Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Frontier Communications SIP Trunking (Metaswitch) with Avaya Aura® Communication Manager Release 6.3 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 Frontier Communications SIP Trunking (Metaswitch) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Release 6.3, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints. Frontier Communications 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 Frontier Communications SIP Trunking (Metaswitch) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Release 6.3, Acme Packet 3800 Net-Net Session Border Controller and various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Frontier Communications SIP Trunking service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site comprised of a Communication Manager with an Avaya G450 Media Gateway, an Acme Packet 3800 Net-Net Session Border Controller, and various types of Avaya IP phones running H.323 firmware. Enterprise SIP endpoints are not supported since they require the use of Avaya Aura® Session Manager which is not part of this solution.

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

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various types of H.323 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 types of H.323 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) configured for H.323. Avaya one-X® Communicator can place calls from the local computer or control a separate physical phone. Both of these modes were tested.
- Various call types including: local, long distance, international, outbound toll-free, operator (0), and local directory assistance (411).

- G.729A and G.711MU codecs.
- DTMF transmission using RFC 2833 for voicemail access and navigation on inbound and outbound calls.
- Caller ID presentation and Caller ID restriction.
- Using REFER messages for call transfer off-net to the PSTN.
- Response to incomplete call attempts and trunk errors.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, forwarding and enterprise mobility (extension to cellular)
- Inbound T.38 fax

Items not supported or not tested included the following:

- Inbound toll-free and emergency 911 calls were not tested.
- Frontier Communications SIP Trunking does not support Operator-Assisted call (0 + 10 digits).
- Frontier Communications SIP Trunking does not support T.38 outbound fax calls.

2.2. Test Results

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

- **OPTIONS Response –** Frontier responded to OPTIONS from the enterprise site with "403 From: URI not recognized" instead of "200 OK". Communication Manager treated the 403 response as a legitimate response from the far end for verifying active state of the SIP trunk connection.
- **Codec Not Locked Down on Outbound Calls –** When Communication Manager was configured with G.711MU and G.729A codecs in that preference order, Frontier responded to the outbound INVITE request with only G.711MU in the SDP as expected. However, when Communication Manager was configured with the same 2 codecs but with G.729A as the preferred codec, Frontier responded to the outbound INVITE with both codecs in the SDP (with G.729A listed first) instead of selecting one from the INVITE SDP list. This behavior had no user impact. Calls were successful. Note also that the Frontier SIP Trunking service requires G711MU in the SDP and it will add G711MU if it is not offered.
- **Call to Invalid PSTN Number –** Frontier returned "500 Internal Server Error" to the outbound call INVITE to an invalid PSTN number. A more appropriate status message like "404 Not Found" would be more appropriate.
- **REFER Signaling –** At the end of an off-net call transfer using REFER, Fronter would terminate both legs of the call first, then sent a NOTIFY to the enterprise (indicating "200 OK" for REFER). This post-termination NOTIFY would elicit a "500 Internal Server Error" response from the Acme Packet SBC since the call was already terminated. Frontier also sent an INVITE to the enterprise after accepting the REFER message with

"202 Accepted", but would not Ack the "200 OK" response to the INVITE causing a series of unanswered “200 OK” messages that eventually would cease after 30 to 45 seconds. Though the signaling exchange as described was not completely clean, user experience was not negatively affected (i.e., the call was transferred successfully).

- **User To User Information (UUI) –** When Communication Manager was configured to have the outbound REFER message contain a redirected number as well as User to User information in the Refer-To header, the subsequent INVITE generated by Frontier to the redirected number did not have a User-To-User header for the UUI, therefore UUI was not delivered to the redirected party.
- **Connected Party Display in PSTN Transfers** – After an existing call between a PSTN caller and an enterprise extension was transferred off-net to another PSTN party, the displayed connected party at both PSTN phones (the transferred party and the transfer-to party) showed the transferring party number (DID associated with the transferring extension at the enterprise) instead of the true connected-party number/ID. The true connected party information was conveyed by Communication Manager in SIP signaling messages to the service provider, but this information was not used to update the true connected party number. The PSTN phone display is ultimately controlled by the backbone PSTN carrier, thus this behavior is not necessarily indicative of a limitation of the Frontier SIP Trunking service. It is listed here simply as an observation.

