Avaya Solution & Interoperability Test Lab

Application Notes for Configuring TELUS SIP Trunking with Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Acme Packet 3800 Net-Net Session Border Controller – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TELUS SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

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

Table of Contents

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TELUS SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

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

2. General Test Approach and Test Results

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

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

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator can place calls from the local computer or control a separate physical phone. Both of these modes were tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP.
- Inbound and outbound calls to/from TELUS Derived Voice endpoints (SIP).
- Inbound and outbound calls to/from TELUS Mobility endpoints.
- Various call types including: local, long distance, international, outbound toll-free, operator, operator assisted calls, and local directory assistance (411).

- G.711MU and G.729A codecs.
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls
- Voicemail Message Waiting Indicator (MWI)
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call transfer, conference, forwarding and enterprise mobility (extension to cellular)
- T.38 Fax

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested.
- Call redirection requested by a 302 response is not supported by TELUS.
- REFER is not supported by TELUS.

2.2. Test Results

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

- **OPTIONS Max-Forwards Value**: TELUS requires that SIP OPTIONS messages sent from the enterprise contain a Max-Forwards value of zero. These messages originate from Session Manager with a non-zero Max-Forwards value when link monitoring is enabled on Session Manager. Thus, the 3800 Net-Net SBC was used to modify this value when the SBC sent the OPTIONS message to the network (see **Section 7.10.3.17**). The SBC can also be configured to originate its own OPTIONS message to the network with Max-Forward set to zero. See the **ping-method** setting in **Section 7.8.1**. This was done as part of the compliance test but it was optional since Session Manager was sending OPTIONS message to determine link status.
- **Session Refresh Time**: The Communication Manager SIP trunk parameter **Preferred Minimum Session Refresh Interval (sec)** on both internal SIP trunk and service provider SIP trunk must be set to at least 900 seconds. Otherwise outbound INVITE would receive response "422 Session Interval Too Small" from TELUS.
- **Use of SA8965**: TELUS requires re-INVITEs to contain Session Description Protocol (SDP) information. Thus, the Communication Manager special application SA8965 must be enabled (see **Section 5.2**). Even with SA8965 enabled, some call scenarios involving enterprise SIP endpoints still resulted in some re-INVITEs without SDP. These calls still completed with no impact to the user. These scenarios included inbound calls that were attended transferred back to the service provider by a SIP endpoint and conferencing of multiple PSTN calls by a SIP endpoint.
- **G.729A Codec**: Though G.729 codec was tested during the compliance test successfully for outbound calls, not all media gateways in the TELUS network support G.729A.

TELUS SIP Tunking officially supports G.711MU only. For inbound call INVITE from TELUS, its SDP specifies only G.711MU.

- **Call Fowarding and EC500**: For inbound PSTN calls that were forwarded back to the PSTN or ring to an EC500 (enterprise mobility) PSTN endpoint, the PSTN destination phone display (if equipped) showed the forwarding party/EC500 host instead of the original PSTN caller. This is the result of differences in the interpretation/implementation of the SIP Diversion header between TELUS and Communication Manager. For the compliance test, a SIP header manipulation was created on the 3800 Net-Net SBC to modify the P-Asserted-Identity (PAI) header with information contained in the Diversion header received by the SBC from Session Manager (see **Sections 7.10.3.14** and **7.10.3.15**). This allowed the call to complete but resulted in the incorrect calling party displayed at the destination as described above.
- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone was not updated to reflect the true connected party on calls that were transferred to the PSTN. After the call transfer was complete, the calling party number displayed the number of the transferring party and not the actual connected party. Communication Manager provides the new connected party information by updating the Contact header in a re-INVITE message in this call scenario. TELUS does not use the updated Contact header for displaying calling party information.
- **T.38 Fax – Network Coverage**: Not all media gateways in the TELUS network support T.38 fax. Communication Manager does not support fallback to G.711 pass-through fax from T.38 fax. Thus, if a T.38 fax call encounters a media gateway in the TELUS network that does not support T.38 then the call will terminate.
- **Transitioning to T.38 for Outbound Calls**: In general, the answering side of a fax call will send a re-INVITE to transition to T.38. For outbound fax calls to the PSTN, this means the network would typically send the re-INVITE to transition to T.38. However, TELUS requires Communication Manager to transition to T.38 for both inbound and outbound fax calls. Relying on Communication Manager to transition to T.38 on an outbound call may have the following impact:
  - On an outbound call, sending of the T.38 INVITE happens on detection of the V.21 preamble of the originating fax machine’s Digital Command Signal (DCS) message. This is part of the T.30 exchange. This request to transition to T.38 may happen too late for some terminating gateways to accommodate the switch to T.38.
  - If the initial call is using the G.729 codec, the compression of the V.21 preamble may cause its detection to be less reliable than if the call was initially using G.711.
  - The ability to transition to T.38 in the middle of the T.30 exchange is supported on the following Avaya media platforms (G430/G450/TN2602). Older platforms (G350/G700/TN2302) may have different behavior.

  The compliance testing was conducted with the G450 media gateway using the G.711MU codec to initially establish the call. Outbound T.38 fax calls in this environment were successful.
- **G.711 Pass-through Fax**: Communication Manager does not support G.711 pass-through fax over SIP trunks. These calls are treated like any other voice call by Communication Manager. If a customer chooses to use G.711 pass-through fax, success is not guaranteed.

- **Call Termination by TELUS Derived Voice and Mobility Endpoints**: When a TELUS Derived Voice endpoint terminated a call with an enterprise phone, TELUS failed to send BYE to the enterprise causing the terminated call to stay up at the enterprise phone. Same failure was observed intermittently with TELUS mobility endpoints. This problem did not happen in past compliance tests with earlier versions of Communication Manager and Session Manager. TELUS is investigating.
- **Avaya one-X® Communicator SIP and "Other Phone" Mode**: In this mode, an outbound call is issued to the associated "Other Phone" when 1XC initiates/receives a call so that 1XC controls the call but voice media is to/from the physical "Other Phone". When Communication Manager placed the call to the "Other Phone", the call was rejected with a 500 Server Error from the TELUS network. It was rejected because the initial INVITE from Communication Manager included a PAI header containing the enterprise extension instead of the DID number for that station. For the compliance test, a Session Manager Adaptation for the 3800 Net-Net SBC SIP Entity was configured to convert Communication Manager extension number to the associated DID number for populating the PAI header (see **Section 6.4**). This Session Manager configuration is only needed for 1XC in SIP Mode since 1XC in H.323 Mode populates the outbound INVITE PAI header properly.
- **Off-net Transfer from one-X® Communicator SIP** – 1XC softphone in SIP Mode failed in transferring an existing call with PSTN back out to PSTN by using the Transfer button directly. TELUS would respond to the transfer INVITE from the enterprise with a "500 Internal Server Error" message indicating caller authentication failure. This failure was caused by the 1XC PAI header containing the existing PSTN connected-party number, not the expected DID associated with the extension. This problem only exists with 1XC in SIP Mode. 1XC in H.323 Mode correctly carries the assigned DID in the PAI header of outbound INVITE. This problem was worked around during the compliance test by making a separate call to the transfer destination first before transferring the original call.
- **Conference from one-X® Communicator SIP** –Direct use of the Conference button on 1XC softphone in SIP Mode for 3-party conference will cause loss of audio sometimes. This problem was worked around during the compliance test by making a separate call to the conference destination first before completing the conference operation.

2.3. Support

For technical support on the TELUS system, please contact your TELUS Account Executive or visit http://telus.com.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

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

For security purposes, any actual public IP addresses used in the compliance test were changed to 192.168.x.x throughout these Application Notes where the 3rd and 4th octets were retained from the real addresses.

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

- HP Proliant DL360G7 Server running Avaya Aura® Solution for Midsize Enterprise 6.2 that includes
  - Communication Manager
  - Session Manager
  - System Manager
  - Communication Manager Messaging
- Avaya G450 Media Gateway
- Acme Packet 3800 Net-Net Session Border Controller
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya 96x1-Series IP Telephones (H.323 and SIP)
- Avaya 9601 IP Telephone (SIP) which uses different firmware than other Avaya 96x1-Series IP Telephones
- Avaya A175 Desktop Video Device a.k.a. Flare (used as a SIP voice endpoint)
- Avaya one-X® Communicator soft phones (H.323 and SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Acme Packet 3800 Net-Net SBC. It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the 3800 Net-Net SBC. In this way, the 3800 Net-Net SBC can protect the enterprise against any SIP-based attacks. The 3800 Net-Net SBC provides network address translation at both the IP and SIP layers.

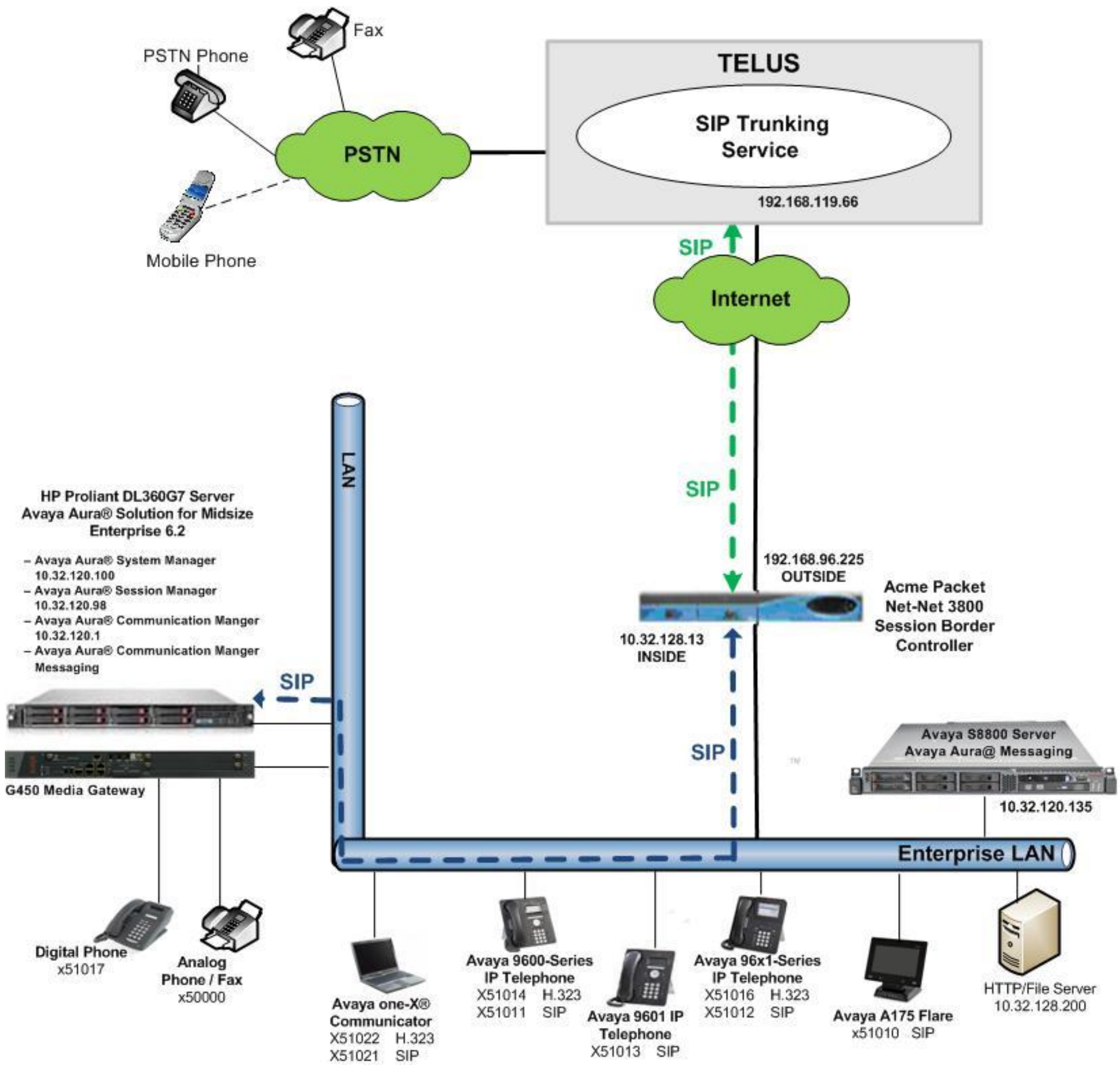


Figure 1: Avaya IP Telephony Network using TELUS SIP Trunking

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

Inbound calls flow from the service provider to the 3800 Net-Net SBC then to Session Manager. Session Manager uses the configured Dial Patterns (or regular expressions) and Routing Policies to determine the recipient (in this case the Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features treatment such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. The Session Manager once again uses the configured Dial Patterns (or regular expressions) and Routing Policies to determine the route to the 3800 Net-Net SBC. From the 3800 Net-Net SBC, the call is sent to TELUS SIP Trunking.

For outbound calls, the enterprise was configured to send 11 digits in the SIP destination headers (Request-URI and To) and 10 digits in the SIP source headers (i.e., From, Contact, and P-Asserted-Identity). For inbound calls, TELUS sent 10 digits in both the source headers and destination headers.

The compliance test used Communication Manager Messaging for testing voice mail access/navigation and MWI (Messaging Wait Indicator) on Avaya enterprise phones. Communication Manager Messaging was chosen since Avaya Aura® Solution for Midsize Enterprise 6.2 includes this voice messaging component. Other voice messaging applications such as Avaya Aura® Messaging (as depicted in **Figure 1**) could have been used to satisfy this test purpose.

