Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager 6.2 and Acme Packet 3820 Net-Net Session Border Controller with Wind Telecom SIP Trunk Service- Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Wind Telecom SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.2, Acme Packet 3820 Net-Net Session Border Controller and various Avaya endpoints.

Wind Telecom 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 procedures for configuring Session Initiation Protocol (SIP) Trunking between the service provider Wind Telecom and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 6.2, Acme Packet 3820 Net-Net Session Border Controller and various Avaya endpoints. The solution does not include Avaya Aura® Session Manager and consequently SIP endpoints are not supported.

The Wind Telecom SIP Trunk Service referenced within these Application Notes is designed for business customers in the Dominican Republic. Customers using this service with the Avaya SIP-enabled enterprise solution 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 analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The enterprise site was configured to connect to the Wind Telecom SIP Trunk service by means of a broadband connection to the public Internet.

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:

- Incoming PSTN calls to various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator softphones using H.323 protocol. Avaya one-X® Communicator supports placing and receiving calls using the local computer or by controlling an external telephone. Usage modes "This Computer" and "Other Phone" were tested.
- Various call types, including: local, long distance, international and outbound toll-free.

- Codecs G729A and G.711MU and proper codec negotiation.
- DTMF tone transmissions passed as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Routing inbound PSTN calls to call center agent queues.

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested as part of the compliance test
- Operator services such as dialing 0 or 0 + 10 digits are not supported.
- Since the solution does not include Avaya Aura® Session Manager, SIP endpoints are not supported.

2.2. Test Results

Interoperability testing with Wind Telecom was completed with successful results with the exception of the observations/limitations described below:

- **OPTIONS** – Wind Telecom was not configured to send OPTIONS messages to the enterprise during the compliance test, but responded correctly with "200 OK" messages to the OPTIONS sent by the 3820 Net-Net SBC at the enterprise to monitor the status of the SIP trunk.
- **Shuffling** – Direct IP-IP Audio Connections (shuffling) needed to be disabled on the SIP trunk, on the signaling group form in Communication Manager, in order to avoid problems of intermittent one way audio path observed during the tests for both incoming and outbound calls.
- **T.38 Fax** – T.38 Fax did not pass compliance testing. The use of T.38 Fax is not recommended with this solution.
- **Network Call Redirection** – On external calls that are transferred back to the PSTN, Wind Telecom responds with a "202 Accepted" to the REFER or the 302 Moved Temporarily messages sent from Communication Manager, but the call between the two PSTN endpoints drops. Network Call Redirection needs to be disabled on the Trunk Group in Communication Manager for the call transfer to complete, otherwise the transfer fails. The implication is that Communication Manager is not released after the call is transferred to the PSTN, and 2 trunks remain busy for the duration of the call.

2.3. Support

For technical support on the Wind Telecom SIP Trunk Service offer, visit www.windtelecom.com.do

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution, connected to the Wind Telecom SIP Trunking Service through a public Internet WAN connection.

For security purposes, private addresses are shown in these Application Notes for the enterprise and the Service Provider public network interfaces, instead of the real public IP addresses used during the tests. Also, PSTN routable phone numbers used in the compliance test have been changed to non-routable ones.

The components used to create the simulated customer site included:

- Avaya Common Server HP Proliant DL360, running Communication Manager and Communication Manager Messaging
- Acme Packet 3820 Net-Net Session Border Controller (SBC).
- Avaya G450 Media Gateway
- Avaya 96x0 and 96x1 Series IP Telephones (H.323)
- Avaya one-X® Communicator soft phones (H.323)
- Avaya digital and analog telephones

The 3820 Net-Net SBC represents the single point of connection between the public network and the Local Area Network in the enterprise. In addition to providing comprehensive security for all SIP and RTP traffic entering the private network, the SBC serves as an interoperability tool between the enterprise and the service provider, by allowing the control and manipulation of the SIP headers in the traffic flowing through its interfaces.

The transport protocol between the 3820 Net-Net SBC at the enterprise and Wind Telecom across the public IP network is UDP. The transport protocol between the 3820 Net-Net SBC and Communication Manager across the enterprise local area network is TCP.

