Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Level 3 SIP Trunking with Avaya Aura® Communication Manager Access Element 5.2.1, Avaya Aura® Session Manager 6.1 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 Level 3 SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager Access Element 5.2.1, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

Level 3 is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Level 3 SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.1, Avaya Aura® Communication Manager Access Element 5.2.1, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Level 3 SIP Trunking are able to place and receive PSTN calls via a broadband WAN connection with SIP. 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 Level 3 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.

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. Please note that SIP endpoints were not tested since SIP endpoints are not supported on a Communication Manager Access Element.

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

- Codec G.711MU and G.729A
- DTMF transmission using RFC 2833
- Caller ID presentation and Caller ID restriction
- Response to incomplete call attempts and trunk errors
- Voicemail navigation for inbound and outbound calls
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding and mobility (extension to cellular)
- T.38 Fax
- Network Call Redirection using the SIP REFER method

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 Level 3.

2.2. Test Results

Interoperability testing of Level 3 SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Max-Forwards**: On incoming PSTN calls to the enterprise, the Max-Forwards value in the incoming SIP INVITE is set to a value of 9. In past compliance tests, this value has been observed to be too small to allow the message to traverse all the SIP hops internal to the enterprise to reach the destination in all cases. Thus, the SBC was used to increase this value when the INVITE arrived at the SBC from the network. (See **Section 7.10.2.1**)
- **No Error Indication if No Matching Codec Offered**: If the Communication Manager SIP trunk is improperly configured to have no matching codec with the service provider and an outbound call is placed, the service provider returns a "480 Temporarily Unavailable" response instead of a "488 Not Acceptable Here" response. The user hears fast busy.
- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. Communication Manager provides the new connected party information by updating the Contact header in an UPDATE message. Level 3 does not use the UPDATE message for this purpose.
- **Outbound Calling Party Number (CPN) Block**: To support outbound privacy calls (calling party number blocking), Communication Manager sends "anonymous" as the calling number in the SIP From header and uses the P-Asserted-Identity (PAI) header to pass the actual calling party number. At the time of the compliance testing, Level 3 did not support use of the PAI header for this purpose so these calls were rejected. This functionality is available directly from Level 3 using network feature access codes to enable or disable CPN blocking on a call-by-call basis but was not tested. Since testing was completed, Level 3 has added support for the PAI header for this purpose but it has not been compliance tested with Avaya.

2.3. Support

For technical support on Level 3 SIP Trunking, contact Level 3 using the Customer Center links at www.level3.com or by calling 1-877-2LEVEL3.

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

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Level 3 SIP Trunking. This is the configuration used for compliance testing.

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

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

Located at the edge of the enterprise is the 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. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

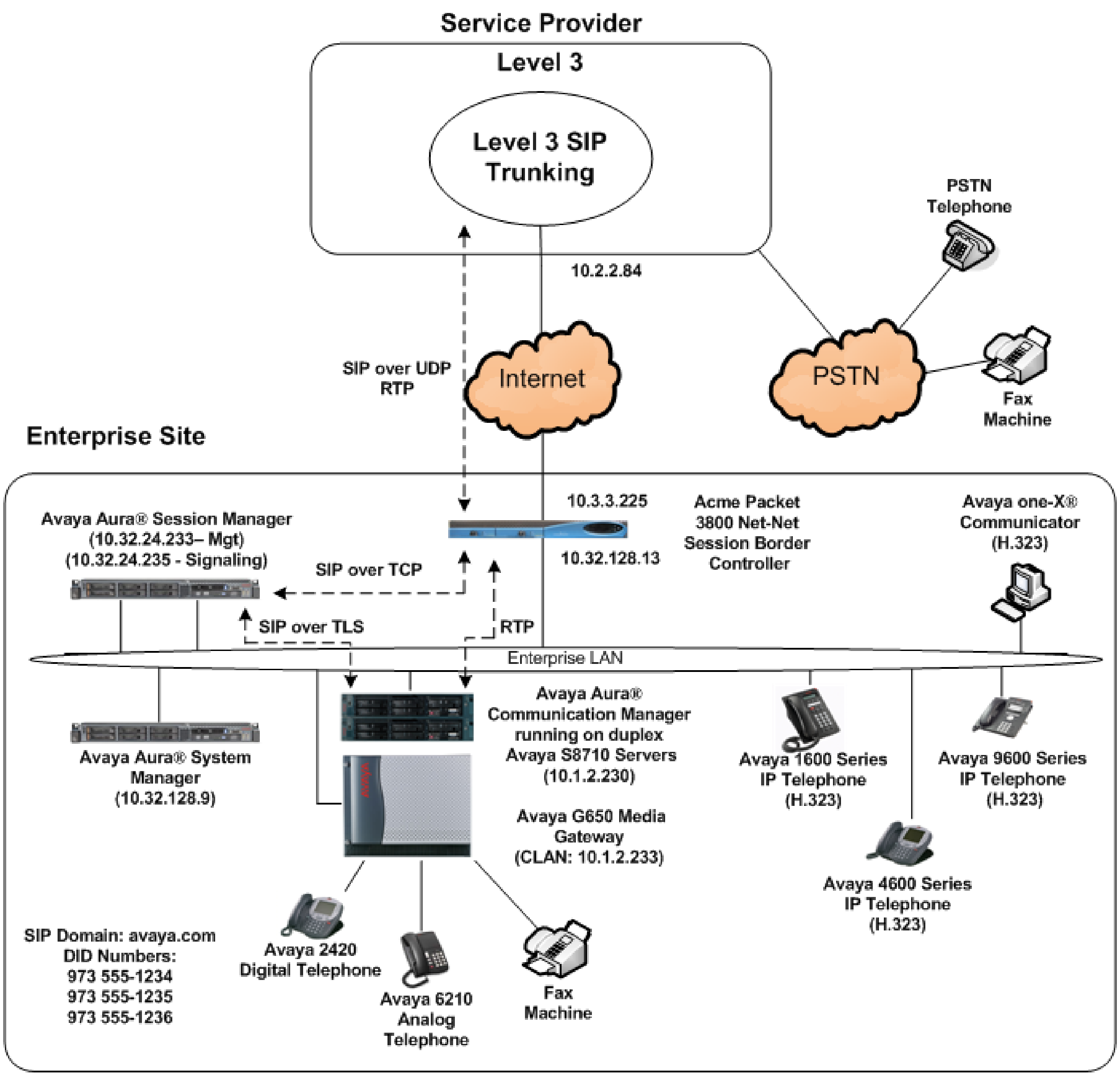


Figure 1: Avaya IP Telephony Network using Level 3 SIP Trunking

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

For inbound calls, the calls flow from the service provider to the 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 such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. The Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to the 3800 Net-Net SBC. From the 3800 Net-Net SBC, the call is sent to Level 3 SIP Trunking.

Level 3 can support 10 digit or E.164 numbering formats for authentication of the calling party. For the compliance test, 10 digit numbering was used for this purpose. Thus for outbound calls, the enterprise sent 10 digits in the SIP source headers (i.e., From, Contact, and P-Asserted-Identity). The enterprise was configured to send 11 digits in the SIP destination headers (Request URI and To). For inbound calls, Level 3 sent 10 digits in both the source headers and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	**Release**
Avaya S8710 Server Pair	Avaya Aura® Communication Manager 5.2.1 SP10 (R015x.02.1.016.4-19191)
Avaya G650 Media Gateway • IP Server Interface (IPSI) TN2312BP • Control LAN (CLAN) TN799DP • IP Media Processor (MEDPRO) TN2602AP	 HW15 FW054 HW01 FW040 HW02 FW061
Avaya S8800 Server	Avaya Aura® System Manager 6.1 SP5 (Build 6.1.0.0.7345-6.1.5.502) (System Platform 6.0.3.3.3)
Avaya S8800 Server	Avaya Aura® Session Manager 6.1 SP5 (Build asm-6.1.5.0.615006)
Avaya 1608 IP Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.3.00B
Avaya 4621SW IP Telephone (H.323)	2.9.2
Avaya 9640 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1 SP2
Avaya one-X® Communicator (H.323)	6.0
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)
Level 3 SIP Trunking Solution Components	
Component	**Release**
Level 3 Enterprise Edge	Version 1

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 Communication Manager

This section describes the procedure for configuring Communication Manager for Level 3 SIP Trunking. A SIP trunk is established between Communication Manager and Session Manager for use by traffic to and from Level 3. 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. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 800 SIP trunks are available and 208 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  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 800   200
           Maximum Concurrently Registered IP Stations: 18000 5
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 800   208
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

5.2. System Features

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

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

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

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

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

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the CLAN circuit pack ***(clan1***) and for Session Manager (***bvSM***). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
bvSM                10.32.24.235
clan1               10.1.2.233
default             0.0.0.0
medpro1             10.1.2.235
procr                . . .
procr1              10.1.2.11
procr2              10.1.2.21
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, G.729A and G.711MU were tested using IP codec set 4. To use these codecs, enter ***G.729A*** and ***G.711MU*** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields.

```
change ip-codec-set 4                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 4

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

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

```
change ip-codec-set 4                                           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
```

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 4 was chosen for the service provider trunk. Use the **change ip-network-region 4** command to configure region 4 with the following parameters:

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