2.3. Support

For technical support on Frontier Communications SIP Trunking, contact Frontier by

- Using the Technical Support link for business customers at http://www.frontier.com, or
- Calling the business customer support number at 877-462-8188 (for former Verizon customers) or 800-921-8102 (for other Frontier customers).

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

3. Reference Configuration

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

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

- Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya Aura® Messaging
- Acme Packet 3800 Net-Net Session Border Controller (SBC)
- Avaya 96x1-Series IP Telephones (H.323)
- Avaya 9600-Series IP Telephones (H.323)
- Avaya 1600-Series IP Telephones (H.323)

- Avaya one-X® Communicator (H.323)
- Fax device

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

The compliance test used Avaya Aura® Messaging for testing voice mail access/navigation and MWI (Messaging Wait Indicator). Other voice messaging application such as Avaya Aura® Communication Manager Messaging could have been used to satisfy this test purpose.

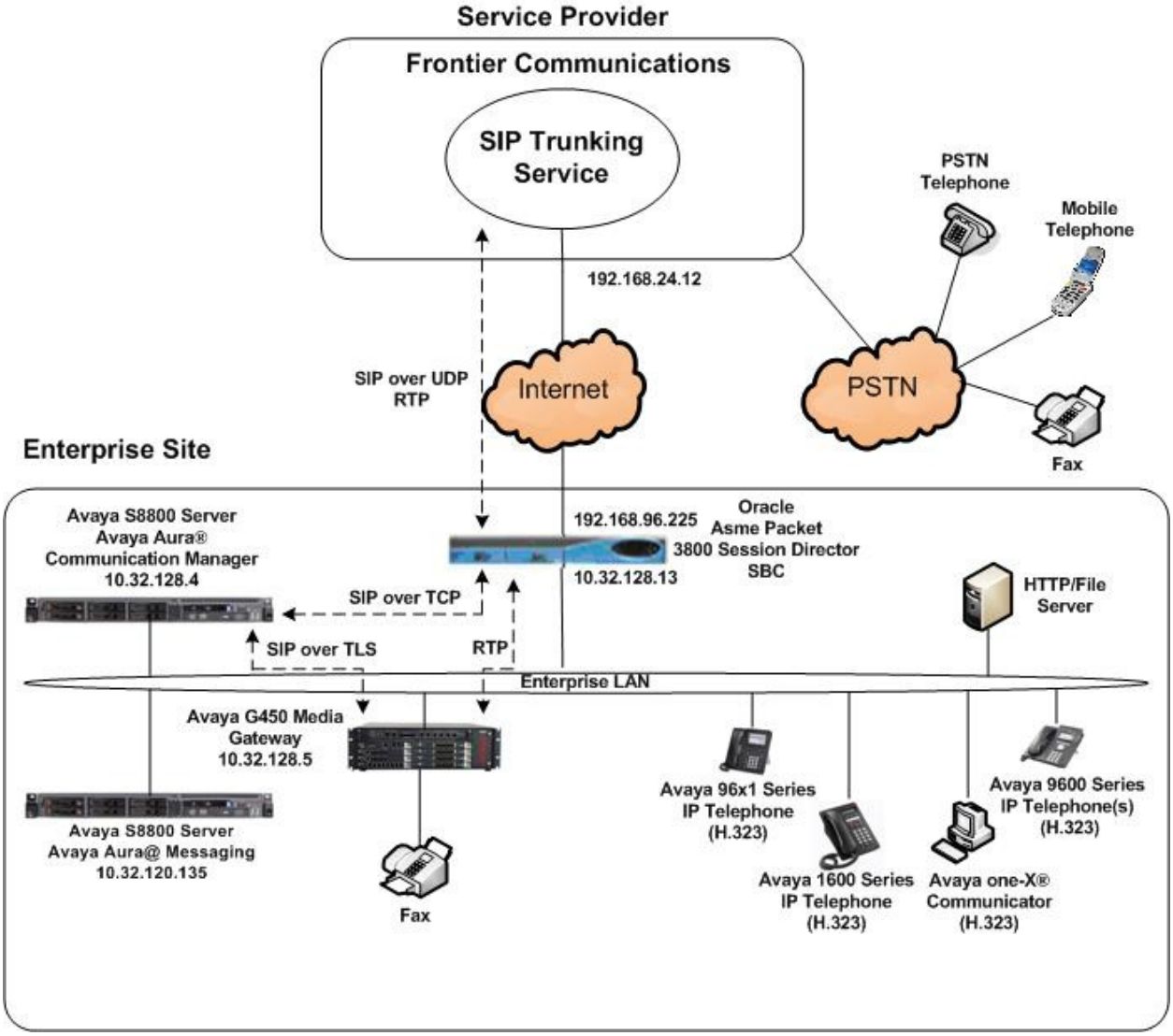

Figure 1: Avaya IP Telephony Network using Frontier Communications SIP Trunking

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

Inbound calls flow from the service provider to the Acme Packet SBC then to Communication Manager. Once the call arrives at Communication Manager, 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 feature treatment such as automatic route selection, digit manipulation and class of service restrictions. Communication Manager routes the call to the Acme Packet SBC after selecting the proper SIP trunk connecting to the SBC. From the Acme Packet SBC, the call is sent to Frontier Communications SIP Trunking.

The administration of Avaya Aura® Messaging and enterprise endpoints is standard. Since the configuration tasks for both are not directly related to the interoperability with the Frontier Communications SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Server	6.3 SP1 (R016x.03.0.124.0-20850)
Avaya G450 Media Gateway – ICC – ANA	33.13.0 HW01 FW001 HW33 FW091
Avaya Aura® Messaging running on Avaya S8800 Server	6.2 SP2 Patch2 (MSG-02.0.823.0-19926)
Acme Packet 3800 Net-Net Session Border Controller	SCX6.3.9 MR-3 GA (Build 528)
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.2
Avaya 9611 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.2.4.08
Avaya 1616 IP Telephone (H.323)	Avaya 1600 IP Deskphone Software Release 1.3 SP3
Avaya one-X® Communicator (H.323)	6.1 SP9 (6.1.9.04-SP9-132)
Fax device	Ventafax Home Version 7.1.212.5421
Frontier Communications SIP Trunking Solution Components	
Component	Release
Acme Packet 4000 Net-Net Session Border Controller	6.2
MSW	8.1

Table 1: Equipment and Software Tested

Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Frontier Communications SIP Trunking. An internal SIP trunk is established between Communication Manager and the Acme Packet SBC for use by signaling traffic to and from the service provider. It is assumed the general installation of Communication Manager and Avaya G450 Media Gateway has been previously completed and is not discussed here.

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

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that ***4000*** SIP trunks are available and ***70*** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  36
          Maximum Concurrently Registered IP Stations: 2400  1
            Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                       Maximum Video Capable Stations: 2400  1