The administration of Communication Manager Messaging and endpoints on Communication Manager and Session Manager are standard. Since the configuration tasks for Communication Manager Messaging and endpoints are not directly related to the inter-operation with TELUS SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	**Release/Version**
Avaya Aura® Solution for Midsize Enterprise 6.2 running on HP Proliant DL360G7 Server • Avaya Aura® Communication Manager • Avaya Aura® Communication Manager Messaging • Avaya Aura® Session Manager • Avaya Aura® System Manager	 6.2 (R016x.02.0.823.0-19883) 6.2-22.0 (CMM-02.0.823.0-0002) 6.2.2.0.622005 6.2.0-SP2 (6.2.14.1.1925)
Avaya G450 Media Gateway	31.22.0 /1
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1 SP4
Avaya 9620 IP Telephone (SIP)	Avaya one-X® Deskphone SIP Edition 2.6.8.4
Avaya 9611 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.2.1
Avaya 9621 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.0 SP4
Avaya 9601 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.1 SP4
Avaya A175 Desktop Video Device	1.1.0
Avaya one-X® Communicator	6.1.5.07-SP5-37405
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Acme Packet 3800 Net-Net Session Border Controller	SCX6.2.0 MR-3 GA (Build 619)
TELUS SIP Trunking Solution Components	
Equipment/Software	**Release/Version**
Acme Packet 4520 Net-Net Session Border Controller	6.1m7p5
Nokia Siemens Networks HiQ 4200	Version 14.0

Table 1: Equipment and Software Tested

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for TELUS SIP Trunking. It is assumed the general installation of Communication Manager, Avaya Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 12000 SIP trunks are available and 275 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 128   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 2
                       Maximum Administered SIP Trunks: 12000 275
  Maximum Administered Ad-hoc Video Conferencing Ports: 12000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Special Application SA8965

TELUS requires that all INVITE messages contain SDP information, including re-INVITEs. In general, when Communication Manager sends a re-INVITE to perform a media shuffling operation (to redirect media directly between two endpoints) the re-INVITE will not include SDP information. In order to change this behavior, special application SA8965 must be enabled. This is done via the **change system-parameters special-applications** command. Navigate to **Page 7** and enter ***y*** next to the special application titled **SA8965 - SIP Shuffling with SDP** in the list below. By enabling this feature, a new protocol variation parameter will appear on **Page 4** of the trunk form (see **Section 5.8**).

```
change system-parameters special-applications                  Page   7 of   9
                             SPECIAL APPLICATIONS

                       (SA8888) - Per Station Music On Hold? n
    (SA8889) - Verizon VoiceGenie SIP MIME Message Bodies? n
                  (SA8891) - Verizon VoiceGenie SIP Headers? n
                                (SA8893) - Blast Conference? n
                       (SA8896) - IP Softphone Lamp Control? n
                  (SA8900) - Support for NTT Call Screening? n
               (SA8904) - Location Based Call Type Analysis? n
                   (SA8911) - Expanded Public Unknown Table? n
     (SA8917) - LSP Redirect using special coverage point? n
                          (SA8927) - Increase Paging Groups? n
    (SA8928) - Display Names on Bridged Appearance Labels? n
             (SA8931) - Send IE with EC500 Extension Number? n
           (SA8942) - Multiple Unicode Message File Support? n
           (SA8944) - Multiple Logins for Single IP Address? n
                             (SA8946) - Site Data Expansion? n
 (SA8958) - Increase BSR Polling/Interflow Pairs to 40000? n
                          (SA8965) - SIP Shuffling with SDP? y
 (SA8967) - Mask CLI and Station Name for QSIG/ISDN Calls? n
```

5.3. System Features

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

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

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

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

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

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

INTERNATIONAL CALL ROUTING PARAMETERS
                 Local Country Code: 1
          International Access Code: 011

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.4. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses for Communication Manager ***(procr***) and Session Manager (***SM***). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM                   10.32.120.98
default              0.0.0.0
nwk-aes1             10.32.120.3
procr                10.32.120.1
procr6               ::
```

5.5. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 5 was used for this purpose. TELUS SIP Trunking supports the G.711MU codec only. Thus, only ***G.711MU*** was included in this codec set. Default values can be used for all other fields.

```
change ip-codec-set 5                                             Page   1 of   2

                          IP Codec Set

    Codec Set: 5

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

On **Page 2**, to enable T.38 fax, set the **Fax Mode** to **t.38-standard**. Otherwise, set the Fax Mode to **off**.

```
change ip-codec-set 5                                             Page   2 of   2

                          IP Codec Set

                              Allow Direct-IP Multimedia? n



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

5.6. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 5 was chosen for the service provider trunk. Use the **change ip-network-region 5** command to configure region 5 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is ***sip.avaya.com***. This name appears in the From header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to ***yes*.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.5**.
- Default values can be used for all other fields.

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

On **Page 4**, define the IP codec set to be used for traffic between region 5 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 5 will be used for calls between region 5 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 5 will automatically create a complementary table entry on the IP network region 1 form for destination region 5. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4**.

```
change ip-network-region 5                                      Page   4 of  20

 Source Region: 5     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    5     y    NoLimit                                             n       t
 2
 3
 4
 5    5                                                                all
```

5.7. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 5 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value (for TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). This is necessary for Session Manager to distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5261***.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field will initially be set to ***Others*** and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to ***SM*** once Communication Manager detects its peer as a Session Manager.

- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of Communication Manager as defined in **Section 5.4**.
- Set the **Far-end Node Name** to ***SM*** This node name maps to the IP address of Session Manager as defined in **Section 5.4**
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to ***n***, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completion.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to ***15***. This defines the number of seconds the Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

```
add signaling-group 5                                           Page   1 of   2
                                SIGNALING GROUP

 Group Number: 5             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



        Near-end Node Name: procr                Far-end Node Name: SM
 Near-end Listen Port: 5261              Far-end Listen Port: 5261
                                      Far-end Network Region: 5
                                 Far-end Secondary Node Name:
Far-end Domain: sip.avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n          Alternate Route Timer(sec): 15
```

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**. For the compliance test, trunk group 5 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

```
add trunk-group 5                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 5                    Group Type: sip            CDR Reports: y
  Group Name: AC SP Trunk                 COR: 1        TN: 1        TAC: *05
   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: 5
                                                     Number of Members: 10
```

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value equal to the **Alternate Route Timer** on the signaling group form described in **Section 5.7**.

Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **900** seconds was used.

```
add trunk-group 5                                              Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 15000

            SCCAN? n                                 Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
```

On **Page 3**, set the **Numbering Format** field to ***private***. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to ***private*** and the **Numbering Format** field in the route pattern was set to ***unk-unk*** (see **Section 5.10**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to ***y***. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.3** if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if an enterprise user requests CPN block on a particular call routed out this trunk.. Default values were used for all other fields.

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



                     Numbering Format: private
                                                 UUI Treatment: service-provider

                                                  Replace Restricted Numbers? y
                                                 Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no


 Show ANSWERED BY on Display? y

 DSN Term? n
```

On **Page 4**, set the **Network Call Redirection** field to ***n***. Setting the **Network Call Redirection** flag to ***y*** enables use of the SIP REFER message (not supported by TELUS SIP Trunking) for call transfer; otherwise the SIP INVITE message will be used for call transfer as verified in the compliance test.

Set the **Send Diversion Header** field to ***y*** and the **Support Request History** field to ***n***. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

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

Set the **Shuffling with SDP** field to ***y***. This will instruct Communication Manager to send SDP information in shuffling re-INVITEs on calls that use this trunk. This parameter only appears if special application SA8965 is enabled. See **Section 5.2** for full details.

```
add trunk-group 5                                                Page   4 of  21
                              PROTOCOL VARIATIONS

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


            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
                                  Enable Q-SIP? n
```

Calls between the enterprise SIP endpoints and TELUS traverse two SIP trunks: the internal SIP trunk for intra-enterprise traffic (trunk 3 in the test configuration) and the service provider SIP trunk to TELUS (trunk 5 described above). In order for SA8965 to be properly applied to these calls, **Shuffling with SDP** must also be enabled on the internal SIP trunk used for SIP endpoints in addition to the trunk to TELUS shown above. Use the **change trunk-group** command to enable **Shuffling with SDP** (on **Page 4**) on the internal enterprise SIP trunk 3 as shown below.

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

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


            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
                                Enable Q-SIP? n
```

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (**Section 5.8**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

The screen below shows the set of DID numbers assigned for testing. These 4 numbers were mapped to the 4 enterprise extensions 51011, 51012, 51014 and 51021. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 4 extensions.

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

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
 0  attd                       0                1     Total Administered: 21
 5  1                                           5        Maximum Entries: 540
 5  2                                           5
 5  3                                           5
 5  4                                           5
 5  5                                           5
 5  6                                           5
 5  7                                           5
 5  8                                           5
 5  51011           5          4033850121       10
 5  51012           5          4033850122       10
 5  51014           5          4033850123       10
 5  51021           5          4033850124       10
```

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

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

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
 5  5                                            5    Total Administered: 10
 5  5                5          90633            10      Maximum Entries: 540
```

5.10. Outbound Routing

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

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

    Dialed   Total  Call     Dialed   Total  Call      Dialed   Total  Call
    String   Length Type     String   Length Type      String   Length Type
   0            1   attd
   1            5   ext
   2            5   ext
   3            5   ext
   4            5   ext
   5            5   ext
   6            5   ext
   7            5   ext
   8            5   ext
   9            1   fac
   *            3   dac
   #            3   dac
```