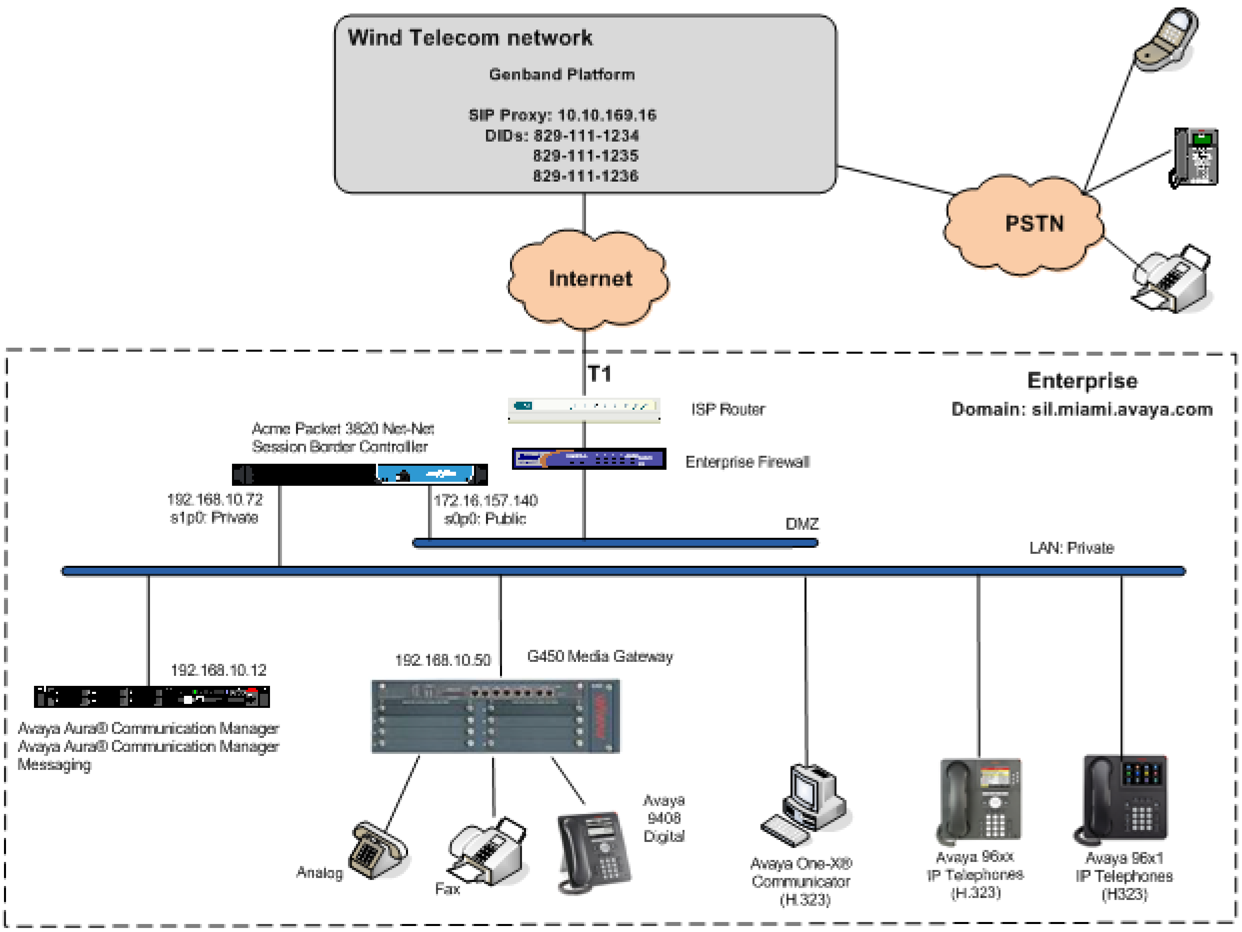

Figure 1: Test Configuration

For inbound calls, the calls flow from the service provider to the external firewall, to the 3820 Net-Net SBC. After performing the necessary security checks and header manipulation, the SBC sends the call to Communication Manager, where 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 for outbound feature treatment such as automatic route selection and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to the 3820 Net-Net SBC for additional interworking treatment before egress to the Wind Telecom network.

Since the Dominican Republic is a country member of the North American Numbering Plan (NANP), the users dialed 10 digits for local calls, including the area code, and 11 (1 + 10) digits for calls to other area codes in the NANP.