                   Maximum Video Capable IP Softphones: 2400  4
                       Maximum Administered SIP Trunks: 4000  70
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

5.2. System Features

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

```
change system-parameters features                                Page   1 of  20
                            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 ***anonymous*** for both.

```
change system-parameters features                                Page   9 of  20
                         FEATURE-RELATED SYSTEM PARAMETERS

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

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

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

SCCAN PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to enter/verify that node names are properly defined for the IP addresses of the server running Communication Manager (***procr***) and the Acme Packet SBC (***Acme***). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                  IP Address
Acme                   10.32.128.13
cmm                    10.32.128.4
default                0.0.0.0
procr                  10.32.128.4
procr6                 ::
sessionMgr             10.32.24.235
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. Frontier Communications SIP Trunking supports the G.729A and G.711MU codecs for both inbound and outbound calls. Thus, these 2 codecs were included in this codec set. Default values can be used for all other fields.

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

                         IP Codec Set

    Codec Set: 2

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

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

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

                         IP Codec Set

                             Allow Direct-IP Multimedia? n




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

5.5. IP Network Region

Create a distinct 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 8 was chosen for the service provider trunk. Use the **change ip-network-region** command to configure region 8 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain or IP address of the service providers SBC or SIP proxy. In this configuration, an IP address of the service provider SBC was used.
- 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 8                                    Page   1 of  20
                              IP NETWORK REGION
  Region: 8
Location:         Authoritative Domain: 192.168.24.12
    Name: Frontier SIPT         Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                       IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to use for traffic between region 8 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 2 will be used for calls between region 8 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for IP network region 8 will automatically create a complementary table entry on the IP network region 1 form for destination region 8. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4** as shown in the second screen below.

```
change ip-network-region 8                                    Page   4 of  20

 Source Region: 8     Inter Network Region Connection Management     I       M
                                                                    G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    2     y    NoLimit                                          n       t
 2
 3
 4
 5
 6
 7
 8    2                                                            all
 9
```