```
change ip-network-region 4                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 4
Location:         Authoritative Domain: avaya.com
    Name: SP Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 4              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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 3**, define the IP codec set to be used for traffic between region 4 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 4 will be used for calls between region 4 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 4 will automatically create a complementary table entry on the IP network region 1 form for destination region 4. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4**.

```
change ip-network-region 4                                      Page   3 of  19

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 34 was used and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). The transport method specified here is used between the Communication Manager and Session Manager.
- Set the **IMS Enabled** field to ***n***. This specifies the Communication Manager will serve as an Access Element for Session Manager.
- Set the **Near-end Node Name** to ***clan1***. This node name maps to the IP address of the CLAN circuit pack as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***bvSM***. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value for the chosen transport protocol. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). At the time of Session Manager installation, a SIP connection between Communication Manager and Session Manager would have been established for use by all Communication Manager SIP traffic using the well-known port value for TLS. By creating a new signaling group with a separate port value, a separate SIP connection is created between Communication Manager and Session Manager for SIP traffic to the service provider. As a result, any signaling group or trunk group settings (**Section 5.7**) will only affect the service provider traffic and not other SIP traffic at the enterprise. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5066***.

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

```
add signaling-group 34                                          Page   1 of   1
                                SIGNALING GROUP

 Group Number: 34             Group Type: sip
                        Transport Method: tls
  IMS Enabled? n





   Near-end Node Name: clan1                  Far-end Node Name: bvSM
 Near-end Listen Port: 5066                 Far-end Listen Port: 5066
                                         Far-end Network Region: 4
Far-end Domain: avaya.com

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

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 34 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 the **Signaling Group** to the signaling group shown in **Section 5.6**.
- 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 34                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 34                   Group Type: sip           CDR Reports: y
  Group Name: SP Trunk                    COR: 1        TN: 1        TAC: 134
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                      Signaling Group: 34
                                                    Number of Members: 10
```

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

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

```
add trunk-group 34                                              Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                              Redirect On OPTIM Failure: 15000

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

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

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

```
add trunk-group 34                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y

                     Numbering Format: public
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? y
                                                Replace Unavailable Numbers? y


 Show ANSWERED BY on Display? y
```

On **Page 4**, set the **Network Call Redirection** field to ***n***. Set the **Send Diversion Header** field to ***y*** 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 Level 3.

```
add trunk-group 34                                              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
```

5.8. Calling Party Information

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

In the sample configuration, multiple DID numbers were assigned for testing. These numbers were assigned to the extensions 30023, 30024 and 30025. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these extensions.

```
change public-unknown-numbering 0                               Page   1 of   1
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext           Trk       CPN            CPN
Len Code          Grp(s)    Prefix         Len
                                                    Total Administered: 4
 5  3                                      5           Maximum Entries: 9999
 5  30023         34        9735551234     10
 5  30024         34        9735551235     10
 5  30025         34        9735551236     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 public-unknown-numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 3 will send the calling party number as the **CPN Prefix** plus the extension number.

```
change public-unknown-numbering 0                                    Page   1 of   1
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext             Trk        CPN            CPN
Len Code            Grp(s)     Prefix         Len
                                Total Administered: 1
 5  3               34         97355          10          Maximum Entries: 9999
```

5.9. Outbound Routing

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

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

       Dialed   Total  Call    Dialed   Total  Call      Dialed   Total  Call
       String   Length Type    String   Length Type      String   Length Type
     1            3    dac
     2            5    ext
     222          5    aar
     3            5    ext
     3234         7    ext
     4            5    ext
     5            5    ext
     6            5    ext
     7            7    ext
     8            1    fac
     9            1    fac
     *            3    fac
     #            3    fac
```

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

```
change feature-access-codes                                     Page   1 of   8
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *01
         Abbreviated Dialing List2 Access Code: *02
         Abbreviated Dialing List3 Access Code: *03
Abbreviated Dial - Prgm Group List Access Code: *04
                      Announcement Access Code: *05
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: *13    All: *11    Deactivation: *12
```

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 34** which contains the SIP trunk to the service provider (as defined next).