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

```
change feature-access-codes                                     Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *10
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *14
                      Announcement Access Code: *19
                       Answer Back Access Code:

      Auto Alternate Routing (AAR) Access Code: *00
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *33    Deactivation: #33
Call Forwarding Activation Busy/DA: *30    All: *31    Deactivation: #30
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *40
                       Call Pickup Access Code: *41
CAS Remote Hold/Answer Hold-Unhold Access Code: *42
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code: *80      Close Code: #80
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern *5*** which contains the SIP trunk to the service provider (as defined next).

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

          Dialed           Total     Route     Call    Node   ANI
          String          Min  Max  Pattern    Type    Num    Reqd
    0                     1    1     5         op             n
    0                     8    8     deny      op             n
    0                     11   11    5         op             n
    00                    2    2     deny      op             n
    01                    9    17    deny      iop            n
    011                   10   18    5         intl           n
    1732                  11   11    5         fnpa           n
    1800                  11   11    5         fnpa           n
    1877                  11   11    5         fnpa           n
    1908                  11   11    5         fnpa           n
    411                   3    3     5         svc1           n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern 5 for the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group ***5*** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: ***1*** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers.
- **Numbering Format**: Set this field to ***unk-unk*** since private Numbering Format should be used for this route (see **Section 5.8**).

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

6. Configure Avaya Aura® Session Manager

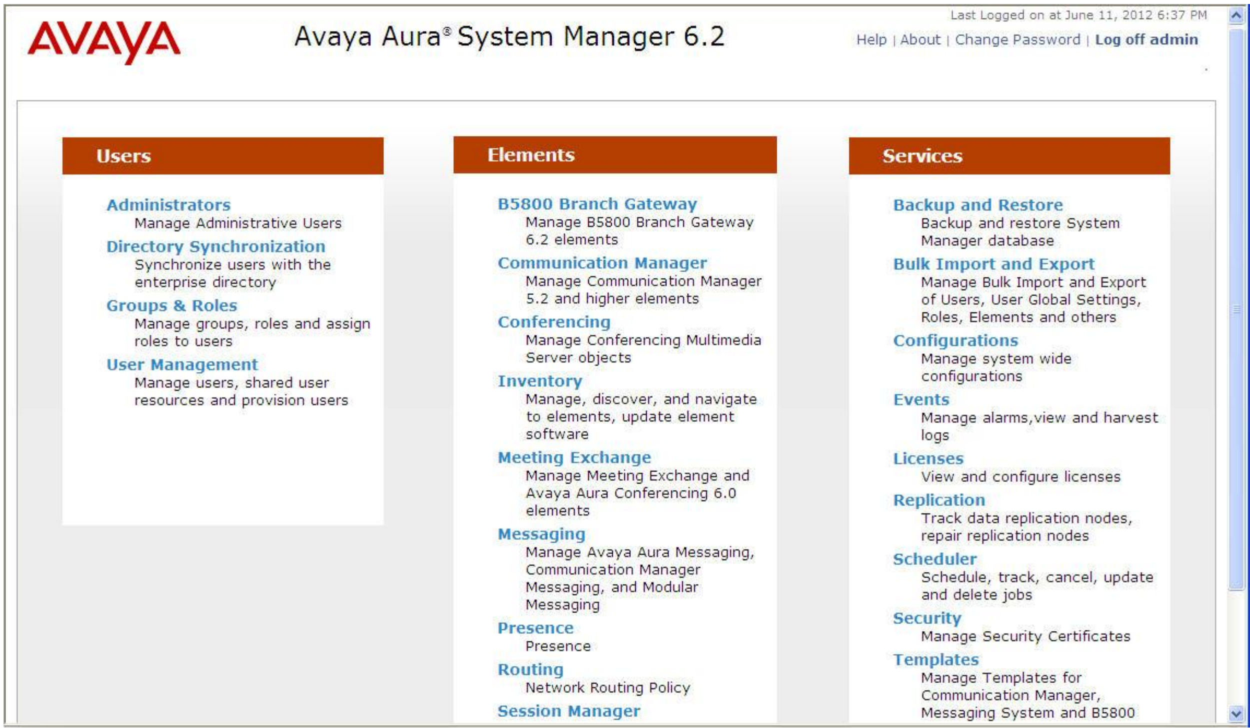
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to Communication Manager, the 3800 Net-Net SBC and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which define route destinations and control call routing between the SIP Entities.
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call.
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

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

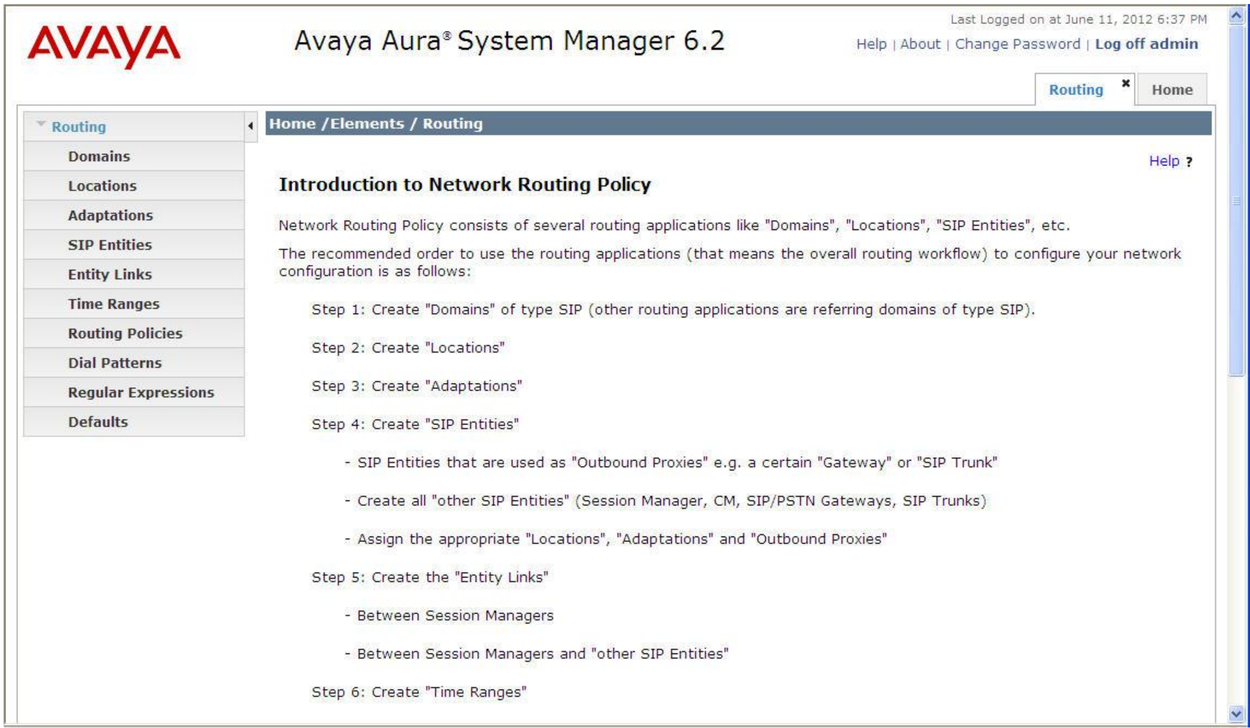
6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



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

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



6.2. Specify SIP Domain

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

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

Click **Commit**.

The screen below shows the entry for the enterprise domain.

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named ***Belleville***, which includes all equipment in the enterprise including Communication Manager, Session Manager and the 3800 Net-Net SBC.

To add a Location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

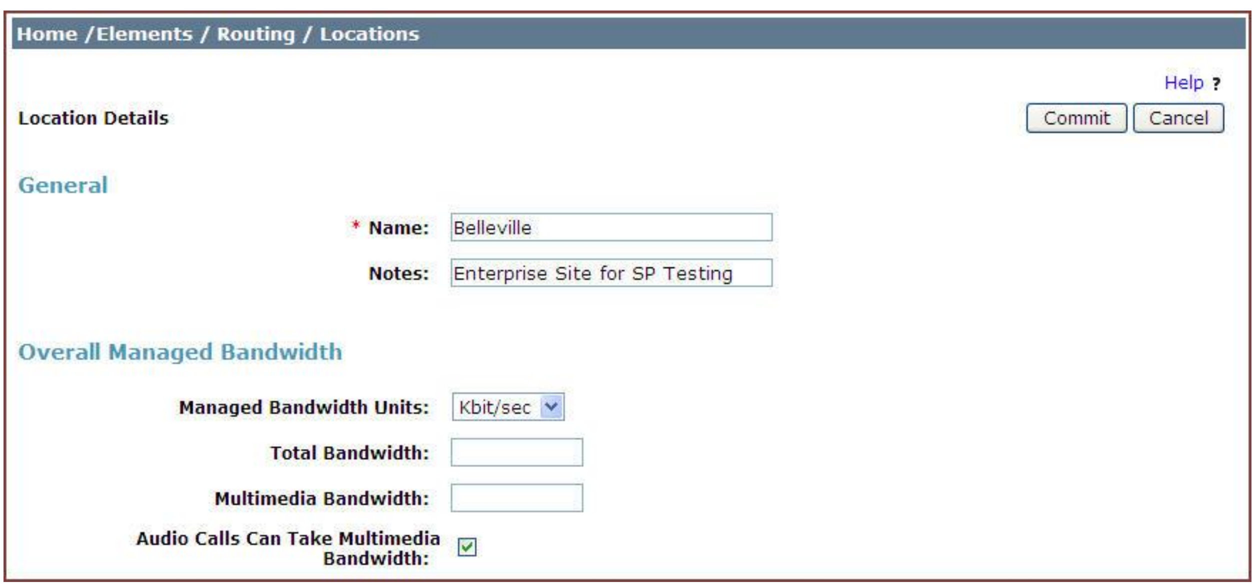
- **Name:** Enter a descriptive name for the Location.
- **Notes:** Add a brief description (optional).

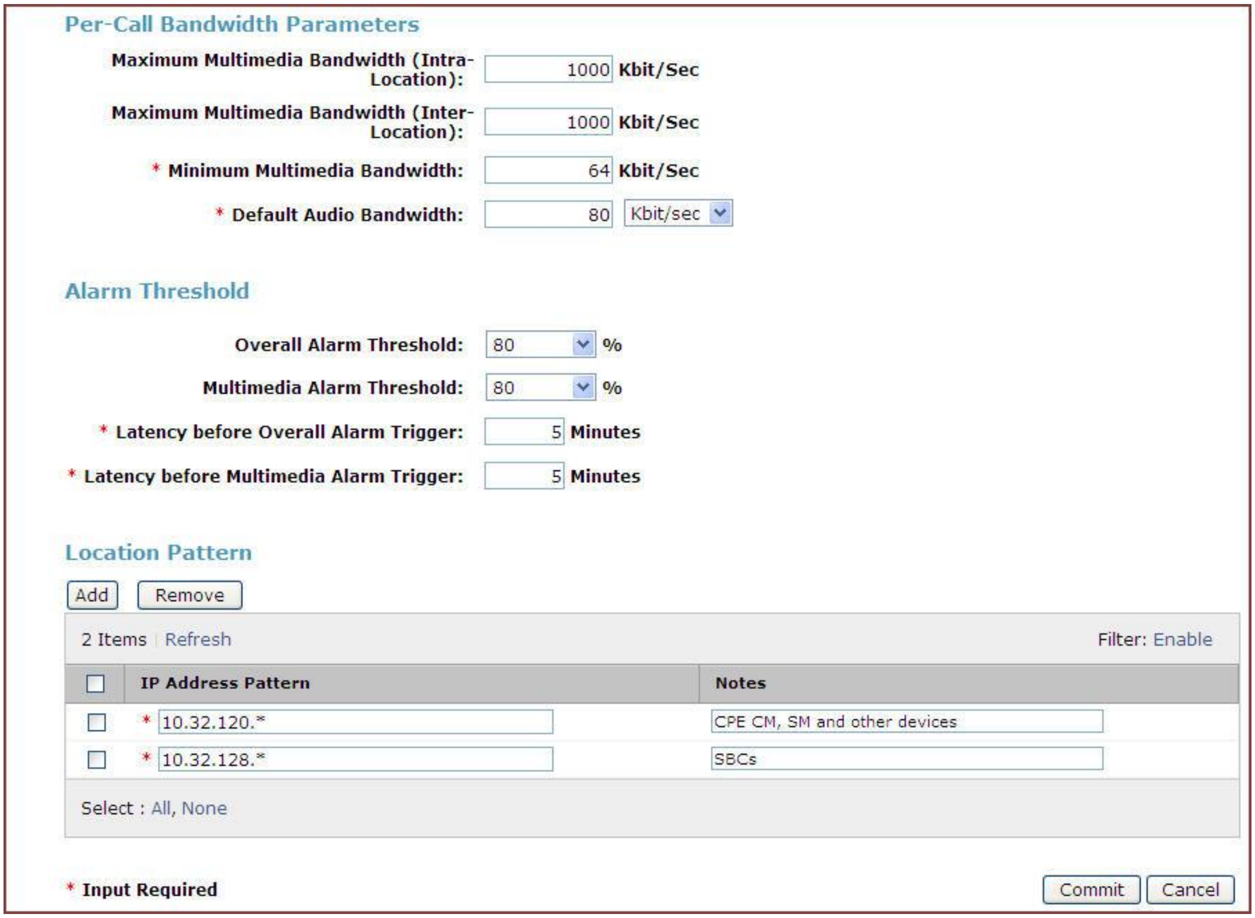
Scroll down to the **Location Pattern** section (see 2nd screen below), click **Add** and enter the following values:

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

Displayed below are the top and bottom halves of the screen for addition of the ***Belleville*** Location, which includes all equipment on the enterprise network.

Click **Commit** to save.





Note that call bandwidth management parameters should be set per customer requirement.

6.4. Add Adaptation Module

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

For the compliance test, two Adaptations were needed. The first Adaptation is applied to the Communication Manager SIP Entity and performs the following tasks:

- Converting the domain part of the inbound PAI header to the enterprise domain (**sip.avaya.com**).
- Mapping inbound DID numbers from TELUS to local Communication Manager extensions.

The second Adaptation is applied to the 3800 Net-Net SBC SIP Entity and performs the following tasks:

- Converting the domain part of the outbound Request-URI header from Session Manager containing the enterprise domain to the TELUS SIP proxy IP address.
- Mapping the internal extension number of the Avaya one-X® Communicator SIP softphone to the assigned DID number (see the **Avaya one-X® Communicator SIP and "Other Phone" Mode** item in the observation/limitation list in **Section 2.2** for details).

To create the adaptation that will be applied to the Communication Manager SIP Entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

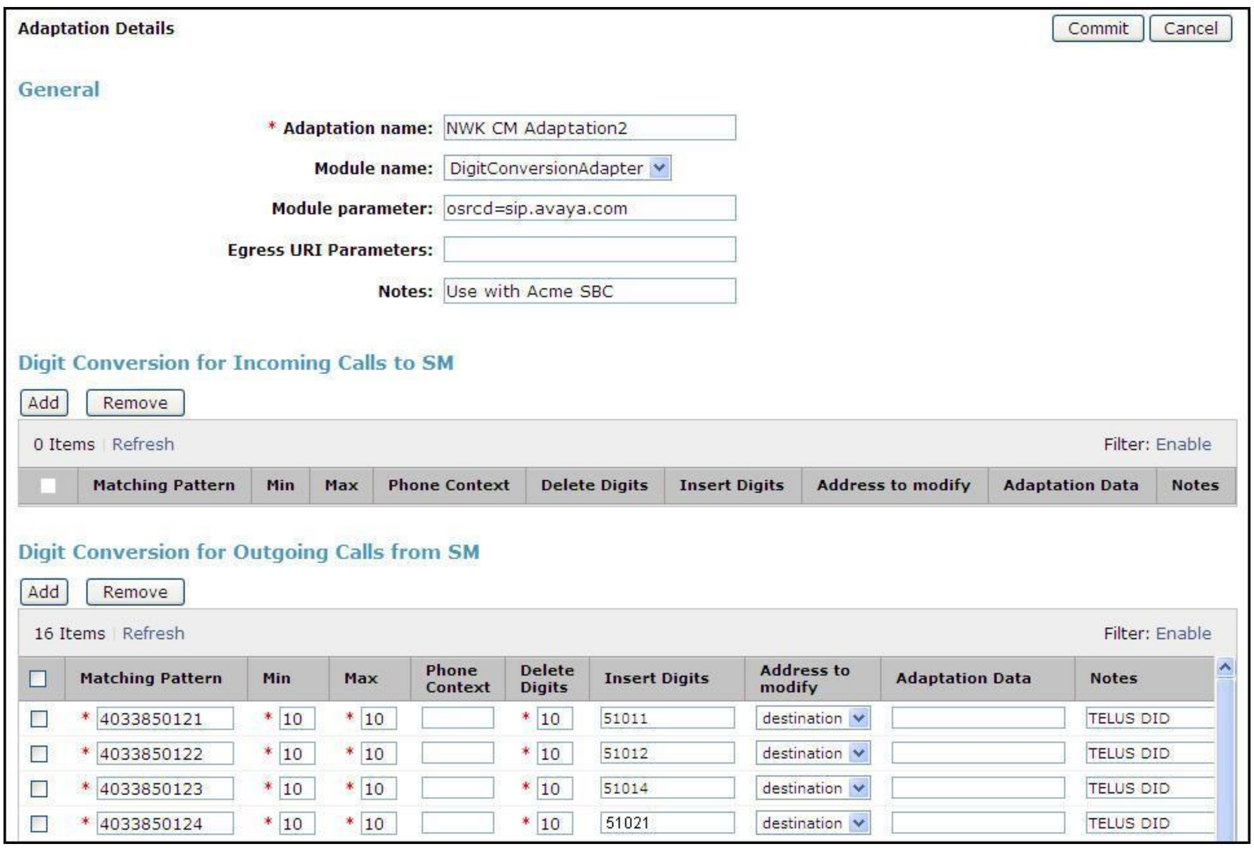
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation name:** Enter a descriptive name for the Adaptation.
- **Module name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***osrcd=sip.avaya.com***. This is the OverrideSourceDomain parameter. This parameter replaces the domain in the inbound PAI header with the given value. This parameter must match the value used for the **Far-end Domain** setting on the Communication Manager signaling group form in **Section 5.7**.

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

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

Click **Commit** to save.



To create the Adaptation that will be applied to the 3800 Net-Net SBC SIP Entity, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

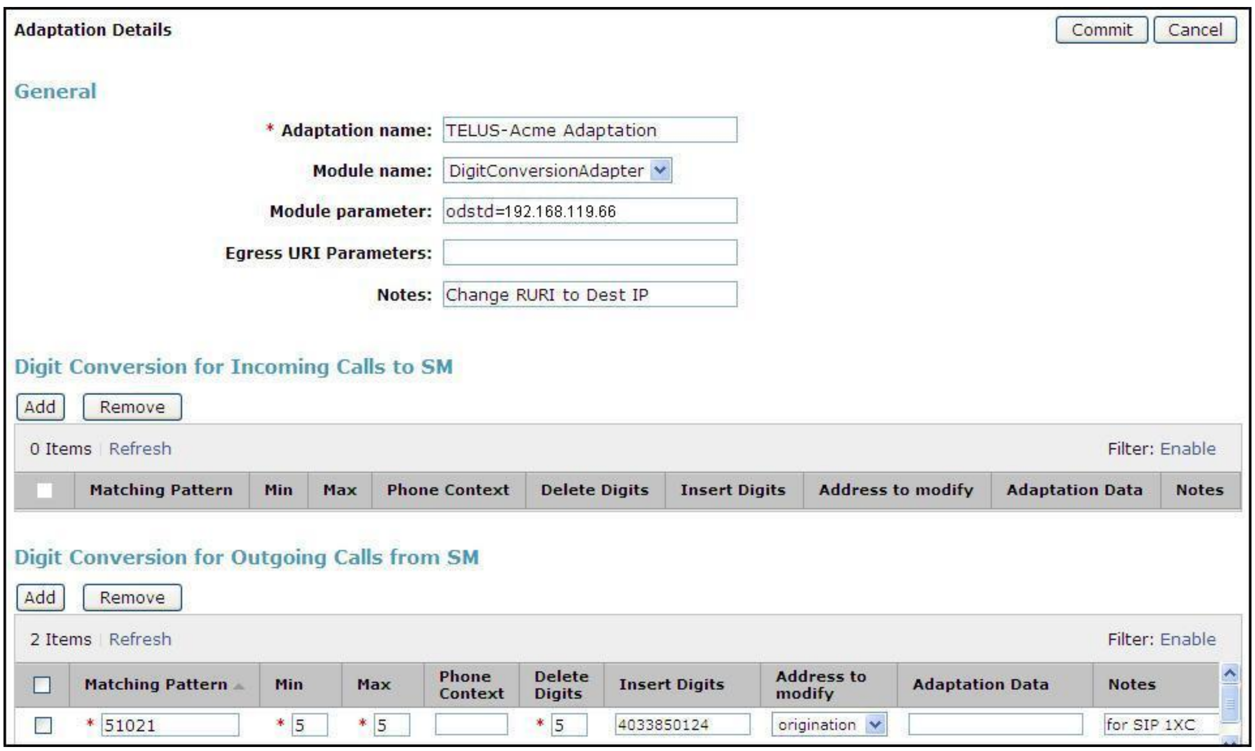
In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation name:** Enter a descriptive name for the Adaptation.
- **Module name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***odstd=192.168.119.66.*** This is the OverrideDestinationDomain parameter. This parameter replaces the domain in the Request-URI header with the given value for outbound calls only.
- **Notes:** Add a brief description (optional).

To map the Communication Manager extension number for the one-X® Communicator SIP softphone to the TELUS DID number assigned to the extension, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each 1XC SIP softphone extension to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields.

- **Matching Pattern:** Enter the 1XC SIP softphone extension.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the DID number assigned to the 1XC SIP softphone extension.
- **Address to modify:** Select ***origination*** since this digit conversion only applies to the origination number.

Click **Commit** to save.



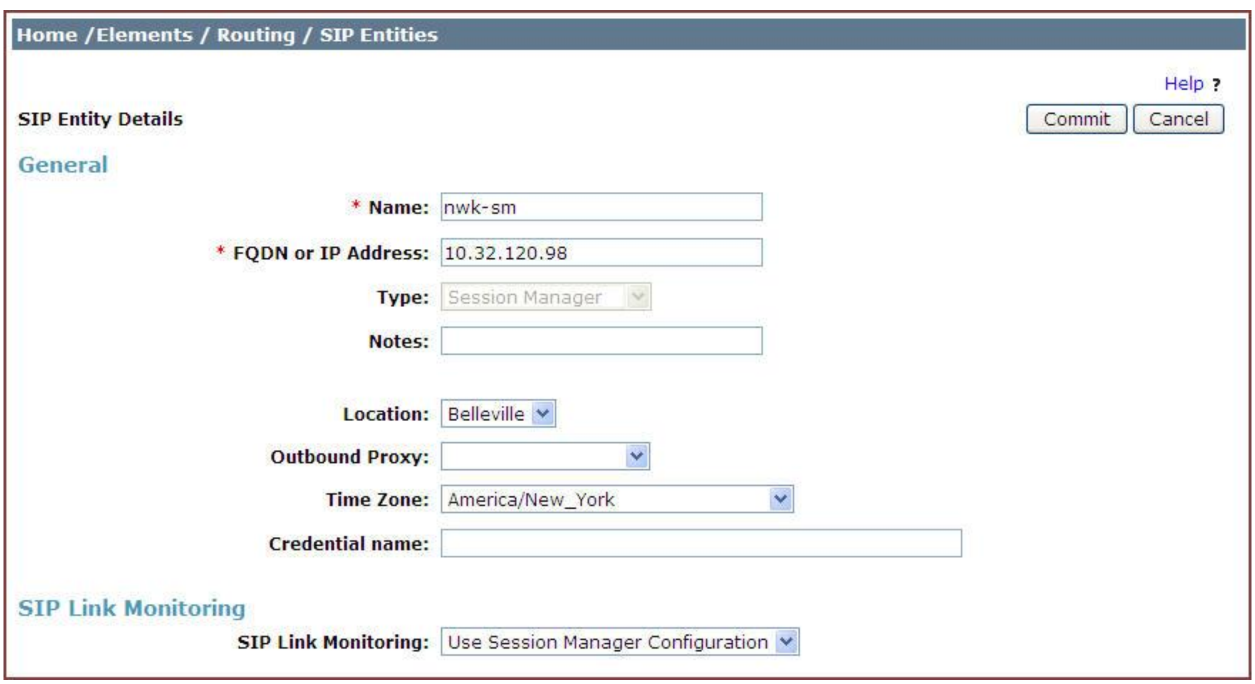
6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the 3800 Net-Net SBC. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** for the 3800 Net-Net SBC.
- **Adaptation:** This field is only present if **Type** is not set to ***Session Manager***. If applicable, select the appropriate Adaptation module created in **Section 6.4** that will be applied to the SIP Entity being created.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location ***Belleville***.
- **Time Zone:** Select the time zone for the Location above.

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



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

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

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

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

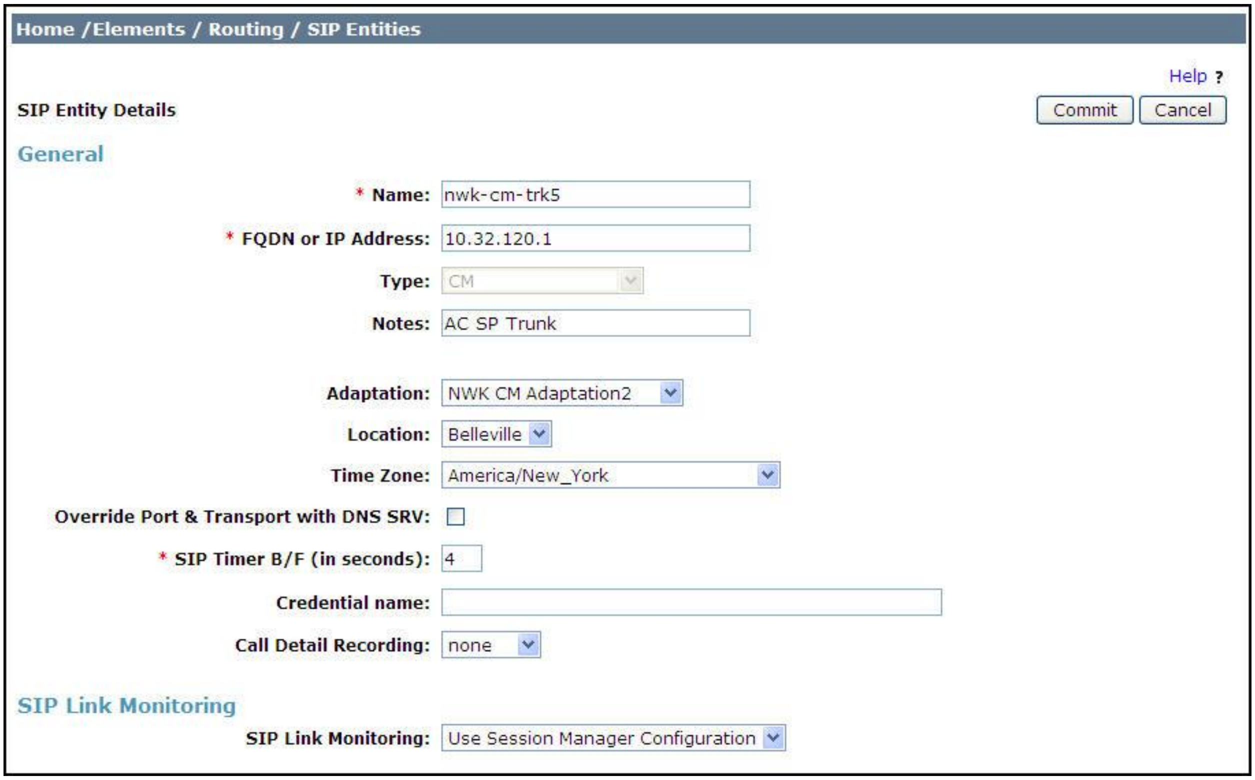
The compliance test used 2 port entries:

– ***5060*** with ***TCP*** for connecting to the 3800 Net-Net SBC
– ***5261*** with ***TLS*** for connecting to Communication Manager

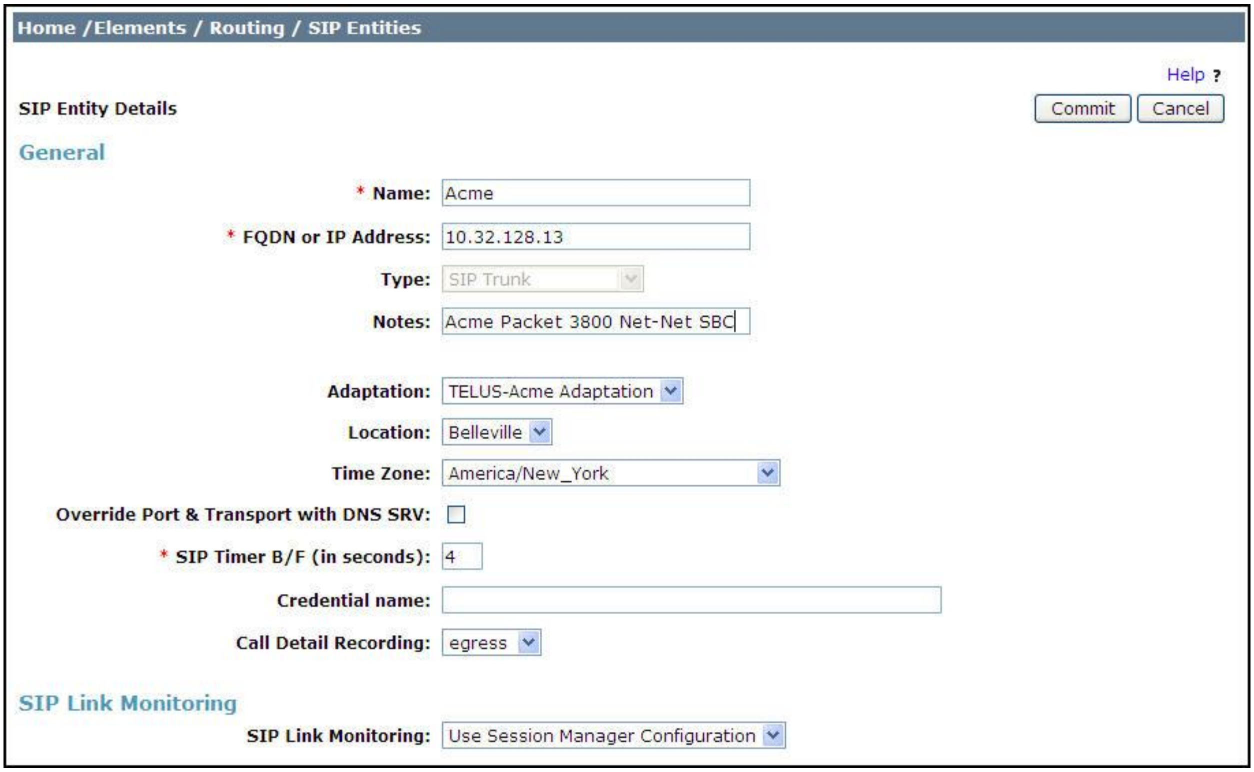
In addition, port 5060 with TCP was also used by a separate SIP Link between Session Manager and Communication Manager for Avaya SIP telephones and SIP soft clients. This SIP Link was part of the standard configuration on Session Manager and was not directly relevant to the inter-operability with TELUS SIP Trunking.

Other entries defined for other projects as shown in the screen were not used.

The following screen shows the addition of the Communication Manager SIP Entity. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created at Session Manager installation for use with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of Communication Manager. For the **Adaptation** field, select the Adaptation module previously defined for use with Communication Manager in **Section 6.4**. The **Location** field is set to ***Belleville*** which is the Location that includes the subnet where Communication Manager resides. Note that ***CM*** was selected for **Type**.



The following screen shows the addition of the 3800 Net-Net SBC. The **FQDN or IP Address** field is set to the IP address of the SBC's private network interface (see **Figure 1**). For the **Adaptation** field, select the Adaptation module previously defined for the SBC in **Section 6.4**. The **Location** field is set to **Belleville** which includes the subnet where the 3800 Net-Net SBC resides. Note that ***SIP Trunk*** was selected for **Type**.



6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the 3800 Net-Net SBC.

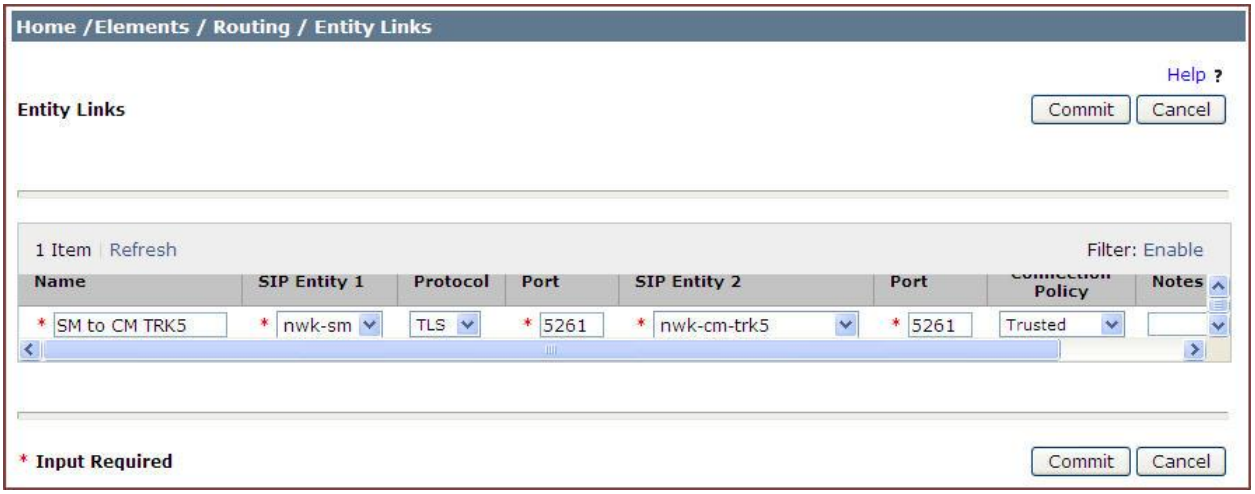
To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **Trusted:** Check this box. Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

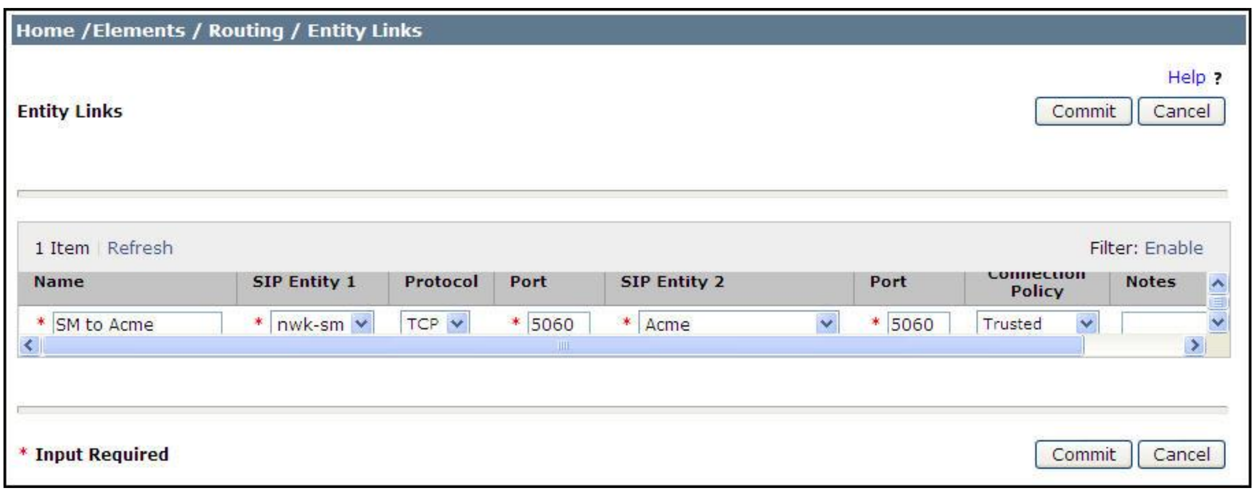
Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and the 3800 Net-Net SBC. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. TCP can be used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

Entity Link to Communication Manager:



Entity Link to the 3800 Net-Net SBC:



6.7. Add Routing Policies

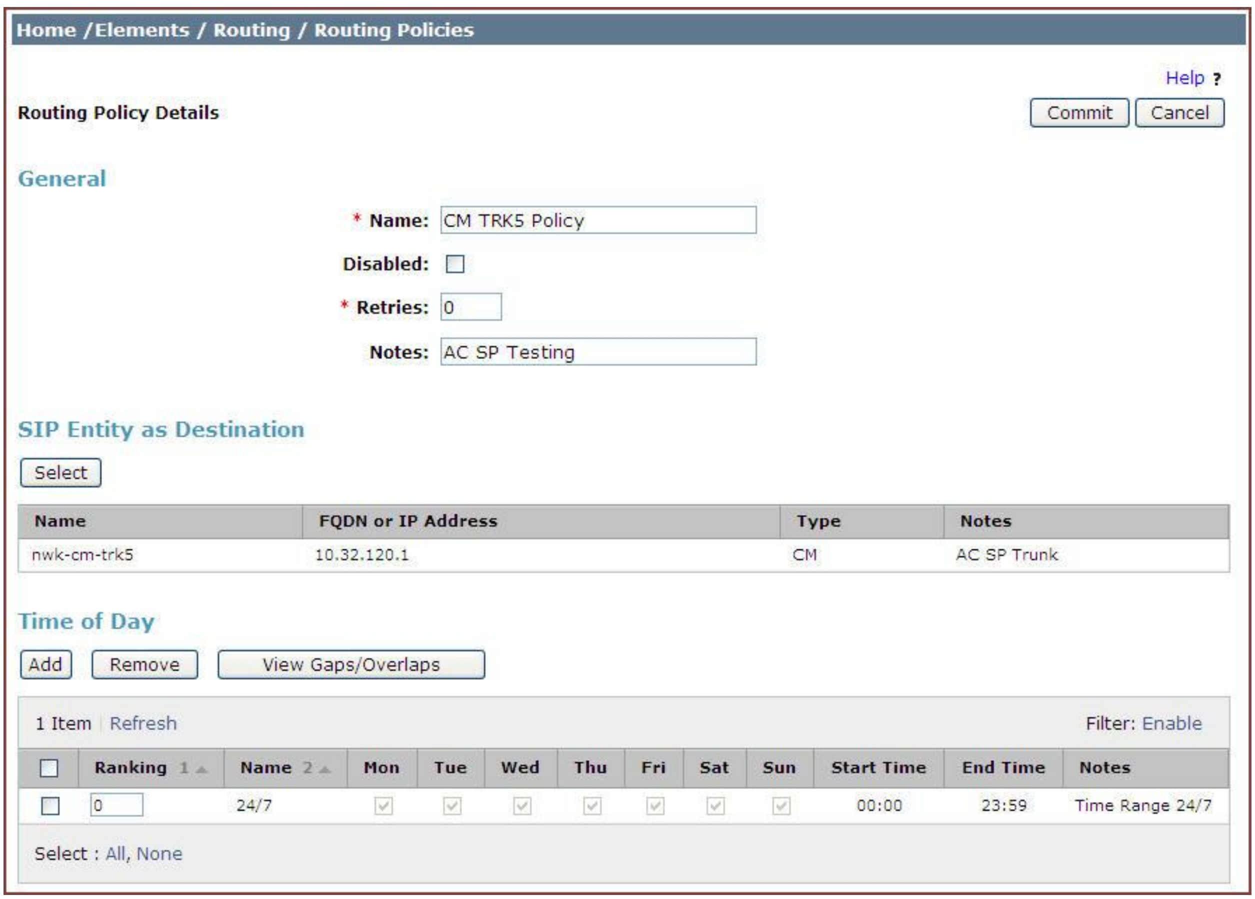
Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two Routing Policies must be added: one for Communication Manager and one for the 3800 Net-Net SBC. To add a Routing Policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

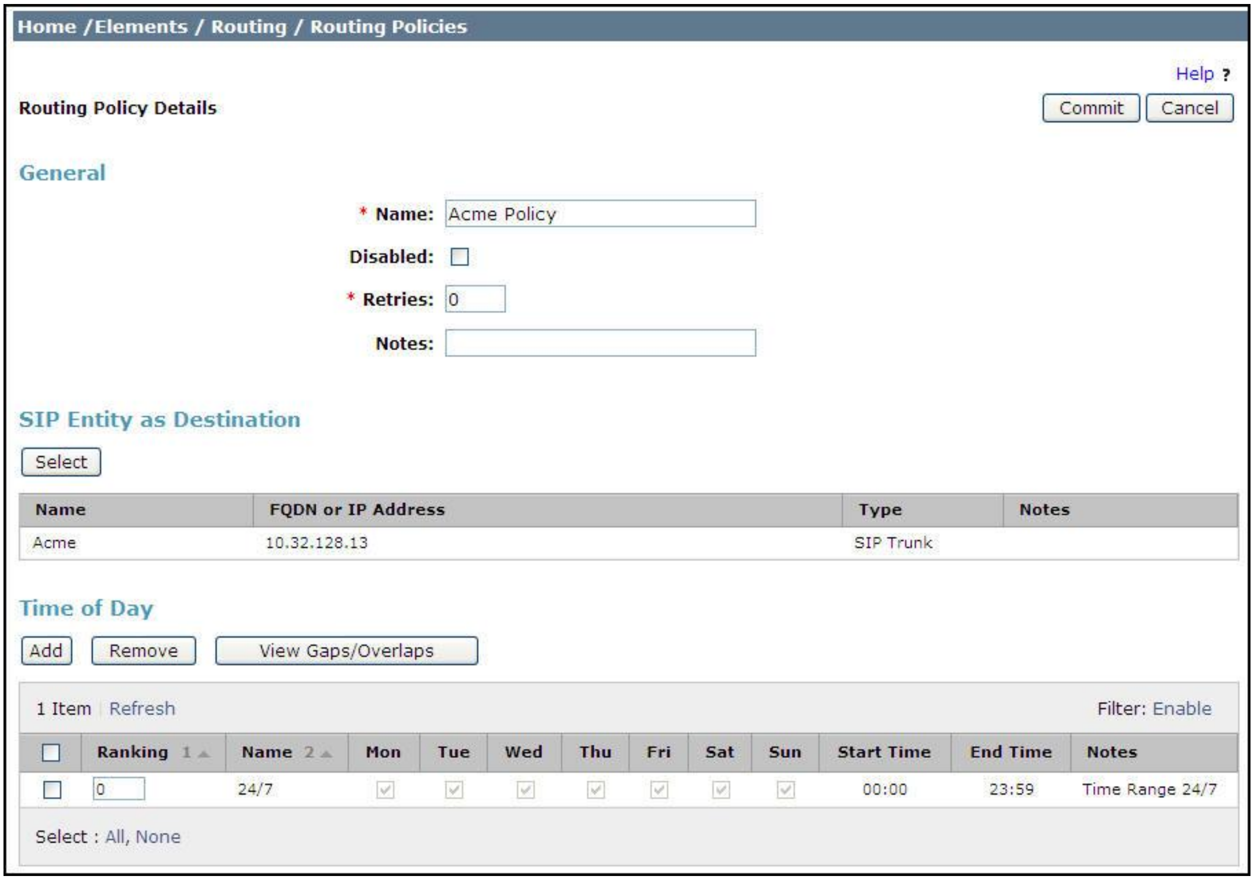
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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

Routing Policy for Communication Manager:



Routing Policy for the 3800 Net-Net SBC:



6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to TELUS and vice versa. Dial Patterns define which Route Policy will be selected as route destination for a particular call based on the dialed digits, destination Domain and originating Location.

To add a Dial Pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

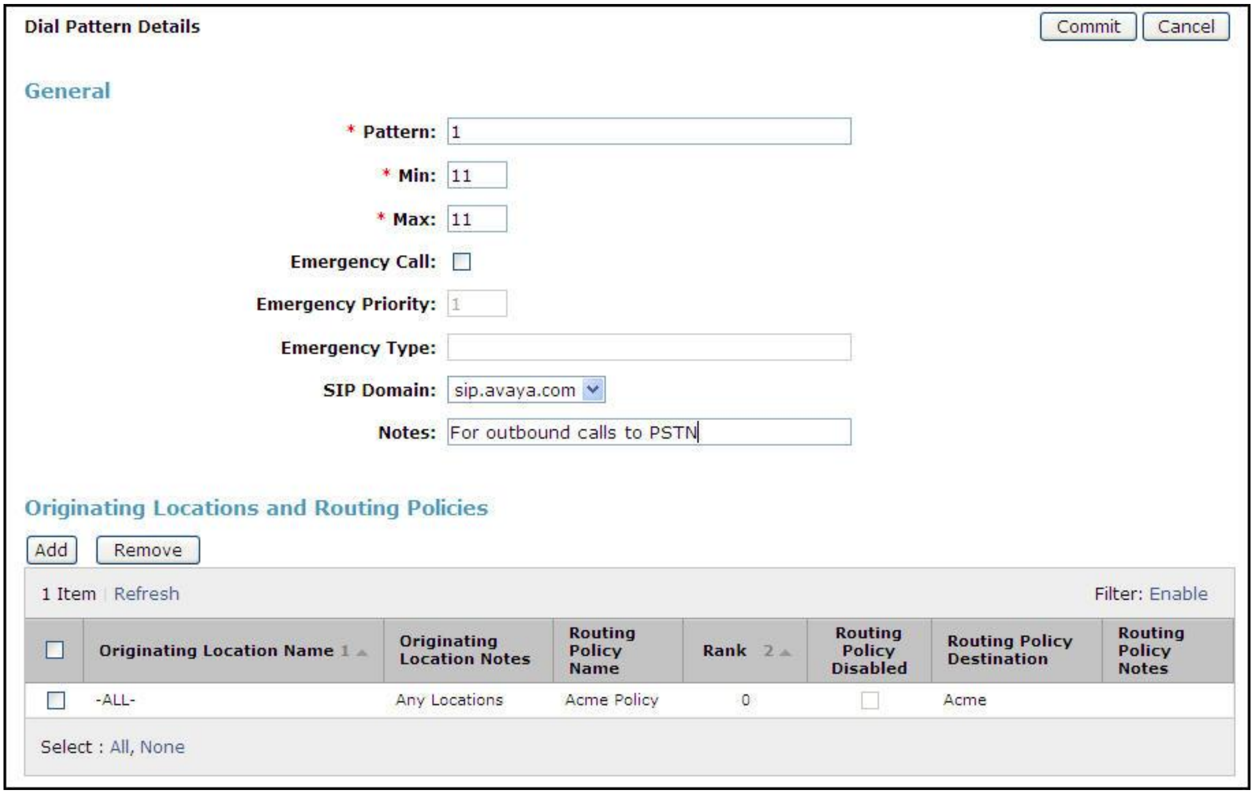
- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:**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

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

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

Two examples of the Dial Patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other Dial Patterns (e.g., 411 directory assistance call, 011 international call, etc.) were similarly defined.

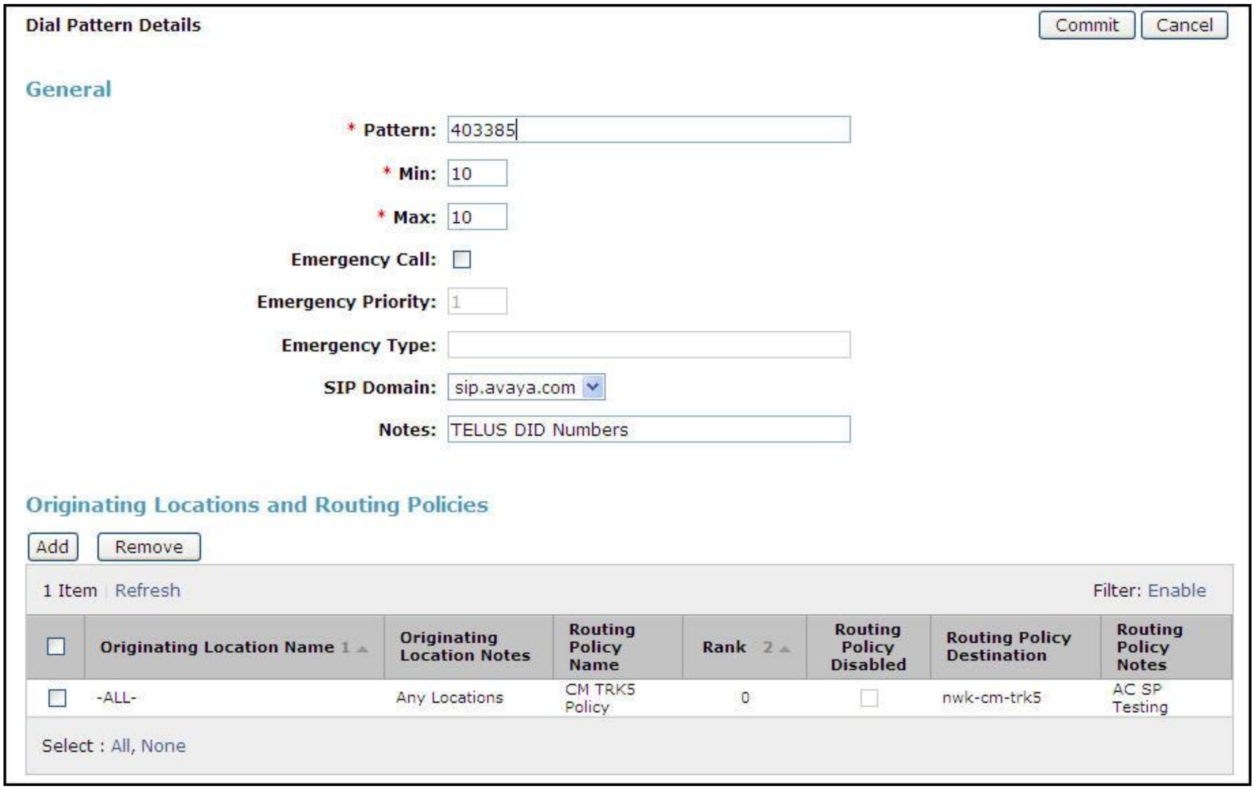
The first example shows that 11-digit dialed numbers that begin with ***1*** and have a destination SIP Domain of ***sip.avaya.com*** uses the ***Acme Policy*** Routing Policy as defined in **Section 6.7**.



Note that the above Dial Pattern did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised (e.g., use Dial Pattern 1908, 1732, etc. with 11 digits) per customer business policies.

Also note that ***-ALL-*** was selected for Originating Location. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed outbound back to the PSTN. For straight-forward outbound calls, like the 411 local directory call, the enterprise Location ***Belleville*** could have been selected.

The second example shows that inbound 10-digit numbers that start with ***403385*** uses Routing Policy ***CM TRK5 Policy*** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by TELUS.



6.9. Add/View Avaya Aura® Session Manager

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

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

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

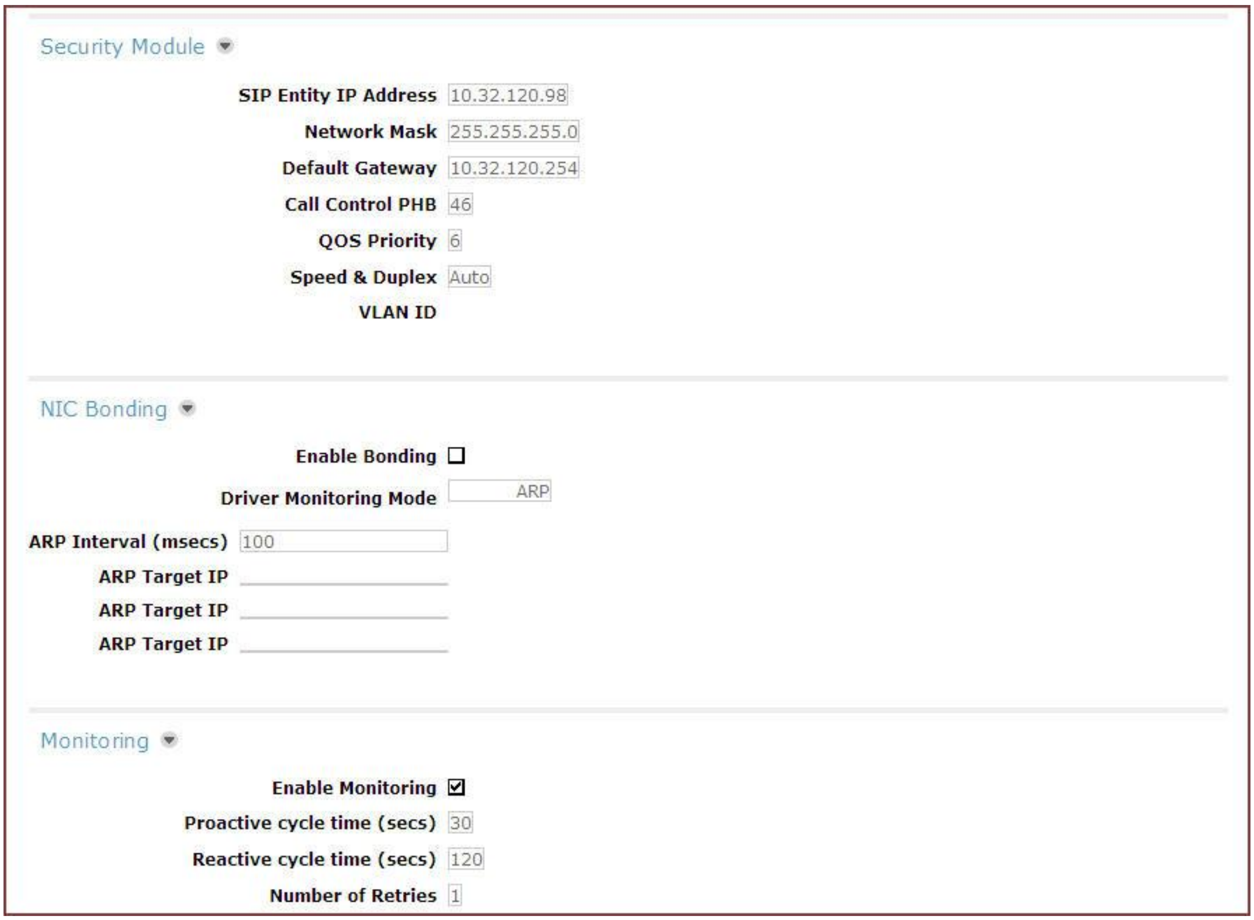
The screen below shows the Session Manager values used for the compliance test.

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

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

In the **Monitoring** section, enter a desired value for **Proactive cycle time (secs)** which determines the interval at which Session Manager sends out OPTIONS message to the connected SIP Entities for checking reachability.

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



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

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

The 3800 Net-Net SBC was configured using the Acme Packet CLI via a serial console port connection. An IP remote connection to a management port is also supported. The following are the generic steps for configuring various elements.

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to (configure*) #*.
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address 192.168.0.0**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4-8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until being returned to the Superuser prompt.
10. Type **save-config** to save the configuration.
11. Type **activate-config** to activate the configuration.

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

7.1. Physical Interfaces

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

7.1.1. Public Interface

Create a phy-interface to the public side of the Acme Packet 3800 Net-Net SBC.

1. Enter **system → phy-interface**
2. Enter **name → s0p0**
3. Enter **operation-type → Media**
4. Enter **port → 0**
5. Enter **slot → 0**
6. Enter **done**
7. Enter **exit**

7.1.2. Private Interface

Create a phy-interface to the private enterprise side of the Acme Packet 3800 Net-Net SBC.

1. Enter **system** → **phy-interface**
2. Enter **name** → **s1p0**
3. Enter **operation-type** → **Media**
4. Enter **port** → **0**
5. Enter **slot** → **1**
6. **virtual-mac** → **00:08:25:a0:f4:8a**
   Virtual MAC addresses are assigned based on the MAC address assigned to the SBC. This MAC address is found by entering the command **show prom-info mainboard** in Superuser mode (the response shows a Starting MAC Address, e.g., **00 08 25 a0 fa 80**). To define a virtual MAC address, replace the last digit with **8** thru **f**.
7. Enter **duplex-mode** → **FULL**
8. Enter **speed** → **100**
9. Enter **done**
10. Enter **exit**

7.2. Network Interfaces

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

7.2.1. Public Interface

Create a network-interface to the public side of the SBC. The compliance test was performed with a direct Internet connection to the service using the settings below.

1. Enter **system** → **network-interface**
2. Enter **name** → **s0p0**
3. Enter **ip-address** → **192.168.96.225**
4. Enter **netmask** → **255.255.255.224**
5. Enter **gateway** → **192.168.96.254**
6. Enter **dns-ip-primary** → **192.168.16.67**
7. Enter **hip-ip-list** → **192.168.96.225**
8. Enter **icmp-ip-list** → **192.168.96.225**
9. Enter **done**
10. Enter **exit**

7.2.2. Private Interface

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

1. Enter **system** → **network-interface**
2. Enter **name** → **s1p0**
3. Enter **ip-address** → **10.32.128.13**
4. Enter **netmask** → **255.255.255.0**
5. Enter **gateway** → **10.32.128.254**

6. Enter **hip-ip-list → 10.32.128.13**
7. Enter **icmp-ip-list → 10.32.128.13**
8. Enter **done**
9. Enter **exit**

7.3. Realms

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

7.3.1. Outside Realm

Create a realm for the external network.

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

7.3.2. Inside Realm

Create a realm for the internal network.

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

7.4. Steering-Pools

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

7.4.1. Outside Steering-Pool

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

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 192.168.96.225**
3. Enter **start-port → 49152**
4. Enter **end-port → 65535**
5. Enter **realm-id → EXTERNAL**
6. Enter **done**
7. Enter **exit**

7.4.2. Inside Steering-Pool

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

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

7.5. Media-Manager

Verify that the media-manager process is enabled.

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

7.6. SIP Configuration

This command sets the values for the 3800 Net-Net SBC SIP operating parameters. The home-realm is the internal default realm for the 3800 Net-Net SBC and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere. If the egress-realm is blank, the home-realm is used instead.

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

7.7. SIP Interfaces

The SIP interface defines the SIP signaling interface (IP address and port) on the 3800 Net-Net SBC.

7.7.1. Outside SIP Interface

Create a sip-interface for the outside network.

1. Enter **session-router → sip-interface**
2. Enter **state → enabled**
3. Enter **realm-id → EXTERNAL**
4. Enter **sip-port**
    a. Enter **address → 192.168.96.225**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → UDP**
    d. Enter **allow-anonymous → agents-only**
    e. Enter **done**
    f. Enter **exit**
5. Enter **stop-recurse → 401,403,407**
6. Enter **done**
7. Enter **exit**

7.7.2. Inside SIP Interface

Create a sip-interface for the inside network.

1. Enter **session-router → sip-interface**
2. Enter **state → enabled**
3. Enter **realm-id → INTERNAL2**
4. Enter **sip-port**
    a. Enter **address → 10.32.128.13**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → TCP**
    d. Enter **allow-anonymous → all**
    e. Enter **done**
    f. Enter **exit**
5. Enter **stop-recurse → 401,403,407**
6. Enter **done**
7. Enter **exit**

7.8. Session-Agents

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

7.8.1. Outside Session-Agent

Create a session-agent for the outside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 192.168.119.66**

3. Enter **ip-address → 192.168.119.66**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP**
8. Enter **realm-id → EXTERNAL**
9. Enter **description → TELUS**
10. Enter **ping-method → OPTIONS;hops=0**
11. Enter **ping-interval → 300**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid →**
14. Enter **out-manipulationid → outManToSP**
15. Enter **done**
16. Enter **exit**

7.8.2. Inside Session-Agent

Create a session-agent for the inside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 10.32.120.98**
3. Enter **ip-address → 10.32.120.98**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → StaticTCP**
8. Enter **realm-id → INTERNAL2**
9. Enter **description → NWK-SM**
10. Enter **ping-method →**
11. Enter **ping-interval → 0**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid → inManFromSM**
14. Enter **out-manipulationid → outManToSM**
15. Enter **done**
16. Enter **exit**

7.9. Local Policies

Local policies allow SIP requests from the **INTERNAL2** realm to be routed to the service provider session agent in the **EXTERNAL** realm (and vice-versa).

7.9.1. INTERNAL2 to EXTERNAL

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

1. Enter **session-router → local-policy**
2. Enter **from-address →** *
3. Enter **to-address →** *

4. Enter **source-realm → INTERNAL2**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 192.168.119.66**
    b. Enter **realm → EXTERNAL**
    c. Enter **terminate-recursion → enabled**
    d. Enter **app-protocol → SIP**
    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

7.9.2. EXTERNAL to INTERNAL2

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

1. Enter **session-router → local-policy**
2. Enter **from-address →** *
3. Enter **to-address → ***
4. Enter **source-realm → EXTERNAL**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 10.32.120.98**
    b. Enter **realm → INTERNAL2**
    c. Enter **terminate-recursion → enabled**
    d. Enter **app-protocol → SIP**
    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

7.10. SIP Manipulations

SIP manipulation specifies rules for manipulating the contents of specified SIP headers. Three separate sets of SIP manipulations were configured for the compliance test as listed below. These sip manipulations are specified in the session-agents configuration in **Section 7.8**.

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

7.10.1. Session Manager to SBC

The following set of SIP HMRs is applied to traffic from Session Manager to the SBC. In some call flows the user part of the SIP Contact header received from the Session Manager was not passed unaltered to the public side of the SBC. To correct this, the user part of the Contact header is stored when received from the Session Manager and used to create a temporary header called X-Contact that will be deleted on the outbound (public) side of the SBC. The information contained in the X-Contact header will be used to recreate the proper Contact header on the public side of the SBC as shown in **Sections 7.10.3.8** and **7.10.3.9**.

To create this set of SIP HMRs:

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

7.10.1.1 Store Contact

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

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

7.10.1.2 Create X-Contact

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

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

7.10.2. SBC to Session Manager

The following SIP HMR is applied to traffic from the SBC to Session Manager. This SIP HMR replaces the host part of Request-URI with the enterprise SIP Domain **sip.avaya.com**.

To create this SIP HMR:

1. Enter **session-router → sip-manipulation**
2. Enter **name → outManToSM**
3. Enter **description → "Outbound SIP HMRs To SM"**
4. Proceed to the following section. Once the section is completed then proceed with **Steps 5** and **6** below.
5. Enter **done**
6. Enter **exit**

7.10.2.1 Change Request-URI

This rule changes the host part of Request-URI to the enterprise SIP Domain **sip.avaya.com**.

1. Enter **header-rule**
2. Enter **name → chgRURI**
3. Enter **header-name → Request-URI**
4. Enter **action → manipulate**
5. Enter **comparison-type → pattern-rule**
6. Enter **msg-type → request**
7. Enter **methods →**
8. Enter **element-rule**
    a. Enter **name → chgRuriHost**

b. Enter **parameter-name →**
c. Enter **type → uri-host**
d. Enter **action → replace**
e. Enter **match-val-type → any**
f. Enter **comparison-type → case-sensitive**
g. Enter **match-value →**
h. Enter **new-value → sip.avaya.com**
i. Enter **done**
j. Enter **exit**

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

7.10.3. SBC to TELUS

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

To create this set of SIP HMRs:

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

7.10.3.1 Change Host of the To Header

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

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

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

7.10.3.2 Change Host of the From Header

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

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

7.10.3.3 Change Host of the History-Info Header

This rule replaces the host part of the History-Info header with the public IP address of the SBC. For the finalized configuration used for the compliance test, History-Info header was turned off on Communication Manager (**Support Request History** was disabled on page 4 of the service provider SIP trunk form in **Section 5.8**). This HMR is included here for completeness.

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

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

7.10.3.4 Change Host of the PAI Header

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

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

7.10.3.5 Change Host of the Diversion Header

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

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

7.10.3.6 Change Host of the Refer-To Header

This rule replaces the host part of the Refer-To header with the service provider's IP address. For the finalized configuration used for the compliance test, REFER was turned off on Communication Manager (**Network Call Redirection** was disabled on page 4 of the service provider SIP trunk form in **Section 5.8**) since TELUS does not officially support REFER. This HMR is included here for completeness.

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

7.10.3.7 Store X-Contact Header

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

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

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

7.10.3.8 Replace Contact Header

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

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

7.10.3.9 Delete X-Contact Header

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

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

7.10.3.10 Delete P-Location Header

This rule deletes the P-Location header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

1. Enter **header-rule**
2. Enter **name → delPloc**
3. Enter **header-name → P-Location**
4. Enter **action → delete**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → any**
7. Enter **methods →**
8. Enter **done**
9. Enter **exit**

7.10.3.11 Delete Alert-Info Header

This rule deletes the Alert-Info header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

1. Enter **header-rule**
2. Enter **name → delAlert**
3. Enter **header-name → Alert-Info**
4. Enter **action → delete**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → any**
7. Enter **methods →**
8. Enter **done**
9. Enter **exit**

7.10.3.12 Delete Endpoint-View Header

This rule deletes the Endpoint-View header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

10. Enter **header-rule**
11. Enter **name → delEdptView**
12. Enter **header-name → Endpoint-View**
13. Enter **action → delete**
14. Enter **comparison-type → case-sensitive**
15. Enter **msg-type → any**
16. Enter **methods →**
17. Enter **done**
18. Enter **exit**

7.10.3.13 Delete P-Charging-Vector Header

This rule deletes the P-Charging-Vector header. This header is not used by the service provider and it may contain internal IP addresses which should not be shared outside of the enterprise. Thus, the header was removed.

19. Enter **header-rule**
20. Enter **name → delPChgVctr**
21. Enter **header-name → P-Charging-Vector**
22. Enter **action → delete**
23. Enter **comparison-type → case-sensitive**
24. Enter **msg-type → any**
25. Enter **methods →**
26. Enter **done**
27. Enter **exit**

7.10.3.14 Store Diversion Header User and Display Name

This rule stores the user and the display name parts of the Diversion header to be used in the next section to modify the PAI header. This is necessary to complete calls from the PSTN which are redirected back to the PSTN. See **Section 2.2** for more details.

1. Enter **header-rule**
2. Enter **name → strDivNum**
3. Enter **header-name → Diversion**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **methods → INVITE**
8. Enter **element-rule**
    a. Enter **name → strval**
    b. Enter **type → uri-user**
    c. Enter **action → store**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **match-value → (.*)**
    g. Enter **done**
    h. Enter **exit**
9. Enter **element-rule**
    a. Enter **name → strDisName**
    b. Enter **type → uri-display**
    c. Enter **action → store**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **match-value → (.*)**
    g. Enter **done**
    h. Enter **exit**

10. Enter **done**
11. Enter **exit**

7.10.3.15 Modify PAI Header with Diversion Header Information

This rule modifies the user and the display name parts of the PAI header using the information stored from the Diversion header in the last section. It only modifies the PAI in the INVITE message if the Diversion header is present. This is determined by checking if any value was stored for the Diversion user from the previous rule. This rule is necessary to complete calls from the PSTN which are redirected back to the PSTN. See **Section 2.2** for more details.

1. Enter **header-rule**
2. Enter **name → chgPAIuser**
3. Enter **header-name → P-Asserted-Identity**
4. Enter **action → manipulate**
5. Enter **comparison-type → boolean**
6. Enter **msg-type → request**
7. Enter **methods → INVITE**
8. Enter **match-value → $strDivNum.$strval.$0**
9. Enter **element-rule**
    a. Enter **name → chgUserFromDiv**
    b. Enter **type → uri-user**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → pattern-rule**
    f. Enter **match-value → (.*)**
    g. Enter **new-value → $strDivNum.$strval.$0**
    h. Enter **done**
    i. Enter **exit**
10. Enter **element-rule**
    a. Enter **name → chgDispName**
    b. Enter **type → uri-display**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → pattern-rule**
    f. Enter **match-value → (.*)**
    g. Enter **$strDivNum.$strDisName.$0**
    h. Enter **done**
    i. Enter **exit**
11. Enter **done**
12. Enter **exit**

7.10.3.16 Delete Diversion Header

This rule deletes the Diversion header. The Diversion header is no longer needed once the PAI has been modified. It may also cause unexpected behavior if forwarded on to the TELUS network.

1. Enter **header-rule**
2. Enter **name → delDiv**
3. Enter **header-name → Diversion**
4. Enter **action → delete**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → any**
7. Enter **methods →**
8. Enter **done**
9. Enter **exit**

7.10.3.17 Modify Max-Forwards in OPTIONS message

This rule changes the value of the Max-Forward header to zero in the OPTIONS message. A Max-Forwards value of zero is a requirement of the TELUS network. See **Section 2.2** for more details.

1. Enter **header-rule**
2. Enter **name → OptZeroMaxFwd**
3. Enter **header-name → Max-Forwards**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **methods → OPTIONS**
    a. Enter **element-rule**
    b. Enter **name → zeroMaxFwd**
    c. Enter **type → header-value**
    d. Enter **action → replace**
    e. Enter **match-val-type → any**
    f. Enter **comparison-type → case-sensitive**
    g. Enter **match-value →**
    h. Enter **new-value → 0**
    i. Enter **done**
    j. Enter **exit**
8. Enter **done**
9. Enter **exit**

8. TELUS SIP Trunking Configuration

TELUS is responsible for the network configuration of the TELUS SIP Trunking service. TELUS will require that the customer provide the public IP address used to reach the 3800 Net-Net SBC at the edge of the enterprise. TELUS will provide the IP address of the TELUS SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for Communication Manager, Session Manager, and the Acme Packet 3800 Net-Net SBC discussed in the previous sections.

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

9. Verification Steps

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

Verification Steps:

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

Troubleshooting:

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

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Acme Packet 3800 Net-Net Session Border Controller to TELUS SIP Trunking. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workarounds.

11. References

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

Avaya Aura® Solution for Midsize Enterprise

[1] *Avaya Aura® Solution for the Midsize Enterprise (ME) 6.2 Intelligent Workbook*, Workbook Version 2.1, September 2012

[2] *Implementing Avaya Aura® Solution for Midsize Enterprise*, Release 6.2, Issue 4.2, July 2012

Avaya Aura® Session Manager/System Manager

[3] *Administering Avaya Aura® Session Manager*, Document ID 03-603324, Release 6.2, July 2012

[4] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Release 6.2, August 2012

[5] *Administering Avaya Aura® System Manager*, Release 6.2, July 2012

Avaya Aura® Communication Manager

[6] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Release 6.2, July 2012

[7] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya one-X™ IP Phones

[8] *Avaya one-X™ Deskphone SIP for 9601 IP Telephone User Guide*, Document ID 16-603618, Issue 1, December 2010

[9] *Avaya one-X™ Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones*, Document ID 16-603596, Issue 1, May 2011

[10] *Avaya one-X™ Deskphone H.323 9608 and 9611G User Guide*, Document ID 16-603593, Issue 3, February 2012

[11] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Document ID 16-601944, Release 2.6, June 2010

[12] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Document ID 16-300698, Release 3.1, November 2009

[13] *Administering Avaya one-X® Communicator*, October 2011

[14] *Using Avaya one-X® Communicator Release 6.1*, October 2011

IETF (Internet Engineering Task Force) SIP Standards Specifications

[15] RFC 3261 *SIP: Session Initiation Protocol*, http://www.ietf.org/

[16] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

Appendix: Acme Packet 3800 Net-Net SBC Configuration File