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

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                    G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                            all
 2    2     y    NoLimit                                          n       t
 3    3     y    NoLimit                                          n       t
 4    4     y    NoLimit                                          n       t
 5
 6
 7
 8    2     y    NoLimit                                          n       t
 9
```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Acme Packet SBC 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 8 was used for this purpose and was configured using the parameters highlighted below.

- Set **Group Type** to ***sip***.
- Set **IMS Enabled** to ***n***.

- Set **Transport Method** to ***tcp***. The transport method specified here is used between Communication Manager and the Acme Packet SBC.
- Set **Peer Detection Enabled** to ***y***. The **Peer-Server** field will automatically be set to ***Others*** and cannot be changed via administration.
- Set **Near-end Node Name** to ***procr***. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set **Far-end Node Name** to ***Acme***. This node name maps to the IP address of the Acme Packet SBC as defined in **Section 5.3**.
- Set **Near-end Listen Port** and **Far-end Listen Port** to ***5060***. Port 5060 is the well-known port for SIP over TCP.
- Set **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set **DTMF over IP** to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk using this signaling group allowing Communication Manager to redirect media traffic to directly between the inside interface of the Acme Packet SBC and the enterprise endpoint. If this value is set to ***n***, then the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completion.
- Set **Alternate Route Timer** to ***15***. This parameter 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 8                                          Page   1 of   2
                              SIGNALING GROUP

 Group Number: 8              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
       Q-SIP? n
    IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y

   Near-end Node Name: procr                Far-end Node Name: Acme
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                       Far-end Network Region: 8
                                 Far-end Secondary Node Name:
Far-end Domain:
                                      Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate           RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3              IP Audio Hairpinning? n
         Enable Layer 3 Test? y              Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n       Alternate Route Timer(sec): 15
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group using the signaling group created in **Section 5.6**. For the compliance test, trunk group 8 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group configured in **Section 5.6**.
- 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 may be retained for all other fields.

```
add trunk-group 8                                              Page   1 of  21
                                TRUNK GROUP

Group Number: 8                      Group Type: sip           CDR Reports: y
  Group Name: DirectTrkToAcme              COR: 1        TN: 1        TAC: 1008
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk           Auth Code? n
                                                Member Assignment Method: auto
                                                          Signaling Group: 8
                                                        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(sec)** 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 or UPDATEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 8                                              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 an enterprise user exercises CPN block on a particular call routed out this trunk. Default values were used for all other fields.

```
add trunk-group 8                                              Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



                     Numbering Format: public
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? y
                                              Replace Unavailable Numbers? y


                                Modify Tandem Calling Number: no



 Show ANSWERED BY on Display? y

 DSN Term? n                       SIP ANAT Supported? n
```

On **Page 4**, set the **Network Call Redirection** field to ***y***. Setting the **Network Call Redirection** flag to ***y*** enables use of the SIP REFER message for off-net call transfers as verified in the compliance test; otherwise the SIP INVITE message will be used for off-net call transfers.

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 **Telephone Event Payload Type** to ***101***, the value preferred by Frontier Communications.

Set **Convert 180 to 183 for Early Media** to ***y*** so that Communication Manager will issue a SIP 183 message for ringing the called enterprise endpoint. This setting was configured to be consistent with Frontier Communications SIP Trunking which uses SIP 183 message for ringing the called PSTN phone.

```
add trunk-group 8                                              Page   4 of  21
                              PROTOCOL VARIATIONS

                                        Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                        Send Transferring Party Information? n
                                    Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                      Send Diversion Header? y
                                    Support Request History? n
                                 Telephone Event Payload Type: 101
                                        Shuffling with SDP? n

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

5.8. Calling Party Information

The calling party number is sent in the SIP From, Contact, PAI and Diversion 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 are assigned by the SIP service provider. It is used to authenticate the caller.

The abbreviated screen below shows a subset of the DID numbers assigned for testing. These 3 numbers were mapped to the 3 enterprise extensions ***41014***, ***41016***, and ***41018***. 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 3 extensions.