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

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     1    1     34       op           n
    0                     11   11    34       op           n
    011                   10   18    34       intl         n
    1800                  11   11    34       fpna         n
    1877                  11   11    34       fpna         n
    1908                  11   11    34       fpna         n
    411                   3    3     34       svcl         n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 34 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 34 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.
- **LAR**: ***next***

```
change route-pattern 34                                         Page   1 of   3
                    Pattern Number: 34  Pattern Name: SP Route
                             SCCAN? n     Secure SIP? n
    Grp  FRL NPA Pfx Hop Toll No.  Inserted                           DCS/ IXC
    No           Mrk Lmt List Del  Digits                             QSIG
                             Dgts                                     Intw
 1: 34   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                                         next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

6. Configure Session Manager

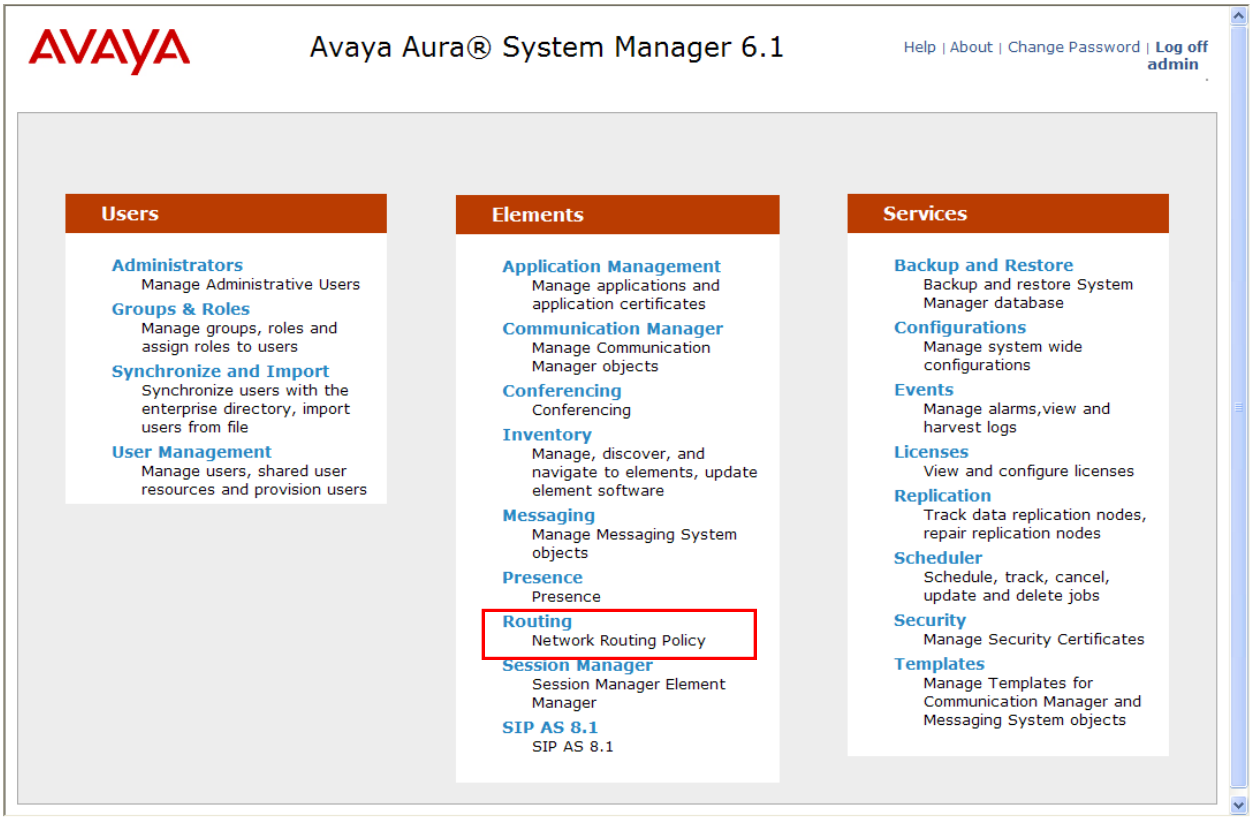
This section provides the procedures for configuring Session Manager. The procedures include configuring the following items:

- 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 SBC and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which governs which Routing Policy is used to service a call.
- Session Manager, corresponding to the Session Manager Server to be managed by System Manager.

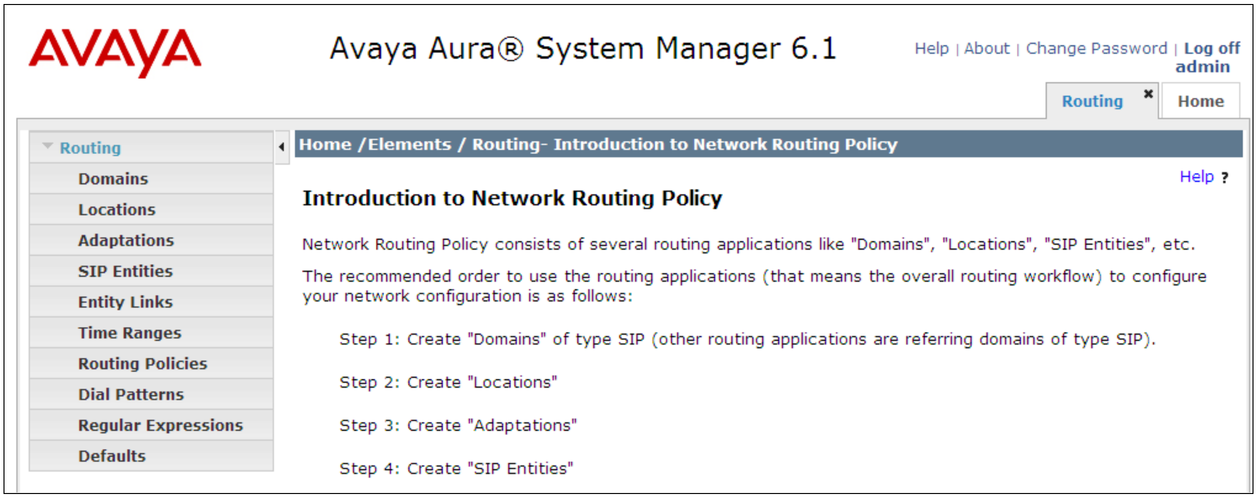
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **Login** (not shown). The **Home** page is displayed. The links displayed below will be referenced in subsequent sections to navigate to items requiring configuration. Most items will be located under the **Elements → Routing** link highlighted below.



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

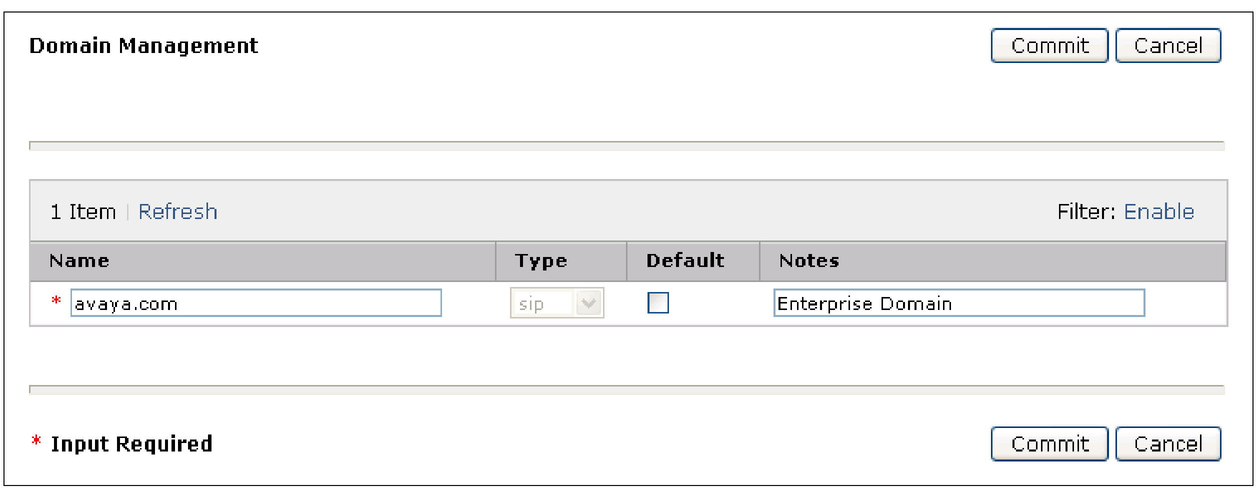


6.2. Specify SIP Domain

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

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

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



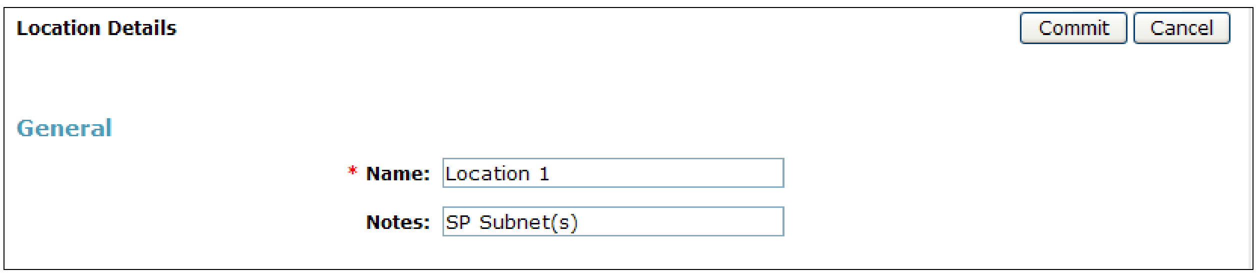
6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the location named ***Location 1***, which includes all equipment on 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 (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

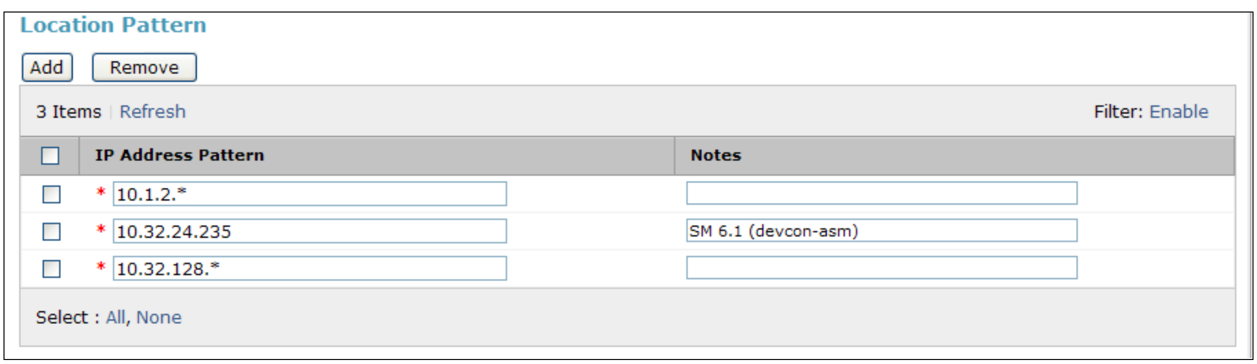
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).



Scroll down to the **Location Pattern** section. Click **Add** and enter the following values. Use default values for all remaining fields.

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

Click **Commit** to save.



6.4. Add Adaptation Module

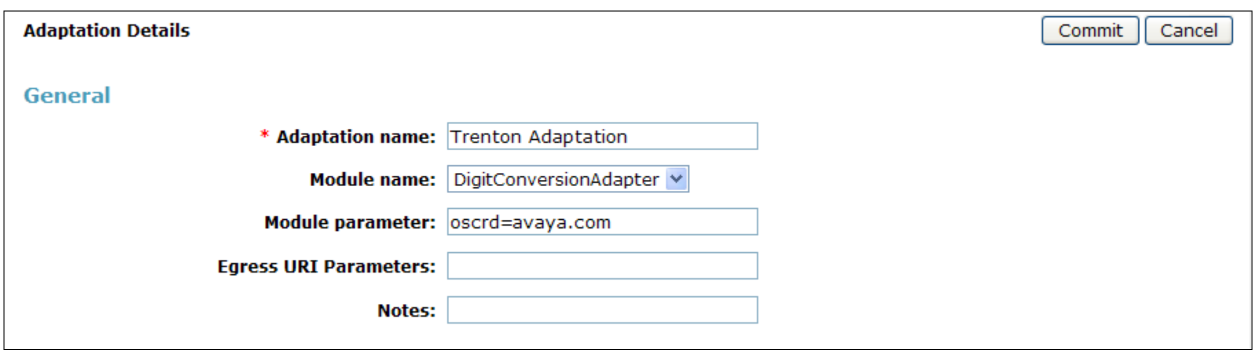
Session Manager can be configured with adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules 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 was applied to the Communication Manager SIP entity and converts the domain part of the inbound PAI header to the enterprise domain (***avaya.com***). In addition, this adaptation maps inbound DID numbers from Level 3 to local Communication Manager extensions. The second adaptation is applied to the 3800 Net-Net SBC SIP entity and converts the domain part of the outbound Request URI header from Session Manager containing the enterprise domain to the Level 3 SIP proxy IP address.

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

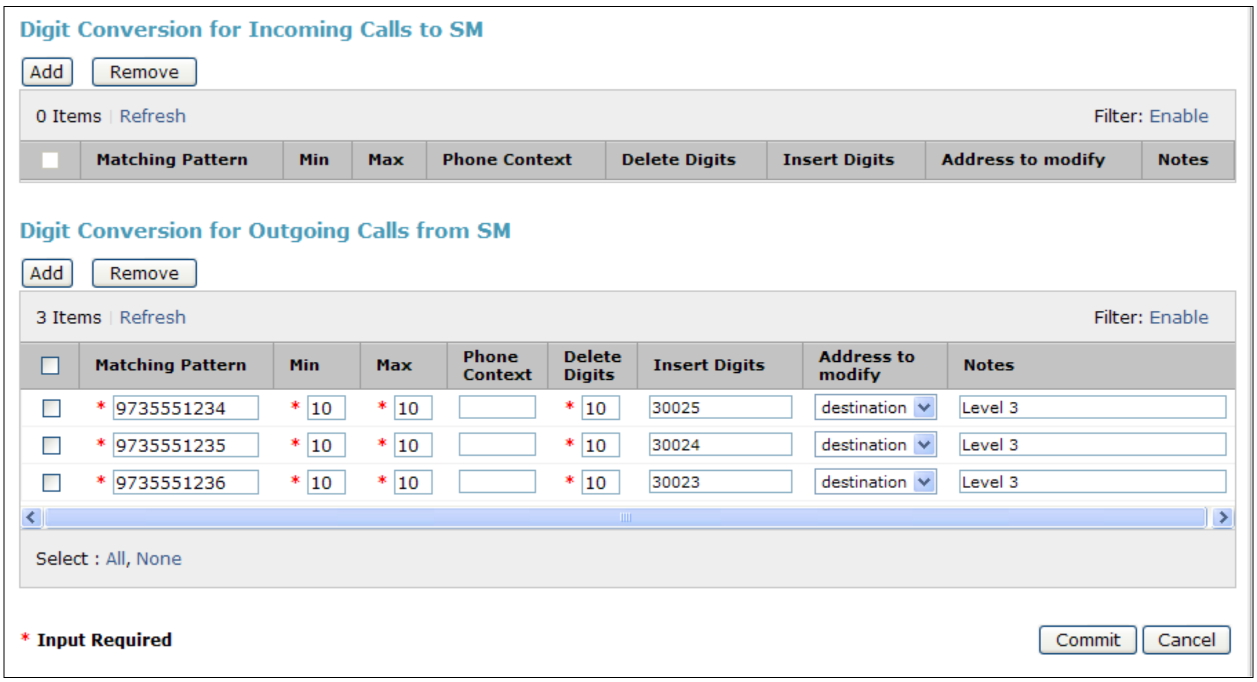
- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***osrcd=avaya.com***. This is the OverrideSourceDomain parameter. This parameter replaces the domain in the inbound PAI header with the given value.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



To map inbound DID numbers from Level 3 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.


Digit Conversion for Incoming Calls to SM

Add Remove

0 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes

Digit Conversion for Outgoing Calls from SM

Add Remove

3 Items | Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
	* 9735551234	* 10	* 10		* 10	30025	destination	Level 3
	* 9735551235	* 10	* 10		* 10	30024	destination	Level 3
	* 9735551236	* 10	* 10		* 10	30023	destination	Level 3

Select : All, None

* Input Required

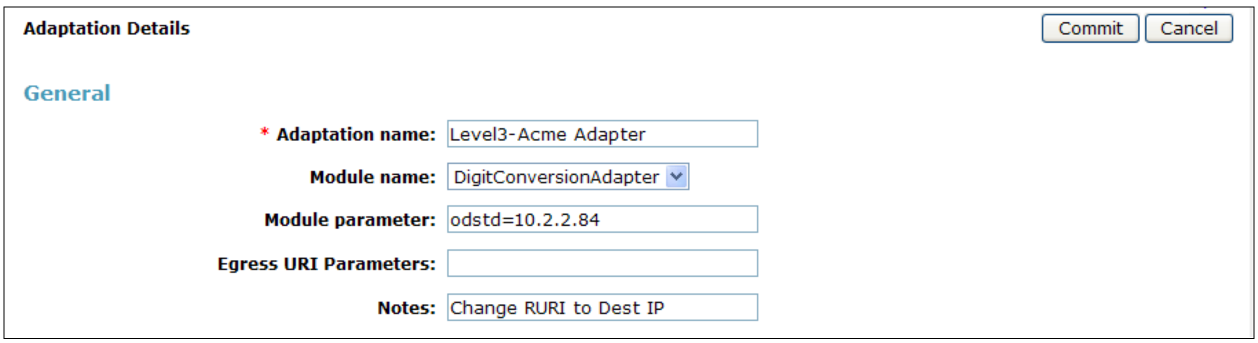
Commit Cancel

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 (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Adaptation name:** Enter a descriptive name for the adaptation.
- **Module name:** Enter ***DigitConversionAdapter***.
- **Module parameter:** Enter ***odstd=10.2.2.84.*** This is the OverrideDestinationDomain parameter. This parameter replaces the domain in the Request URI header with the given value for outbound only.
- **Notes:** Add a brief description (optional).

Click **Commit** to save.



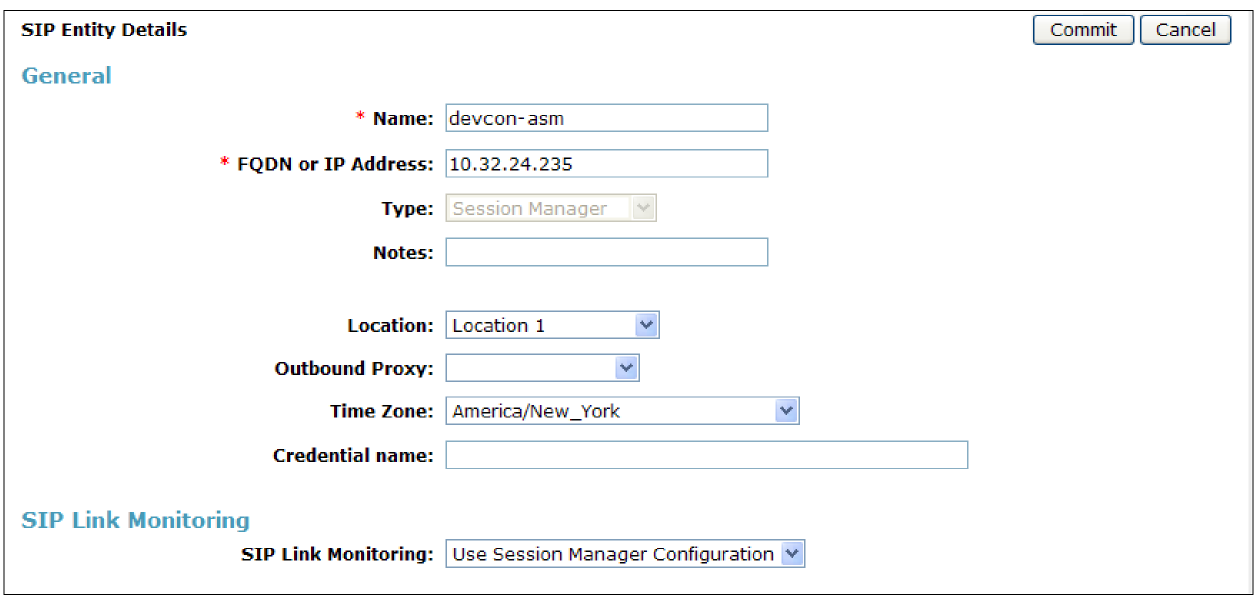
6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and the 3800 Net-Net SBC. Navigate to **Routing → SIP Entities** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter ***Session Manager*** for Session Manager, ***CM*** for Communication Manager and ***SIP Trunk*** for the 3800 Net-Net SBC.
- **Adaptation:** This field is only present if **Type** is not set to ***Session Manager***. If applicable, select the appropriate **Adaptation name** created in **Section 6.4** that will be applied to this entity.
- **Location:** Select the location that applies to the SIP entity being created. For the compliance test, all components were located in location ***Location 1***.