```
host-routes
      dest-network                   10.1.2.0
      netmask                        255.255.255.0
      gateway                        10.32.128.254
      description
      last-modified-by               admin@192.168.168.37
      last-modified-date             2011-10-27 16:57:53
host-routes
      dest-network                   10.32.0.0
      netmask                        255.255.0.0
      gateway                        10.32.128.254
      description                    DevConnectLAN
      last-modified-by               admin@135.11.141.118
      last-modified-date             2010-08-05 15:25:58
host-routes
      dest-network                   192.168.0.0
      netmask                        255.255.0.0
      gateway                        10.32.128.254
      description                    Route to remote testers
      last-modified-by               admin@192.168.168.37
      last-modified-date             2011-09-10 10:50:25
local-policy
      from-address
                                     *
      to-address
                                     *
      source-realm
                                     INTERNAL2
      description
      activate-time                  N/A
      deactivate-time                N/A
      state                          enabled
      policy-priority                none
      last-modified-by               admin@192.168.168.37
      last-modified-date             2011-12-19 13:06:16
      policy-attribute
            next-hop                       192.168.119.66
            realm                          EXTERNAL
            action                         none
            terminate-recursion            enabled
            carrier
            start-time                     0000
            end-time                       2400
            days-of-week                   U-S
            cost                           0
            app-protocol                   SIP
            state                          enabled
            methods
            media-profiles
            lookup                         single
            next-key
            eloc-str-lkup                  disabled
            eloc-str-match
local-policy
      from-address
                                     *
      to-address
                                     *
```