```
change public-unknown-numbering 0                              Page   1 of   2
                     NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext  Ext             Trk        CPN       CPN
Len  Code            Grp(s)     Prefix    Len
                                                 Total Administered: 18
 5   41014           8          5853515305  10       Maximum Entries: 240
 5   41016           8          5853515306  10
 5   41018           8          5853515308  10   Note: If an entry applies to
                                                 a SIP connection to Avaya
                                                 Aura(R) Session Manager,
                                                 the resulting number must
                                                 be a complete E.164 number.
```

5.9. Outbound Routing

In the configuration used for the compliance test, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. 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: 3

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   1           4   dac
   3           5   ext
   4           5   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  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code:
                       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: *01    All: *02    Deactivation: *03
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

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

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

          Dialed          Total      Route    Call    Node  ANI
          String         Min  Max  Pattern   Type    Num   Reqd
    0                     1    1     8        op            n
    0                     8    8     deny     op            n
    0                     11   11    8        op            n
    00                    2    2     deny     op            n
    01                    9    17    deny     iop           n
    011                   10   18    8        intl          n
    041                   4    4     8        op            n
    1732                  11   11    8        fnpa          n
    1800                  11   11    8        fnpa          n
    1877                  11   11    8        fnpa          n
    1908                  11   11    8        fnpa          n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used in route pattern 8 for the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group ***8*** (as configured in **Section 5.7)** 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**: The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers.

```
change route-pattern 8                                          Page   1 of   3
                    Pattern Number: 8   Pattern Name: SP Route No SM
                              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: 8    0       1                                                   n   user
 2:                                                                  n   user
 3:                                                                  n   user
 4:                                                                  n   user
 5:                                                                  n   user
 6:                                                                  n   user

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

5.10. Incoming Call Handling Treatment

Incoming call handling treatment is used to manipulate incoming numbers on a particular trunk to facilitate routing of the call to its intended destination. To map incoming DID numbers on the service provider trunk (trunk group 8) to an internal extension, use the **change inc-call-handling-trmt trunk-group 8** command. Set the following:

- Set **Service/Feature** to **public-ntwrk**.
- Set **Number Len** field to the number of digits to use when matching the incoming number.
- Set **Number Digits** to the incoming number to match on.
- Set **Del** to the number of digits to delete from the incoming number.
- Set **Insert** to the internal extension that will replace the deleted 10 digits.

```
change inc-call-handling-trmt trunk-group 8                    Page   1 of  3
                        INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 5853515305       10  41014
 public-ntwrk    10 5853515306       10  41016
 public-ntwrk    10 5853515308       10  41018
```

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

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

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

1. Log in with the appropriate credentials.
2. Enable the Superuser mode by entering **enable** and the appropriate password (prompt will end with #).
3. In Superuser mode, type **configure terminal** and press <ENTER>. The prompt will change to (configure)#.
4. Type the name of the element that will be configured (e.g., **session-router**).
5. Type the name of the sub-element, if any (e.g., **session-agent**).
6. Type the name of the parameter followed by its value (e.g., **ip-address 192.168,0,0**).
7. Type **done**.
8. Type **exit** to return to the previous menu.
9. Repeat steps 4-8 to configure all the elements. When finished, exit from the configuration mode by typing **exit** until being returned to the Superuser prompt.
10. Type **save-config** to save the configuration.
11. Type **verify-config** to verify the configuration
12. Type **activate-config** to activate the configuration.

Once the provisioning is complete, the configuration may be viewed in its entirety by entering the **show running-config** command.

6.1. Physical Interfaces

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

6.1.1. Public Interface

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

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

6.1.2. Private Interface

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

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

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

6.2. Network Interfaces

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

6.2.1. Public Interface

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

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

6.2.2. Private Interface

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

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

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

6.3. 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.

6.3.1. 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**

6.3.2. 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**

6.4. Steering-Pools

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

6.4.1. Outside Steering-Pool

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

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

6.4.2. Inside Steering-Pool

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

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

6.5. 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**

6.6. SIP Configuration

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

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

6.7. SIP Interfaces

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

6.7.1. Outside SIP Interface

Create a sip-interface for the outside network.

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

6.7.2. 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 **redirect-action → Proxy**
6. Enter **stop-recurse → 401,403,407**
7. Enter **done**
8. Enter **exit**

6.8. Session-Agents

A session-agent defines "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 Communication Manager (inside).

6.8.1. Outside Session-Agent

Create a session-agent for the outside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 192.168.24.12**
3. Enter **ip-address → 192.,168. 24.12**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP**
8. Enter **realm-id → EXTERNAL**
9. Enter **description → Frontier**
10. Enter **ping-method → OPTIONS;hops=70**
11. Enter **ping-interval → 120**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid →**
14. Enter **out-manipulationid → outManToSP**
15. Enter **done**
16. Enter **exit**

6.8.2. Inside Session-Agent

Create a session-agent for the inside network.