- **Time Zone:** Select the time zone for the location above.

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



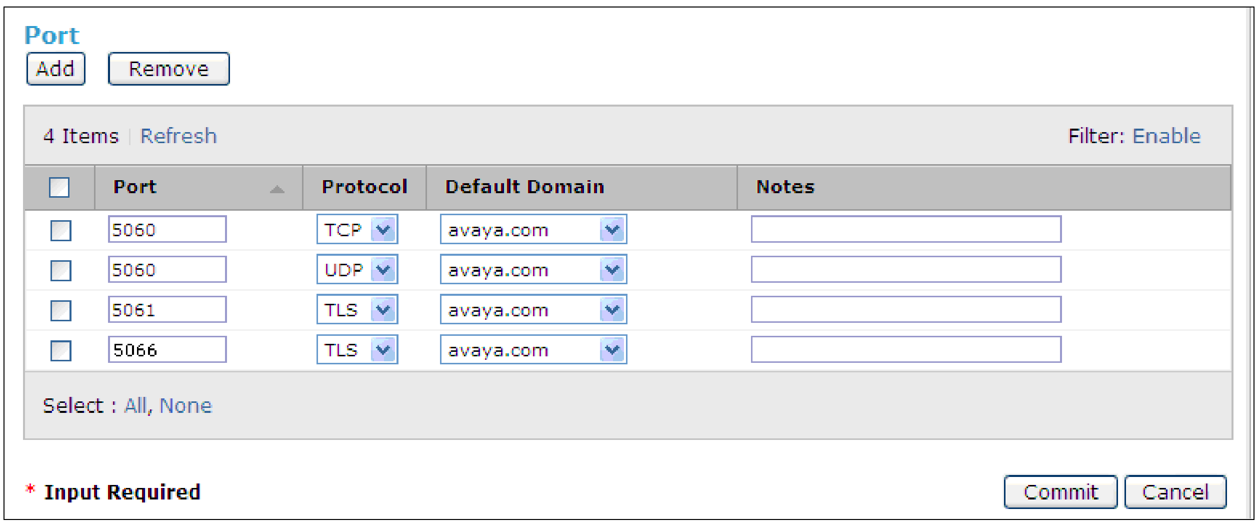
To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities.

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

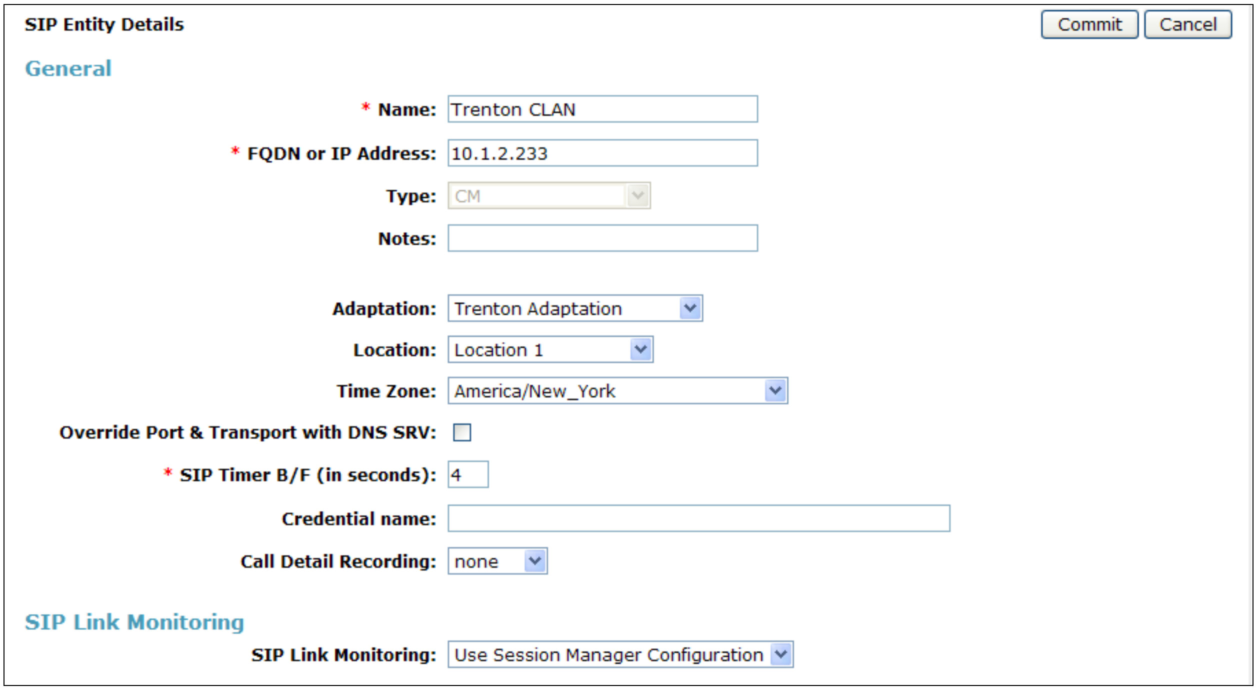
- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP domain.

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

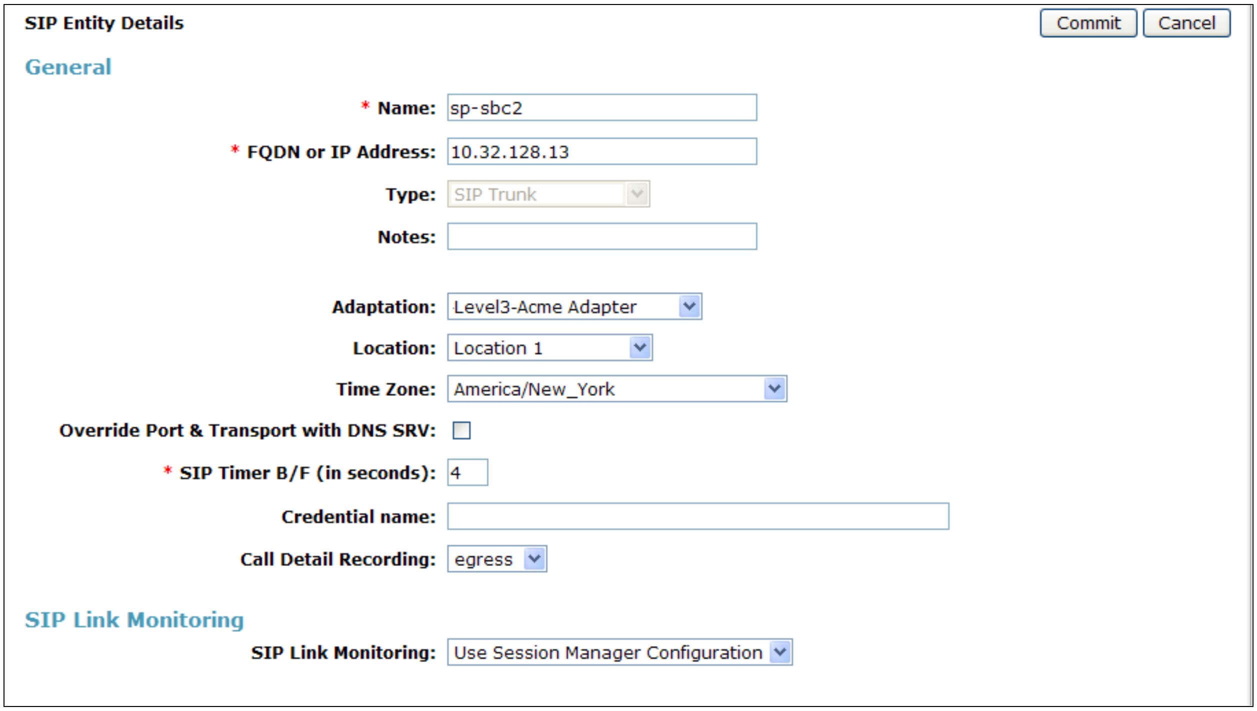
For the compliance test, four port entries were used. The first three are the standard ports used for SIP traffic: port 5060 for UDP/TCP and port 5061 for TLS. In addition, port 5066 defined in **Section 5.6** for use with service provider SIP traffic between Communication Manager and Session Manager was added to the list.



The following screen shows the addition of Communication Manager. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, this requires the creation of a separate SIP entity for Communication Manager other than the one created at Session Manager installation for use with all other SIP traffic. The **FQDN or IP Address** field is set to the IP address of the Avaya Server running Communication Manager. For the **Adaptation** field, select the adaptation module previously defined for Communication Manager in **Section 6.4**. The **Location** field is set to ***Location 1*** which is the location defined for the subnet where Communication Manager resides.



The following screen shows the addition of the 3800 Net-Net SBC. The **FQDN or IP Address** field is set to the IP address of its 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 ***Location 1*** which is the location defined for the subnet where the 3800 Net-Net SBC resides.

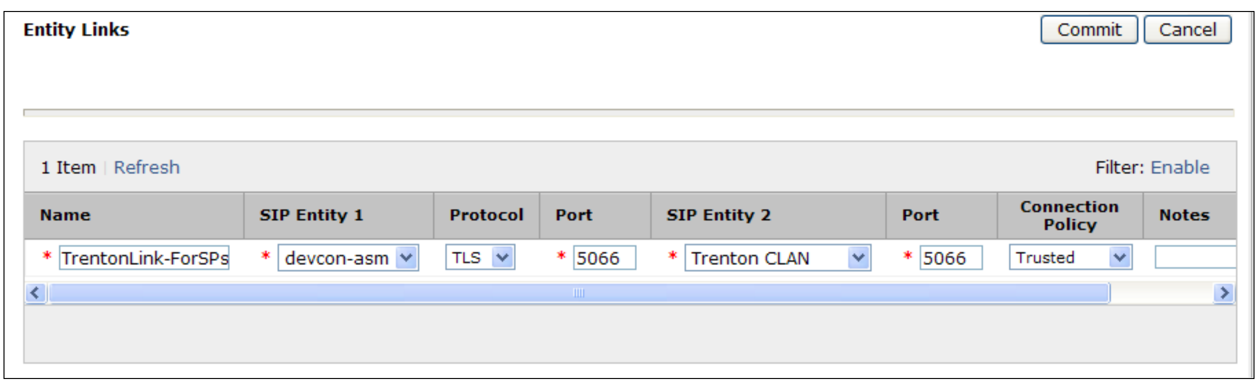


6.6. Add Entity Links

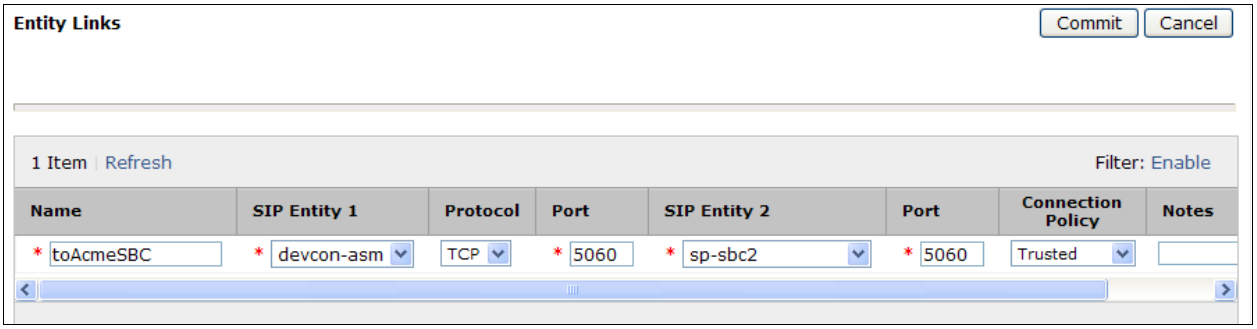
A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the 3800 Net-Net SBC. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the Communication Manager Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For the Communication Manager Entity Link, select the Communication Manager SIP Entity defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **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 screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.



The following screen illustrates the Entity Link to the 3800 Net-Net SBC.



6.7. Add Routing Policies

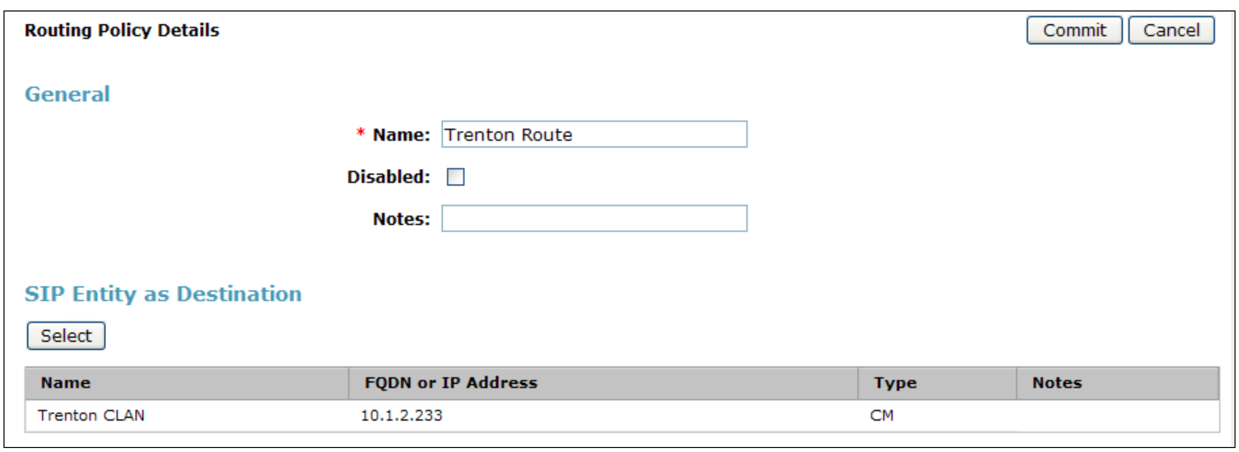
Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added: one for Communication Manager and one for the 3800 Net-Net SBC. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

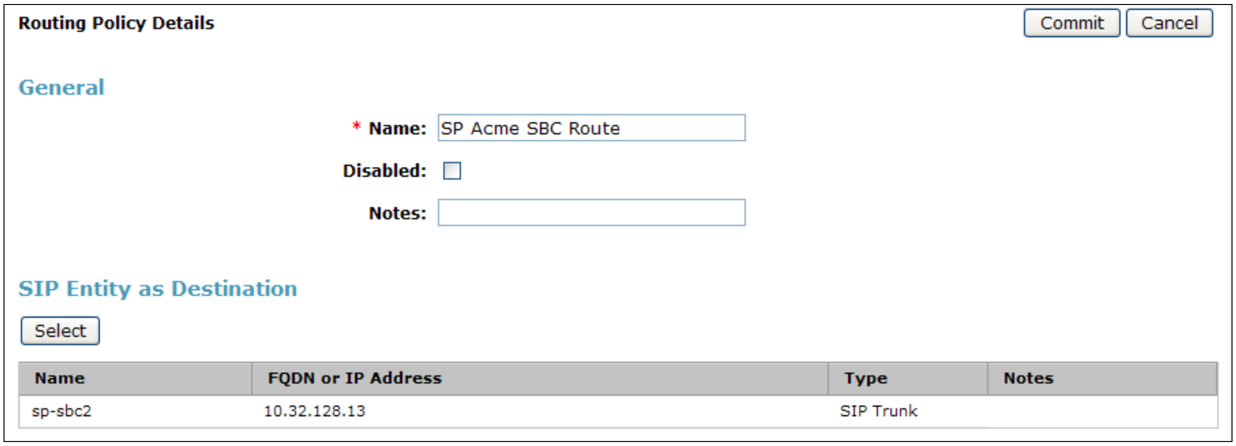
In the **General** section, enter the following values. Use default values for all remaining fields.

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

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

The following screens show the Routing Policies for Communication Manager and the 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 needed to route calls from Communication Manager to Level 3 and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane (**Section 6.1**) and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

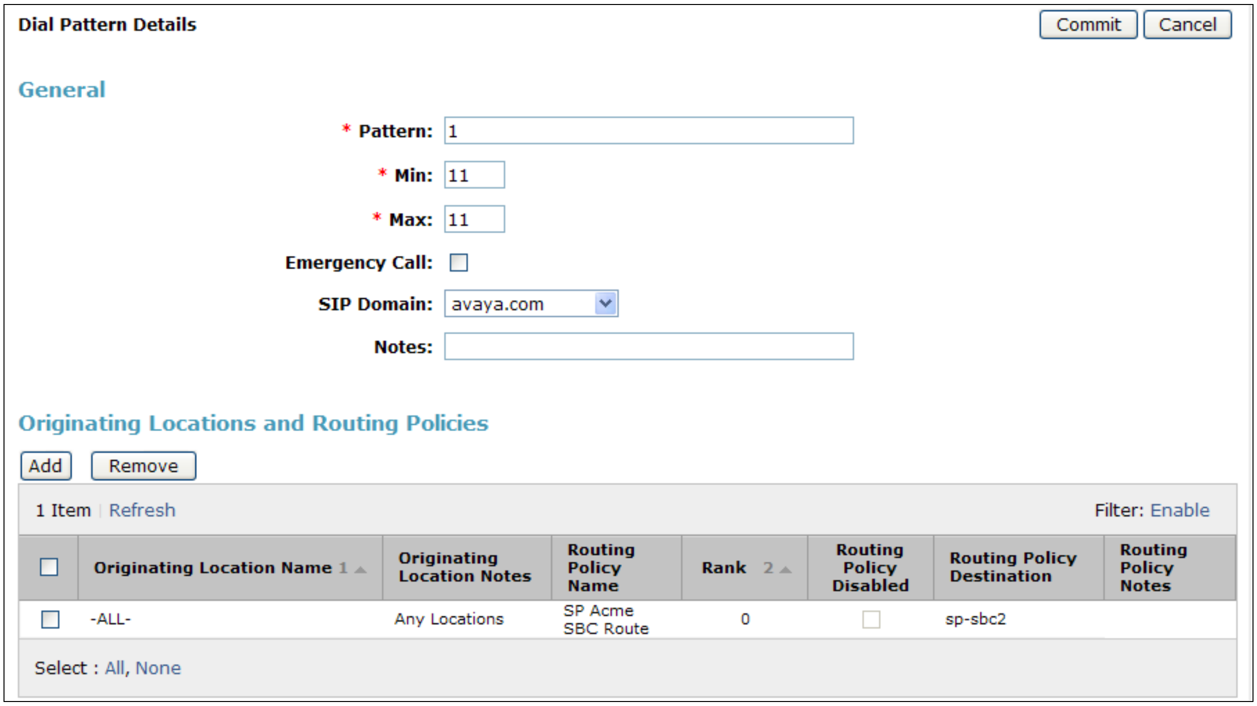
In the **General** section, enter the following values. Use default values for all remaining fields.

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

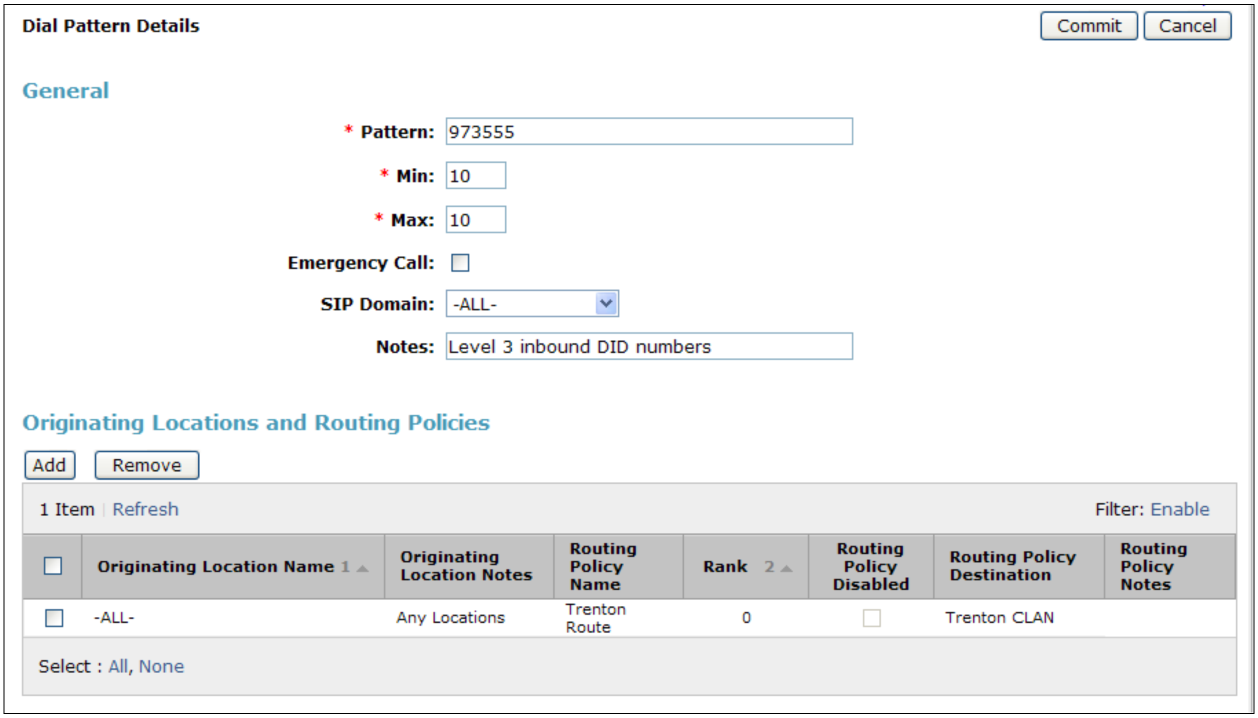
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used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

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

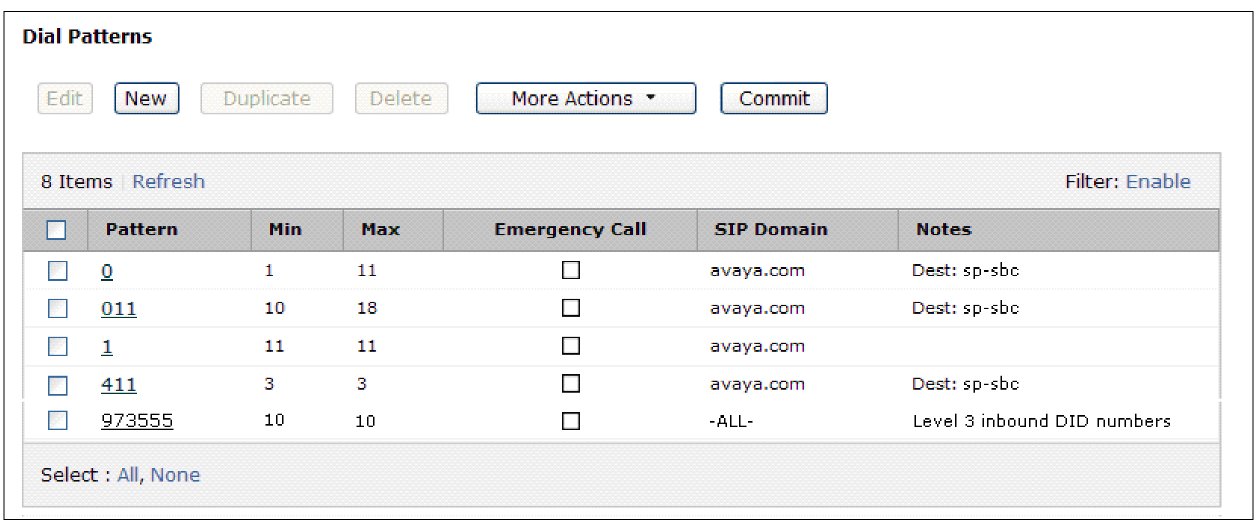
Two examples of the dial patterns used for the compliance test are shown below. The first example shows that 11 digit numbers that begin with a 1 and have a destination domain of ***avaya.com*** from ***ALL*** locations uses route policy ***SP Acme SBC route***.



The second example shows that **10** digit numbers that start with ***973555*** to any domain and originating from any location uses route policy ***Trenton Route***. These are the DID numbers assigned to the enterprise from Level 3.



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



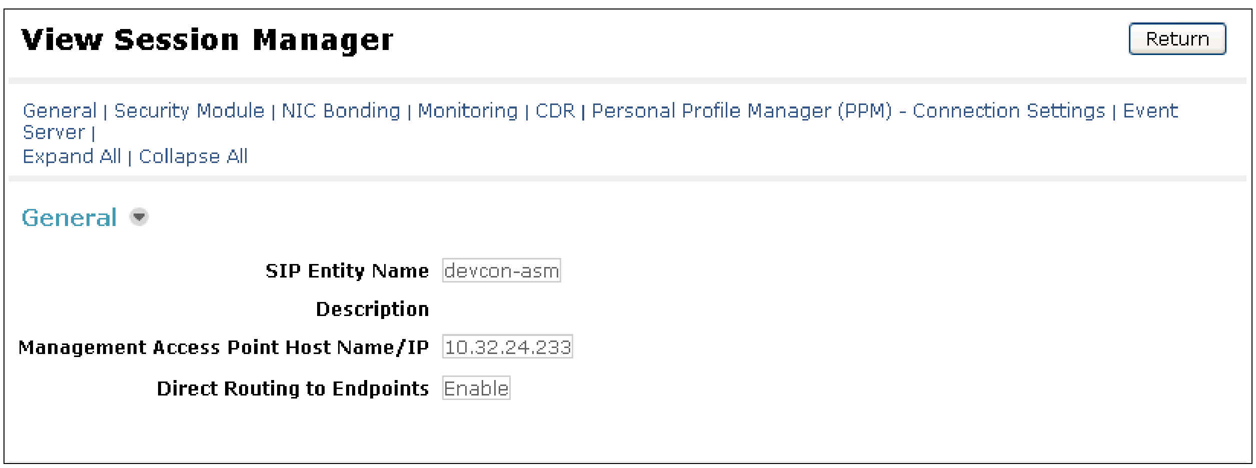
6.9. Add/View Session Manager

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

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

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

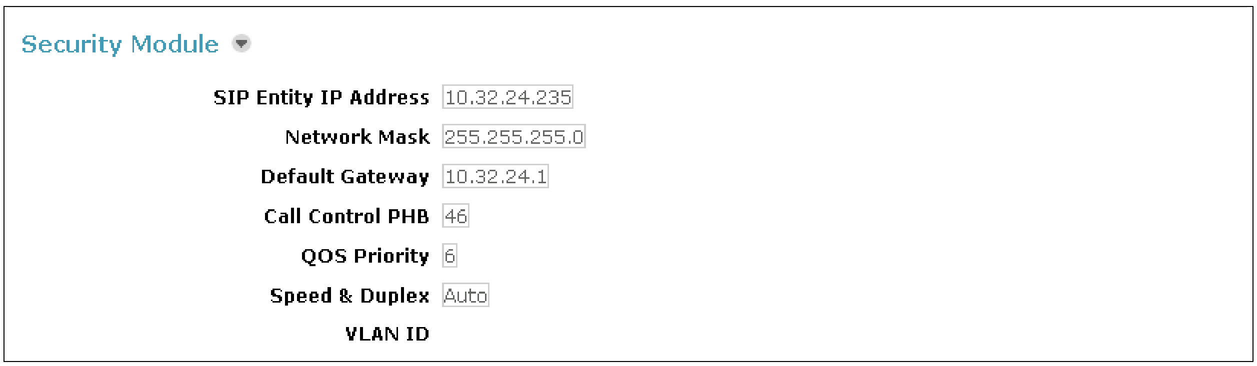
The screen below shows the Session Manager values used for the compliance test.



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

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

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



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

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

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

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

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

7.1. Physical Interfaces

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

7.1.1. Public Interface

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

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

7.1.2. Private Interface

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

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

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

7.2. Network Interfaces

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

7.2.1. Public Interface

Create a network-interface to the public side of the Acme. If IP VPN connectivity is purchased from Level 3 for access to the SIP Trunking service, as opposed to using direct Internet connectivity, then a sub-port-id will also need to be provisioned on the network-interface. Details may be obtained from Level 3. 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 → 10.3.3.225**