```
      source-realm
                                   EXTERNAL
      description
      activate-time                N/A
      deactivate-time              N/A
      state                        enabled
      policy-priority              none
      last-modified-by             admin@192.168.168.37
      last-modified-date           2011-10-27 17:17:00
      policy-attribute
            next-hop                     10.32.120.98
            realm                        INTERNAL2
            action                       none
            terminate-recursion          enabled
            carrier
            start-time                   0000
            end-time                     2400
            days-of-week                 U-S
            cost                         0
            app-protocol                 SIP
            state                        enabled
            methods
            media-profiles
            lookup                       single
            next-key
            eloc-str-lkup                disabled
            eloc-str-match
media-manager
      state                        enabled
      latching                     enabled
      flow-time-limit              86400
      initial-guard-timer          300
      subsq-guard-timer            300
      tcp-flow-time-limit          86400
      tcp-initial-guard-timer      300
      tcp-subsq-guard-timer        300
      tcp-number-of-ports-per-flow   2
      hnt-rtcp                     disabled
      algd-log-level               NOTICE
      mbcd-log-level               NOTICE
      red-flow-port                1985
      red-mgcp-port                1986
      red-max-trans                10000
      red-sync-start-time          5000
      red-sync-comp-time           1000
      media-policing               enabled
      max-signaling-bandwidth      10000000
      max-untrusted-signaling      100
      min-untrusted-signaling      30
      app-signaling-bandwidth      0
      tolerance-window             30
      rtcp-rate-limit              0
      trap-on-demote-to-deny       enabled
      min-media-allocation         2000
      min-trusted-allocation       4000
      deny-allocation              64000
      anonymous-sdp                disabled
      arp-msg-bandwidth            32000
      fragment-msg-bandwidth       0
      rfc2833-timestamp            disabled
      default-2833-duration        100
      rfc2833-end-pkts-only-for-non-sig enabled
```