1. Enter **session-router → session-agent**
2. Enter **hostname → 10.32.128.4**
3. Enter **ip-address → 10.32. 128.4**
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 → Princeton-CM**
10. Enter **ping-method →**
11. Enter **ping-interval → 0**
12. Enter **ping-send-mode → keep-alive**
13. Enter **in-manipulationid →**
14. Enter **out-manipulationid →**
15. Enter **done**
16. Enter **exit**

6.9. 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).

6.9.1. INTERNAL2 to EXTERNAL

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

1. Enter **session-router → local-policy**
2. Enter **from-address →** *
3. Enter **to-address →** *
4. Enter **source-realm → INTERNAL2**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → 192.168.24.12**
    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**

6.9.2. 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 → 10.32.128.4**
    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**

6.10. SIP Manipulations – SBC to Service Provider

SIP manipulation specifies rules for manipulating the contents of specified SIP headers. For the compliance test, one set of SIP manipulations, **outManToSP,** was configured that contains a set of SIP header manipulation rules (HMR) on traffic from the SBC to the service provider network. This SIP manipulation was applied to the outside session agent 192.168.24.12 in **Section 6.8**.

To create this set of SIP HMRs:

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

6.10.1. Change Host of the To Header

This rule replaces the host part of the To header with the service provider's IP address.

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

6.10.2. Change Host of the From Header

This rule replaces the host part of the From header with the public IP address of the Acme Packet 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**

6.10.3. 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 Acme Packet 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**

6.10.4. Change Host of the Diversion Header

This rule replaces the host part of the Diversion header with the public IP address of the Acme Packet 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**

6.10.5. 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**

6.10.6. Delete Alert-Info Header

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

1. Enter **header-rule**
2. Enter **name → delAlert**
3. Enter **header-name → Alert-Info**
4. Enter **action → delete**
5. Enter **comparison-type → case-sensitive**

6. Enter **msg-type → any**
7. Enter **methods →**
8. Enter **done**
9. Enter **exit**

7. Frontier Communications SIP Trunking Configuration

To use Frontier Communications SIP Trunking, a customer must request the service from Frontier Communications using the established sales and provisioning processes.

The customer will need to provide the public IP address used to reach the Acme Packet SBC at the edge of the enterprise network. Frontier Communications will provide the customer the necessary information to configure the SIP-enabled Avaya enterprise solution. The provided information from Frontier Communications includes:

- IP address of the Frontier Communications SIP proxy server / network edge SBC.
- IP addresses and port numbers used for signaling and media through security devices, if any.
- Transport and port number for the SIP connection from enterprise to Frontier Communications.
- Supported codecs and preference order.
- DID numbers assigned to the enterprise.

The above information is used to complete the configurations of Communication Manager and the Acme Packet SBC described in the previous sections.

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

8. 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 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 commands on Communication Manager::

- **list trace station** <extension number> - Traces calls to and from a specific station.
- **list trace tac** <trunk access code number> - Traces calls over a specific trunk group.
- **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
- **status trunk** <trunk group number> - Displays trunk group information.
- **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and Acme Packet 3800 Net-Net Session Border Controller to Frontier Communications SIP Trunking (Metaswitch). Frontier Communications SIP Trunking passed compliance testing. Please refer to **Section 2.2** for any exceptions or limitations observed.

10. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com. Product documentation for Acme Packet products is available from http://support.acmepacket.com.

Avaya Aura® Communication Manager

[1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Release 6.3, Issue 8, May 2013

[2] *Programming Call Vectoring Features in Avaya Aura® Call Center Elite*, Release 6.3, Issue 1, May 2013

Avaya Endpoints

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

[4] *Avaya one-X® Deskphone H.323 for 9630 and 9630G IP Deskphone User Guide,* Document ID 16-300700, June 2013

[5] *Avaya one-X® Deskphone Value Edition 1616 IP Deskphone User Guide,* Document ID 16-601448, June 2013

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

Acme Packet 3800 Net-Net Session Border Controller

[7] *Net-Net® Session Director User Guide*, Release C[xz]6.3.9 Final, June 2012, Document ID 400-0170-00 Rev. 2.0.