4. Enter **netmask → 255.255.255.224**
5. Enter **gateway → 10.3.3.254**
6. Enter **dns-ip-primary → 10.3.184.199**
7. Enter **hip-ip-list → 10.3.3.225**
8. Enter **icmp-ip-list → 10.3.3.225**
9. Enter **done**
10. Enter **exit**

7.2.2. Private Interface

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

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

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

7.3. Realms

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

7.3.1. Outside Realm

Create a realm for the external network.

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

7.3.2. Inside Realm

Create a realm for the internal network.

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

7.4. Steering-Pools

Steering pools define sets of ports that are used for steering media flows thru the 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 → 10.3.3.225**
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 5.5**.

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 defines the SIP daemon location, and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere.

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

7.7. SIP Interfaces

The SIP interface defines the SIP signaling interface (IP address and port) on the 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 → 10.3.3.225**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → TCP**

d. Enter **allow-anonymous → agents-only**
e. Enter **done**
f. Enter **exit**
5. Enter **stop-recurse → 401,407**
6. Enter **done**
7. Enter **exit**

7.7.2. Inside SIP Interface

Create a sip-interface for the inside network.

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

7.8. Session-Agents

A session-agent defines an internal "next hop" signaling entity for the SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent is defined for the service provider (outside) and Session Manager (inside). SIP header manipulations can be applied to the 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 → 10.2.2.84**
3. Enter **ip-address → 10.2.2.84**
4. Enter **port → 5070**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → DynamicTCP**
8. Enter **realm-id → EXTERNAL**
9. Enter **description → Level 3**
10. Enter **ping-method → OPTIONS**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid → inManFromSP**
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 → 10.32.24.235**
3. Enter **ip-address → 10.32.24.235**
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 → SM_SPenv**
10. Enter **ping-method →**
11. Enter **ping-interval → 0**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid → inManFromSM**
14. Enter **done**
15. Enter **exit**

7.9. Local Policies

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

7.9.1. INTERNAL2 to EXTERNAL

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

1. Enter **session-router → local-policy**
2. Enter **from-address → ***
3. Enter **to-address → ***
4. Enter **source-realm → INTERNAL2**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 10.2.2.84**
    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 → 10.32.24.235**
    b. Enter **realm → INTERNAL2**
    c. Enter **terminate-recursion → enabled**
    d. Enter **app-protocol → SIP**
    e. Enter **state → enabled**
    f. Enter **done**
    g. Enter **exit**
7. Enter **done**
8. Enter **exit**

7.10. SIP Manipulations

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

- inManFromSM – A set of SIP header manipulation rules (HMRs) on traffic from Session Manager to the SBC.
- inManFromSP – A set of SIP header manipulation rules on traffic from the service provider (Level 3) to the SBC.
- outManToSP - A set of SIP header manipulation rules on traffic from the SBC to service provider (Level 3).

7.10.1. Session Manager to SBC

The following set of SIP HMRs is applied to traffic from the Session Manager to the SBC. In some call flows the user part of the SIP Contact header 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 → add-X**
   b. Enter **type → header-value**
   c. Enter **action → replace**
   d. Enter **match-val-type → any**
   e. Enter **comparison-type → pattern-rule**
   f. Enter **new-value → $strcon.$strval.$0**
   g. Enter **done**
   h. Enter **exit**
9. Enter **done**
10. Enter **exit**

7.10.2. Level 3 to SBC

The following set of SIP HMRs is applied to traffic from Level 3 to the SBC. To create this set of SIP HMRs:

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

7.10.2.1 Increase Max-Forwards Value

This rule increases the Max-Forwards value in an incoming INVITE from Level 3. On incoming PSTN calls to an enterprise SIP phone, the Max-Forwards value in the incoming SIP INVITE was too small to allow the message to traverse all the SIP hops internal to the enterprise to reach the SIP phone. Thus, the SBC was used to increase this value when the INVITE arrived at the SBC from the Level 3.

1. Enter **header-rule**
2. Enter **name → IncrMaxFwd**
3. Enter **header-name → Max-Forwards**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule**
    a. Enter **name → chgval**
    b. Enter **type → header-value**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → 70**
    g. Enter **done**
    h. Enter **exit**
8. Enter **done**
9. Enter **exit**

7.10.3. SBC to Level 3

The following set of SIP HMRs is applied to traffic from the SBC to Level 3.

To create this set of SIP HMRs:

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

5. Enter **done**
6. Enter **exit**

7.10.3.1 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 → case-sensitive**
6. Enter **msg-type → request**
7. Enter **element-rule →**
