-strip                      disabled
      trunk-context
      early-media-allow
      enforcement-profile
      additional-prefixes
      restricted-latching            none
      restriction-mask               32
      accounting-enable              enabled
      user-cac-mode                  none
      user-cac-bandwidth             0
      user-cac-sessions              0
      icmp-detect-multiplier         0
      icmp-advertisement-interval    0
      icmp-target-ip
      monthly-minutes                0
      net-management-control         disabled
      delay-media-update             disabled
      refer-call-transfer            disabled
      refer-notify-provisional       none
      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
      tcp-media-profile
      subscription-id-type           END_USER_NONE
      alt-family-realm
      pref-network-type              none
      last-modified-by               admin@10.80.150.50
      last-modified-date             2013-09-10 14:29:55
session-agent
      hostname                       10.64.19.226
```


©2013 Avaya Inc. All Rights Reserved.

```
ip-address                    10.64.19.226
port                          5060
state                         enabled
app-protocol                  SIP
app-type
transport-method              UDP+TCP
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
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
load-balance-dns-query        hunt
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
```


©2013 Avaya Inc. All Rights Reserved.

```
      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
      refer-notify-provisional       none
      reuse-connections              NONE
      tcp-keepalive                  none
      tcp-reconn-interval            0
      max-register-burst-rate        0
      register-burst-window          0
      sip-profile
      sip-isup-profile
      kpml-interworking              inherit
      last-modified-by               admin@10.80.150.50
      last-modified-date             2013-08-19 18:11:47
session-agent
      hostname                       192.168.183.13
      ip-address                     192.168.183.13
      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
```


©2013 Avaya Inc. All Rights Reserved.

```
      ping-send-mode                keep-alive
      ping-all-addresses            disabled
      ping-in-service-response-codes
      out-service-response-codes
      load-balance-dns-query        hunt
      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
      refer-notify-provisional      none
      reuse-connections             NONE
      tcp-keepalive                 none
      tcp-reconn-interval           0
      max-register-burst-rate       0
      register-burst-window         0
      sip-profile
      sip-isup-profile
      kpml-interworking             inherit
      last-modified-by              admin@10.80.150.50
      last-modified-date            2013-09-06 09:55:51
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
      initial-inv-trans-expire      0
      invite-expire                 180
      inactive-dynamic-conn         32
```


©2013 Avaya Inc. All Rights Reserved.

```
      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
      extra-enum-stats               disabled
      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
      allow-pani-for-trusted-only    disabled
      pass-gruu-contact              disabled
      sag-lookup-on-redirect         disabled
      set-disconnect-time-on-bye     disabled
      msrp-delayed-bye-timer         15
      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                        192.168.62.123
            port                           5060
            transport-protocol             UDP
            tls-profile
            multi-home-addrs
            allow-anonymous                agents-only
            ims-aka-profile
      carriers
      trans-expire                   0
      initial-inv-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
```


©2013 Avaya Inc. All Rights Reserved.

```
      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
      subscribe-reg-event             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                    preferred
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                 disabled
      enforcement-profile
      route-unauthorized-calls
      tcp-keepalive                   none
      add-sdp-invite                  reinvite
      add-sdp-profiles
      sip-profile
      sip-isup-profile
      tcp-conn-dereg                  0
      register-keep-alive             none
      kpml-interworking               disabled
      tunnel-name
      msrp-delay-egress-bye           disabled
      send-380-response
      session-timer-profile
      last-modified-by                admin@10.80.150.50
      last-modified-date              2013-09-06 10:25:08
sip-interface
      state                           enabled
```


©2013 Avaya Inc. All Rights Reserved.

```
realm-id                       core
description
sip-port
      address                        10.64.19.150
      port                           5060
      transport-protocol             TCP
      tls-profile
      multi-home-addrs
      allow-anonymous                all
      ims-aka-profile
carriers
trans-expire                   0
initial-inv-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
subscribe-reg-event            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
```


©2013 Avaya Inc. All Rights Reserved.