RFC Documents

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

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

Appendix: Acme Packet 3800 Net-Net SBC Configuration File

```
host-routes
       dest-network                  10.1.2.0
       netmask                       255.255.255.0
       gateway                       10.32.128.254
       description
       last-modified-by              admin@192.168.168.37
       last-modified-date            2011-10-27 16:57:53
host-routes
       dest-network                  10.32.0.0
       netmask                       255.255.0.0
       gateway                       10.32.128.254
       description                   DevConnectLAN
       last-modified-by              admin@192.168.168.37
       last-modified-date            2010-08-05 15:25:58
host-routes
       dest-network                  192.168.0.0
       netmask                       255.255.0.0
       gateway                       10.32.128.254
       description                   Route to remote testers
       last-modified-by              admin@192.168.168.37
       last-modified-date            2012-09-10 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            2013-09-19 13:06:16
       policy-attribute
              next-hop                      192.168.24.12
              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              2013-09-19 13:02:16
        policy-attribute
               next-hop                         10.32.128.4
               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@192.168.168.37
       last-modified-date             2010-06-16 05:40:01
network-interface
       name                           s0p0
       sub-port-id                    0
       description
       hostname
       ip-address                     192.168.96.225
       pri-utility-addr
       sec-utility-addr
       netmask                        255.255.255.224
       gateway                        192.168.96.254
       sec-gateway
       gw-heartbeat
              state                          disabled
              heartbeat                      0
              retry-count                    0
              retry-timeout                  1
              health-score                   0
       dns-ip-primary                 192.168.16.67
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                    11
       hip-ip-list                    192.168.96.225
       ftp-address
       icmp-address                   192.168.96.225
       snmp-address
       telnet-address
       ssh-address
       last-modified-by               admin@192.168.168.37
       last-modified-date             2011-09-10 10:08:47
network-interface
       name                           s1p0
       sub-port-id                    0
       description
       hostname
       ip-address                     10.32.128.13
       pri-utility-addr
       sec-utility-addr
       netmask                        255.255.255.0
       gateway                        10.32.128.254
       sec-gateway
       gw-heartbeat
              state                          disabled
              heartbeat                      0
              retry-count                    0
              retry-timeout                  1
              health-score                   0
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                    11
       hip-ip-list                    10.32.128.13
       ftp-address                    10.32.128.13
       icmp-address                   10.32.128.13
       snmp-address
       telnet-address                 10.32.128.13
```