```
        translate-non-rfc2833-event    disabled
        media-supervision-traps        disabled
        dnsalg-server-failover         disabled
        last-modified-by               admin@135.11.141.142
        last-modified-date             2010-06-16 05:40:01
network-interface
        name                           s0p0
        sub-port-id                    0
        description
        hostname
        ip-address                     192.168.96.225
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.224
        gateway                        192.168.96.254
        sec-gateway
        gw-heartbeat
                state                          disabled
                heartbeat                      0
                retry-count                    0
                retry-timeout                  1
                health-score                   0
        dns-ip-primary                 192.168.16.67
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    192.168.96.225
        ftp-address
        icmp-address                   192.168.96.225
        snmp-address
        telnet-address
        ssh-address
        last-modified-by               admin@192.168.168.37
        last-modified-date             2011-09-10 10:08:47
network-interface
        name                           s1p0
        sub-port-id                    0
        description
        hostname
        ip-address                     10.32.128.13
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.0
        gateway                        10.32.128.254
        sec-gateway
        gw-heartbeat
                state                          disabled
                heartbeat                      0
                retry-count                    0
                retry-timeout                  1
                health-score                   0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    10.32.128.13
        ftp-address                    10.32.128.13
        icmp-address                   10.32.128.13
        snmp-address
        telnet-address                 10.32.128.13
```