    a. Enter **name → chgToHost**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value → $REMOTE_IP**
    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.

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.

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 the only the user part of the Contact header as it was originally received from the Session Manager as described in **Section 7.10.1**.

1. Enter **header-rule**
2. Enter **name → storexcontact**
3. Enter **header-name → X-Contact**
4. Enter **action → manipulate**
5. Enter **comparison-type → case-sensitive**

6. Enter **msg-type → request**
7. Enter **methods → INVITE,UPDATE**
8. Enter **element-rule →**
    a. Enter **name → storexcontact**
    b. Enter **type → header-value**
    c. Enter **action → store**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **match-value → (.*)**
    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**

8. Level 3 SIP Trunking Configuration

To use Level 3 SIP Trunking, a customer must request the service from Level 3 using their sales processes. The process can be started by contacting Level 3 via the corporate web site at www.level3.com and requesting information via the online sales links or telephone numbers.

During the signup process, Level 3 will require that the customer provide the public IP address used to reach the 3800 Net-Net SBC at the edge of the enterprise. Level 3 will provide the IP address of the Level 3 SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager, Session Manager, and the SBC configuration discussed in the previous sections.

The configuration between Level 3 and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the Level 3 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.

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 Level 3 SIP Trunking. Level 3 SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Level 3 SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Please refer to **Section 2.2** for any exceptions or workarounds.

11. References

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

[1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.0.3, February 2011.
[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.
[3] *Administering Avaya Aura® Communication Manager*, August 2010, Document Number 03-300509.
[4] *Avaya Aura® Communication Manager Feature Description and Implementation,* August 2010, Document Number 555-245-205.
[5] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
[6] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010.
[7] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Document Number 03-603473.
[8] *Administering Avaya Aura® Session Manager,* Release 6.1, October 2011, Document Number 03-603324.
[9] *Avaya 1600 Series IP Deskphones Administrator Guide Release Release 1.3.x*, May 2010, Document Number 16-601443.
[10] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.
[11] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.
[12] *Administering Avaya one-X® Communicator*, July 2011.
[13] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/
[14] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,* http://www.ietf.org/

Appendix A: 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 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              2011-10-28 11:02:32
       policy-attribute
              next-hop                        10.2.2.84
              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                        10.32.24.235
                realm                           INTERNAL2
                action                          none
                terminate-recursion             enabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol                    SIP
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
media-manager
        state                           enabled
        latching                        enabled
        flow-time-limit                 86400
        initial-guard-timer             300
        subsq-guard-timer               300
        tcp-flow-time-limit             86400
        tcp-initial-guard-timer         300
        tcp-subsq-guard-timer           300
        tcp-number-of-ports-per-flow    2
        hnt-rtcp                        disabled
        algd-log-level                  NOTICE
        mbcd-log-level                  NOTICE
        red-flow-port                   1985
        red-mgcp-port                   1986
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        media-policing                  enabled
        max-signaling-bandwidth         10000000
        max-untrusted-signaling         100
        min-untrusted-signaling         30
        app-signaling-bandwidth         0
        tolerance-window                30
        rtcp-rate-limit                 0
        trap-on-demote-to-deny          enabled
        min-media-allocation            2000
        min-trusted-allocation          4000
        deny-allocation                 64000
        anonymous-sdp                   disabled
        arp-msg-bandwidth               32000
        fragment-msg-bandwidth          0
        rfc2833-timestamp               disabled
```

```
        default-2833-duration          100
        rfc2833-end-pkts-only-for-non-sig enabled
        translate-non-rfc2833-event    disabled
        media-supervision-traps        disabled
        dnsalg-server-failover         disabled
        last-modified-by               admin@135.11.141.142
        last-modified-date             2010-06-16 05:40:01
network-interface
        name                           s0p0
        sub-port-id                    0
        description
        hostname
        ip-address                     10.3.3.225
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.224
        gateway                        10.3.3.254