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

```
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        ext-policy-svr
        symmetric-latching             disabled
        pai-strip                      disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching            none
        restriction-mask               32
        accounting-enable              enabled
        user-cac-mode                  none
        user-cac-bandwidth             0
        user-cac-sessions              0
        icmp-detect-multiplier         0
        icmp-advertisement-interval    0
        icmp-target-ip
        monthly-minutes                0
        net-management-control         disabled
        delay-media-update             disabled
        refer-call-transfer            disabled
        dyn-refer-term                 disabled
        codec-policy
        codec-manip-in-realm           disabled
        constraint-name
        call-recording-server-id
        xnq-state                      xnq-unknown
        hairpin-id                     0
        stun-enable                    disabled
        stun-server-ip                 0.0.0.0
        stun-server-port               3478
        stun-changed-ip                0.0.0.0
        stun-changed-port              3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                     disabled
        hide-egress-media-update       disabled
        last-modified-by               admin@192.168.168.37
        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@192.168.168.37
        last-modified-date            2010-12-16 17:25:01
session-agent
```

```
hostname                        10.32.128.4
ip-address                      10.32.128.4
port                            5060
state                           enabled
app-protocol                    SIP
app-type
transport-method                StaticTCP
realm-id                        INTERNAL2
egress-realm-id
description                     Princeton_CM
carriers
allow-next-hop-lp               enabled
constraints                     disabled
max-sessions                    0
max-inbound-sessions            0
max-outbound-sessions           0
max-burst-rate                  0
max-inbound-burst-rate          0
max-outbound-burst-rate         0
max-sustain-rate                0
max-inbound-sustain-rate        0
max-outbound-sustain-rate       0
min-seizures                    5
min-asr                         0
time-to-resume                  0
ttr-no-response                 0
in-service-period               0
burst-rate-window               0
sustain-rate-window             0
req-uri-carrier-mode            None
proxy-mode
redirect-action
loose-routing                   enabled
send-media-session              enabled
response-map
ping-method
ping-interval                   0
ping-send-mode                  keep-alive
ping-all-addresses              disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                        disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                     disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate       0
early-media-allow
invalidate-registrations        disabled
rfc2833-mode                    none
rfc2833-payload                 0
```

```
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@192.168.168.37
        last-modified-date              2013-09-20 22:39:03
session-agent
        hostname                        192.168.24.12
        ip-address                      192.168.24.12
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        EXTERNAL
        egress-realm-id
        description                     Frontier
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=70
        ping-interval                   120
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
```

```
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid              outManToSP
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@192.168.168.51
        last-modified-date              2013-09-20 12:21:24
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   INTERNAL2
        egress-realm-id
        nat-mode                        Public
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        add-reason-header               disabled
        sip-message-len                 4096
        enum-sag-match                  disabled
        extra-method-stats              enabled
        registration-cache-limit        0
        register-use-to-for-lp          disabled
        options                         max-udp-length=0
        refer-src-routing               disabled
```

```
      add-ucid-header                 disabled
      proxy-sub-events
      pass-gruu-contact               disabled
      sag-lookup-on-redirect          disabled
      last-modified-by                admin@192.168.168.37
      last-modified-date              2010-11-02 16:18:33
sip-interface
      state                           enabled
      realm-id                        EXTERNAL
      description
      sip-port
            address                         192.168.96.225
            port                            5060
            transport-protocol              UDP
            tls-profile
            allow-anonymous                 agents-only
            ims-aka-profile
      carriers
      trans-expire                    0
      invite-expire                   0
      max-redirect-contacts           0
      proxy-mode
      redirect-action                 Proxy
      contact-mode                    none
      nat-traversal                   none
      nat-interval                    30
      tcp-nat-interval                90
      registration-caching            disabled
      min-reg-expire                  300
      registration-interval           3600
      route-to-registrar              disabled
      secured-network                 disabled
      teluri-scheme                   disabled
      uri-fqdn-domain
      trust-mode                      all
      max-nat-interval                3600
      nat-int-increment               10
      nat-test-increment              30
      sip-dynamic-hnt                 disabled
      stop-recurse                    401,403,407
      port-map-start                  0
      port-map-end                    0
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      sip-ims-feature                 disabled
      operator-identifier
      anonymous-priority              none
      max-incoming-conns              0
      per-src-ip-max-incoming-conns   0
      inactive-conn-timeout           0
      untrusted-conn-timeout          0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode            pass
      charging-function-address-mode  pass
      ccf-address
      ecf-address
      term-tgrp-mode                  none
      implicit-service-route          disabled
```

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

```
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@192.168.168.37
        last-modified-date             2011-08-03 16:00:53
sip-manipulation
        name                           outManToSP
        description                    Outbound SIP HMRs To SP
        split-headers
        join-headers
        header-rule
                name                           manipTo
                header-name                    To
                action                         manipulate
                comparison-type                pattern-rule
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           chgToHost
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
                        comparison-type                case-sensitive
                        match-value
                        new-value                      $REMOTE_IP
        header-rule
                name                           manipFrom
                header-name                    From
                action                         manipulate
                comparison-type                case-sensitive
                msg-type                       request
                methods
                match-value
                new-value
                element-rule
                        name                           From
                        parameter-name
                        type                           uri-host
                        action                         replace
                        match-val-type                 any
```

```
              comparison-type                case-sensitive
              match-value
              new-value                      $LOCAL_IP
header-rule
       name                           manipDiversion
       header-name                    Diversion
       action                         manipulate
       comparison-type                case-sensitive
       msg-type                       request
       methods
       match-value
       new-value
       element-rule
              name                           Diversion
              parameter-name
              type                           uri-host
              action                         replace
              match-val-type                 any
              comparison-type                case-sensitive
              match-value
              new-value                      $LOCAL_IP
header-rule
       name                           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                           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                           delAlert
       header-name                    Alert-Info
       action                         delete
       comparison-type                case-sensitive
```

```
            msg-type                        any
            methods
            match-value
            new-value
      last-modified-by              admin@192.168.168.37
      last-modified-date            2013-09-22 18:09:26
steering-pool
      ip-address                    192.168.96.225
      start-port                    49152
      end-port                      65535
      realm-id                      EXTERNAL
      network-interface
      last-modified-by              admin@192.168.168.37
      last-modified-date            2011-09-10 10:11:31
steering-pool
      ip-address                    10.32.128.13
      start-port                    2048
      end-port                      65535
      realm-id                      INTERNAL2
      network-interface
      last-modified-by              admin@192.168.168.37
      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.