```
        ssh-address
        last-modified-by              admin@192.168.168.37
        last-modified-date            2011-11-03 11:42:43
phy-interface
        name                          s0p0
        operation-type                Media
        port                          0
        slot                          0
        virtual-mac
        admin-state                   enabled
        auto-negotiation              enabled
        duplex-mode
        speed
        overload-protection           disabled
        last-modified-by              admin@console
        last-modified-date            2011-09-09 19:39:05
phy-interface
        name                          s1p0
        operation-type                Media
        port                          0
        slot                          1
        virtual-mac                   00:08:25:a0:f4:8a
        admin-state                   enabled
        auto-negotiation              enabled
        duplex-mode                   FULL
        speed                         100
        overload-protection           disabled
        last-modified-by              admin@console
        last-modified-date            2011-09-09 19:38:24
realm-config
        identifier                    EXTERNAL
        description
        addr-prefix                   0.0.0.0
        network-interfaces
                                      s0p0:0
        mm-in-realm                   disabled
        mm-in-network                 enabled
        mm-same-ip                    enabled
        mm-in-system                  enabled
        bw-cac-non-mm                 disabled
        msm-release                   disabled
        generate-UDP-checksum         disabled
        max-bandwidth                 0
        fallback-bandwidth            0
        max-priority-bandwidth        0
        max-latency                   0
        max-jitter                    0
        max-packet-loss               0
        observ-window-size            0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit            0
        access-control-trust-level    none
```