        sec-gateway
        gw-heartbeat
                state                          disabled
                heartbeat                      0
                retry-count                    0
                retry-timeout                  1
                health-score                   0
        dns-ip-primary                 10.3.184.199
        dns-ip-backup1                 10.3.184.7
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
         hip-ip-list                    10.3.3.225
        ftp-address
         icmp-address                   10.3.3.225
        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                     FULL
        speed                           100
        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                       10.32.24.235
        ip-address                     10.32.24.235
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               StaticTCP
        realm-id                       INTERNAL2
        egress-realm-id
        description                    SM_SPenv
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method
        ping-interval                  0
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid              inManFromSM
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
```

```
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        last-modified-by               admin@192.168.168.37
        last-modified-date             2011-09-20 22:39:03
session-agent
        hostname                       10.2.2.84
        ip-address                     10.2.2.84
        port                           5070
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               DynamicTCP
        realm-id                       EXTERNAL
        egress-realm-id
        description                    Level 3
        carriers
        allow-next-hop-lp              enabled
        constraints                    disabled
        max-sessions                   0
        max-inbound-sessions           0
        max-outbound-sessions          0
        max-burst-rate                 0
        max-inbound-burst-rate         0
        max-outbound-burst-rate        0
        max-sustain-rate               0
        max-inbound-sustain-rate       0
        max-outbound-sustain-rate      0
        min-seizures                   5
        min-asr                        0
        time-to-resume                 0
        ttr-no-response                0
        in-service-period              0
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
```

```
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid              inManFromSP
        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             2011-10-27 16:10:09
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INTERNAL2
        egress-realm-id
        nat-mode                       Public
        registrar-domain               *
        registrar-host                 *
        registrar-port                 5060
        register-service-route         always
        init-timer                     500
        max-timer                      4000
        trans-expire                   32
        invite-expire                  180
        inactive-dynamic-conn          32
        enforcement-profile
        pac-method
        pac-interval                   10
        pac-strategy                   PropDist
        pac-load-weight                1
        pac-session-weight             1
        pac-route-weight               1
        pac-callid-lifetime            600
        pac-user-lifetime              3600
        red-sip-port                   1988
        red-max-trans                  10000
        red-sync-start-time            5000
        red-sync-comp-time             1000
        add-reason-header              disabled
        sip-message-len                4096
        enum-sag-match                 disabled
        extra-method-stats             enabled
        registration-cache-limit       0
        register-use-to-for-lp         disabled
```

```
        options                        max-udp-length=0
        refer-src-routing              disabled
        add-ucid-header                disabled
        proxy-sub-events
        pass-gruu-contact              disabled
        sag-lookup-on-redirect         disabled
        last-modified-by               admin@135.11.207.156
        last-modified-date             2010-11-02 16:18:33
sip-interface
        state                          enabled
        realm-id                       EXTERNAL
        description
        sip-port
                address                        10.3.3.225
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                agents-only
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
```

```
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@192.168.168.37
        last-modified-date             2011-10-27 15:13:47
sip-interface
        state                          enabled
        realm-id                       INTERNAL2
        description
        sip-port
                address                        10.32.128.13
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
```

```
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@135.105.224.163
        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                case-sensitive
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           chgToHost
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $REMOTE_IP
        header-rule
                name                           manipFrom
                header-name                    From
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           From
                        parameter-name
                        type                           uri-host
```