```
      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
      tcp-conn-dereg                  0
      register-keep-alive             none
      kpml-interworking               disabled
      tunnel-name
      msrp-delay-egress-bye           disabled
      send-380-response
      session-timer-profile
      last-modified-by                admin@10.80.150.50
      last-modified-date              2013-08-26 11:07:32
sip-manipulation
      name                            NatIP
      description
      split-headers
      join-headers
      header-rule
            name                            natFROM
            header-name                     From
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods
            match-value
            new-value
            element-rule
                  name                            natHost
                  parameter-name
                  type                            uri-host
                  action                          replace
                  match-val-type                  any
                  comparison-type                 case-sensitive
                  match-value
                  new-value                       $LOCAL_IP
      header-rule
            name                            natTO
            header-name                     To
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods
            match-value
            new-value
            element-rule
                  name                            natHost
                  parameter-name
```


©2013 Avaya Inc. All Rights Reserved.

```
            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                            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                            RmEndpointView
        header-name                     Endpoint-View
        action                          delete
        comparison-type                 case-sensitive
        msg-type                        any
        methods
        match-value
        new-value
    last-modified-by                admin@10.80.150.50
    last-modified-date              2013-09-06 09:18:04
sip-manipulation
    name                            AddDomain
    description
    split-headers
```


©2013 Avaya Inc. All Rights Reserved.

```
join-headers
header-rule
      name                            FromDomain
      header-name                     From
      action                          manipulate
      comparison-type                 case-sensitive
      msg-type                        request
      methods
      match-value
      new-value
      element-rule
            name                            From
            parameter-name
            type                            uri-host
            action                          replace
            match-val-type                  any
            comparison-type                 case-sensitive
            match-value
            new-value                       avayalab.com
header-rule
      name                            PaiDomain
      header-name                     P-Asserted-Identity
      action                          manipulate
      comparison-type                 case-sensitive
      msg-type                        request
      methods
      match-value
      new-value
      element-rule
            name                            Pai
            parameter-name
            type                            uri-host
            action                          replace
            match-val-type                  any
            comparison-type                 case-sensitive
            match-value
            new-value                       avayalab.com
header-rule
      name                            natTO
      header-name                     To
      action                          manipulate
      comparison-type                 case-sensitive
      msg-type                        request
      methods
      match-value
      new-value
      element-rule
            name                            To
            parameter-name
            type                            uri-host
            action                          replace
            match-val-type                  any
            comparison-type                 case-sensitive
            match-value
            new-value                       $REMOTE_IP
last-modified-by                admin@10.80.150.50
last-modified-date              2012-06-21 12:09:39
```


©2013 Avaya Inc. All Rights Reserved.

```
steering-pool
      ip-address                    192.168.62.123
      start-port                    49152
      end-port                      65535
      realm-id                      peer
      network-interface
      last-modified-by              admin@10.80.150.50
      last-modified-date            2012-06-06 15:07:34
steering-pool
      ip-address                    10.64.19.150
      start-port                    49152
      end-port                      65535
      realm-id                      core
      network-interface
      last-modified-by              admin@10.80.150.50
      last-modified-date            2012-06-06 15:08:02
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
```


©2013 Avaya Inc. All Rights Reserved.

```
      cli-more                      disabled
      terminal-height               24
      debug-timeout                 0
      trap-event-lifetime           0
      default-v6-gateway            ::
      ipv6-signaling-mtu            1500
      ipv4-signaling-mtu            1500
      cleanup-time-of-day           00:00
      snmp-engine-id-suffix
      snmp-agent-mode               v1v2
      comm-monitor
            state                         disabled
            qos-enable                    enabled
            sbc-grp-id                    0
            tls-profile
      last-modified-by              admin@console
      last-modified-date            2011-11-01 10:30:52
task done
```


©2013 Avaya Inc. All Rights Reserved.

©2013 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.