```
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        ext-policy-svr
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        dyn-refer-term                 disabled
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        xnq-state                      xnq-unknown
        hairpin-id                     0
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
        last-modified-by               admin@135.11.207.156
        last-modified-date             2010-11-03 08:55:21
realm-config
        identifier                     INTERNAL2
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       s1p0:0
        mm-in-realm                    disabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        generate-UDP-checksum          disabled
        max-bandwidth                  0
        fallback-bandwidth             0
        max-priority-bandwidth         0
        max-latency                    0
```

```
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        ext-policy-svr
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        dyn-refer-term                  disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@135.11.207.156
        last-modified-date              2010-12-16 17:25:01
session-agent
```

```
hostname                        10.32.120.98
ip-address                      10.32.120.98
port                            5060
state                           enabled
app-protocol                    SIP
app-type
transport-method                StaticTCP
realm-id                        INTERNAL2
egress-realm-id
description                     NWK_SM
carriers
allow-next-hop-lp               enabled
constraints                     disabled
max-sessions                    0
max-inbound-sessions            0
max-outbound-sessions           0
max-burst-rate                  0
max-inbound-burst-rate          0
max-outbound-burst-rate         0
max-sustain-rate                0
max-inbound-sustain-rate        0
max-outbound-sustain-rate       0
min-seizures                    5
min-asr                         0
time-to-resume                  0
ttr-no-response                 0
in-service-period               0
burst-rate-window               0
sustain-rate-window             0
req-uri-carrier-mode            None
proxy-mode
redirect-action
loose-routing                   enabled
send-media-session              enabled
response-map
ping-method
ping-interval                   0
ping-send-mode                  keep-alive
ping-all-addresses              disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                        disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                     disabled
in-manipulationid               inManFromSM
out-manipulationid              outManToSM
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate       0
early-media-allow
invalidate-registrations        disabled
rfc2833-mode                    none
rfc2833-payload                 0
```

```
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        last-modified-by               admin@192.168.168.37
        last-modified-date             2011-09-20 22:39:03
session-agent
        hostname                       192.168.119.66
        ip-address                     192.168.119.66
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       EXTERNAL
        egress-realm-id
        description                    TELUS
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=0
        ping-interval                  300
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
```

```
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid
        out-manipulationid             outManToSP
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        last-modified-by               admin@192.168.168.37
        last-modified-date             2011-10-10 12:21:24
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INTERNAL2
        egress-realm-id
        nat-mode                       Public
        registrar-domain               *
        registrar-host                 *
        registrar-port                 5060
        register-service-route         always
        init-timer                     500
        max-timer                      4000
        trans-expire                   32
        invite-expire                  180
        inactive-dynamic-conn          32
        enforcement-profile
        pac-method
        pac-interval                   10
        pac-strategy                   PropDist
        pac-load-weight                1
        pac-session-weight             1
        pac-route-weight               1
        pac-callid-lifetime            600
        pac-user-lifetime              3600
        red-sip-port                   1988
        red-max-trans                  10000
        red-sync-start-time            5000
        red-sync-comp-time             1000
        add-reason-header              disabled
        sip-message-len                4096
        enum-sag-match                 disabled
        extra-method-stats             enabled
        registration-cache-limit       0
        register-use-to-for-lp         disabled
        options                        max-udp-length=0
        refer-src-routing              disabled
```

```
        add-ucid-header                disabled
        proxy-sub-events
        pass-gruu-contact              disabled
        sag-lookup-on-redirect         disabled
        last-modified-by               admin@135.11.207.156
        last-modified-date             2010-11-02 16:18:33
sip-interface
        state                          enabled
        realm-id                       EXTERNAL
        description
        sip-port
                address                        192.168.96.225
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                agents-only
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,403,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
```

```
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@192.168.168.37
        last-modified-date             2011-11-18 10:38:42
sip-interface
        state                          enabled
        realm-id                       INTERNAL2
        description
        sip-port
                address                        10.32.128.13
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,403,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
```

```
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@135.105.224.163
        last-modified-date             2011-08-03 16:00:53
sip-manipulation
        name                           outManToSP
        description                    Outbound SIP HMRs To SP
        split-headers
        join-headers
        header-rule
                name                           manipTo
                header-name                    To
                action                         manipulate
                comparison-type                pattern-rule
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           chgToHost
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $REMOTE_IP
        header-rule
                name                           manipFrom
                header-name                    From
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           From
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
```

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

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

```
            action                          store
            match-val-type                  any
            comparison-type                 case-sensitive
            match-value                     (.*)
            new-value
    header-rule
        name                            manipRefer
        header-name                     Refer-To
        action                          manipulate
        comparison-type                 case-sensitive
        msg-type                        request
        methods
        match-value
        new-value
        element-rule
            name                            chgHostRefer
            parameter-name
            type                            uri-host
            action                          replace
            match-val-type                  any
            comparison-type                 case-sensitive
            match-value
            new-value                       $REMOTE_IP
    header-rule
        name                            delPloc
        header-name                     P-Location
        action                          delete
        comparison-type                 case-sensitive
        msg-type                        any
        methods
        match-value
        new-value
    header-rule
        name                            delAlert
        header-name                     Alert-Info
        action                          delete
        comparison-type                 case-sensitive
        msg-type                        any
        methods
        match-value
        new-value
    header-rule
        name                            delEdptView
        header-name                     Endpoint-View
        action                          delete
        comparison-type                 case-sensitive
        msg-type                        any
        methods
        match-value
        new-value
    header-rule
        name                            delPChgVctr
        header-name                     P-Charging-Vector
        action                          delete
        comparison-type                 case-sensitive
        msg-type                        any
        methods
        match-value
        new-value
    header-rule
        name                            chgPAIuser
        header-name                     P-Asserted-Identity
```

```
            action                          manipulate
            comparison-type                 boolean
            msg-type                        request
            methods                         INVITE
            match-value                     $strDivNum.$strval.$0
            new-value
            element-rule
                   name                           chgUserFromDiv
                   parameter-name
                   type                           uri-user
                   action                         replace
                   match-val-type                 any
                   comparison-type                pattern-rule
                   match-value                    (.*)
                   new-value                      $strDivNum.$strval.$0
            element-rule
                   name                           chgDispName
                   parameter-name
                   type                           uri-display
                   action                         replace
                   match-val-type                 any
                   comparison-type                pattern-rule
                   match-value                    (.*)
                   new-value                      $strDivNum.$strDisName.$0
      header-rule
            name                            delDiv
            header-name                     Diversion
            action                          delete
            comparison-type                 case-sensitive
            msg-type                        any
            methods
            match-value
            new-value
      header-rule
            name                            OptZeroMaxFwd
            header-name                     Max-Forwards
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods                         OPTIONS
            match-value
            new-value
            element-rule
                   name                           zeroMaxFwd
                   parameter-name
                   type                           header-value
                   action                         replace
                   match-val-type                 any
                   comparison-type                case-sensitive
                   match-value
                   new-value                      0
      last-modified-by               admin@192.168.168.37
      last-modified-date             2012-02-06 14:06:04
sip-manipulation
      name                           inManFromSM
      description                    Inbound SIP HMRs From SM
      split-headers
      join-headers
      header-rule
            name                            strcon
            header-name                     Contact
            action                          manipulate
```

```
            comparison-type               case-sensitive
            msg-type                      request
            methods                       INVITE,UPDATE
            match-value
            new-value
            element-rule
                  name                          strval
                  parameter-name
                  type                          uri-user
                  action                        store
                  match-val-type                any
                  comparison-type               case-sensitive
                  match-value                   (.*)
                  new-value
      header-rule
            name                          addXcontact
            header-name                   X-Contact
            action                        add
            comparison-type               pattern-rule
            msg-type                      request
            methods                       INVITE,UPDATE
            match-value
            new-value
            element-rule
                  name                          addX
                  parameter-name
                  type                          header-value
                  action                        replace
                  match-val-type                any
                  comparison-type               pattern-rule
                  match-value
                  new-value                     $strcon.$strval.$0
sip-manipulation
      name                          outManToSM
      description                   Outbound SIP HMRs to SM
      split-headers
      join-headers
      header-rule
            name                          chgRURI
            header-name                   Request-URI
            action                        manipulate
            comparison-type               pattern-rule
            msg-type                      request
            methods
            match-value
            new-value
            element-rule
                  name                          chgRuriHost
                  parameter-name
                  type                          uri-host
                  action                        replace
                  match-val-type                any
                  comparison-type               case-sensitive
                  match-value
                  new-value                     sip.avaya.com
      last-modified-by              admin@192.168.168.37
      last-modified-date            2012-08-07 18:09:26
steering-pool
      ip-address                    192.168.96.225
      start-port                    49152
      end-port                      65535
      realm-id                      EXTERNAL
```

```
        network-interface
        last-modified-by              admin@192.168.168.37
        last-modified-date            2011-09-10 10:11:31
steering-pool
        ip-address                    10.32.128.13
        start-port                    2048
        end-port                      65535
        realm-id                      INTERNAL2
        network-interface
        last-modified-by              admin@135.11.141.118
        last-modified-date            2010-10-06 11:28:26
system-config
        hostname
        description
        location
        mib-system-contact
        mib-system-name
        mib-system-location
        snmp-enabled                  enabled
        enable-snmp-auth-traps        disabled
        enable-snmp-syslog-notify     disabled
        enable-snmp-monitor-traps     disabled
        enable-env-monitor-traps      disabled
        snmp-syslog-his-table-length  1
        snmp-syslog-level             WARNING
        system-log-level              WARNING
        process-log-level             NOTICE
        process-log-ip-address        0.0.0.0
        process-log-port              0
        collect
                sample-interval               5
                push-interval                 15
                boot-state                    disabled
                start-time                    now
                end-time                      never
                red-collect-state             disabled
                red-max-trans                 1000
                red-sync-start-time           5000
                red-sync-comp-time            1000
                push-success-trap-state       disabled
        call-trace                    enabled
        internal-trace                enabled
        log-filter                    all
        default-gateway               10.3.3.254
        restart                       enabled
        exceptions
        telnet-timeout                0
        console-timeout               0
        remote-control                enabled
        cli-audit-trail               enabled
        link-redundancy-state         disabled
        source-routing                disabled
        cli-more                      disabled
        terminal-height               24
        debug-timeout                 0
        trap-event-lifetime           0
        default-v6-gateway            ::
        ipv6-support                  disabled
        cleanup-time-of-day           00:00
        last-modified-by              admin@192.168.168.37
        last-modified-date            2011-09-10 11:04:14
```

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.