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

```
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods                         INVITE,UPDATE
            match-value
            new-value
            element-rule
                  name                            storeXcontact
                  parameter-name
                  type                            header-value
                  action                          store
                  match-val-type                  any
                  comparison-type                 case-sensitive
                  match-value                     (.*)
                  new-value
      header-rule
            name                            replacecontact
            header-name                     Contact
            action                          manipulate
            comparison-type                 pattern-rule
            msg-type                        request
            methods                         INVITE,UPDATE
            match-value
            new-value
            element-rule
                  name                            replacecontact
                  parameter-name
                  type                            uri-user
                  action                          replace
                  match-val-type                  any
                  comparison-type                 pattern-rule
                  match-value                     (.*)
                  new-value                       $storeXcontact.$storeXcontact.$0
      header-rule
            name                            delXcontact
            header-name                     X-Contact
            action                          delete
            comparison-type                 pattern-rule
            msg-type                        request
            methods                         INVITE,UPDATE
            match-value
            new-value
      header-rule
            name                            manipRefer
            header-name                     Refer-To
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods
            match-value
            new-value
            element-rule
                  name                            chgHostRefer
                  parameter-name
                  type                            uri-host
                  action                          replace
                  match-val-type                  any
                  comparison-type                 case-sensitive
                  match-value
                  new-value                       $REMOTE_IP
      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
sip-manipulation
      name                            inManFromSM
      description                     storecontact
      split-headers
      join-headers
      header-rule
            name                            strcon
            header-name                     Contact
            action                          manipulate
            comparison-type                 case-sensitive
            msg-type                        request
            methods                         INVITE,UPDATE
            match-value
            new-value
            element-rule
                  name                            strval
                  parameter-name
                  type                            uri-user
                  action                          store
                  match-val-type                  any
                  comparison-type                 case-sensitive
                  match-value                     (.*)
                  new-value
      header-rule
            name                            addXcontact
            header-name                     X-Contact
            action                          add
            comparison-type                 pattern-rule
            msg-type                        request
            methods                         INVITE,UPDATE
            match-value
            new-value
            element-rule
                  name                            addX
                  parameter-name
                  type                            header-value
                  action                          replace
                  match-val-type                  any
                  comparison-type                 pattern-rule
                  match-value
                  new-value                       $strcon.$strval.$0
sip-manipulation
      name                            inManFromSP
      description                     Inbound SIP HMRs From SP
      split-headers
      join-headers
```

```
        header-rule
              name                          IncrMaxFwd
              header-name                   Max-Forwards
              action                        manipulate
              comparison-type               case-sensitive
              msg-type                      request
              methods
              match-value
              new-value
              element-rule
                    name                          chgVal
                    parameter-name
                    type                          header-value
                    action                        replace
                    match-val-type                any
                    comparison-type               case-sensitive
                    match-value
                    new-value                     70
        last-modified-by              admin@192.168.168.37
        last-modified-date            2011-10-28 09:50:58
steering-pool
        ip-address                    10.3.3.225
        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.