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® Communication Manager on a HP® Proliant DL360 G7 Server.	6.2 Service Pack 2 (R016x.02.0.823.0)
Avaya Aura® Communication Manager Messaging	CMM-02.0.823.0-0002
Avaya G450 Media Gateway	31.26.0
Avaya 96x0 Series IP Telephones (H.323)	Avaya one-X® Deskphone Edition 3.1 SP4
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X® Deskphone Edition 6.2
Avaya one-X® Communicator (H.323)	6.1.7.04-SP7-39506
Avaya 9408 Digital Telephone	2.00
Avaya 6210 Analog Telephone	n/a
Acme Packet 3820 Net-Net Session Border Controller	SCX6.4.0 Patch 1 (Build 115)
Wind Telecom SIP Trunk Service	
Genband Softswitch	C20 CVM 14

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager to connect to the Wind Telecom SIP Trunk Service. A SIP trunk is established between Communication Manager and the 3820 Net-Net SBC for use by signaling traffic to and from Wind Telecom. It is assumed the general installation of Communication Manager, Messaging, Avaya G450 Media Gateway and endpoints has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to and from the service provider. The example shows that **24000** licenses are available and **287** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 12000 10
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 2
                   Maximum Video Capable IP Softphones: 18000 4
                       Maximum Administered SIP Trunks: 24000 287
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 100   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*** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to ***none***.

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

                 Music (or Silence) on Transferred Trunk Calls? no
                          DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                     Automatic Circuit Assurance (ACA) Enabled? n



                Abbreviated Dial Programming by Assigned Lists? n
        Auto Abbreviated/Delayed Transition Interval (rings): 2
                         Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

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 ***restricted*** for restricted calls and ***unavailable*** for unavailable calls.

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

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: restricted
  CPN/ANI/ICLID Replacement for Unavailable Calls: unavailable

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: _____
```

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been defined for the IP addresses of the Communication Manager SIP signaling interface *(***procr**) and the inside interface of the 3820 Net-Net SBC (**Acme_s1p0**). These node names will be needed when configuring the service provider signaling group in **Section 5.6**.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
ASBCE_A1               192.168.10.72
Acme_s1p0              192.168.10.52
HG_CM                  172.16.5.12
HG_SM                  172.16.5.32
asm                    192.168.10.32
default                0.0.0.0
msgserver              192.168.10.12
procr                  192.168.10.12
procr6                 ::
```

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 **4** was used for this purpose. The Wind telecom SIP Trunk Service supports codecs G.729A and G.711MU, in this order of preference. Enter ***G.729A*** and ***G.711MU*** in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

                          IP Codec Set

    Codec Set: 4

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

Since T.38 fax did not pass the compliance test, it is recommended to disable T.38 fax by setting the **Fax Mode** field to ***off*** on **Page 2**.

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

                          IP Codec Set

                              Allow Direct-IP Multimedia? n

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

5.5. IP Network Region

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

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the test configuration, the domain name is ***sil.miami.avaya.com***. This domain name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to ***yes*,** the default setting. This will 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. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
change ip-network-region 4                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 4
Location: 1          Authoritative Domain: sil.miami.avaya.com
    Name: CM-ASBCE
MEDIA PARAMETERS                          Intra-region IP-IP Direct Audio: yes
      Codec Set: 4                        Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                                IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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

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

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the 3820 Net-Net 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 **4** was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **IMS Enabled** field to ***n***. This specifies that Communication Manager will serve as an Evolution Server.
- Set the **Transport Method** to the value of ***tcp***, to be used between Communication Manager and the private interface of the 3820 Net-Net SBC. In order to facilitate tracing and fault analysis, the compliance test was conducted with the **Transport Method** set to ***tcp.*** For security purposes, it is recommended in an actual customer environment to use the default Transport Method value of ***tls***.
- Set the **Peer Detection Enabled** field to ***y***. The **Peer-Server** field defaults to **Others** and cannot be changed via administration.
- Set the **Near-end Node Name** to ***procr***. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to ***Acme_s1p0***. This node name maps to the IP address of the inside interface of the 3820 Net-Net SBC, as defined in **Section 5.3**.

- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port. The default well-known port value for SIP over TCP is 5060 (port 5061 if TLS is used). The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5060***.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Leave the **Far-end Domain** field blank.
- Set **Direct IP-IP Audio Connections** to ***n***. This setting will effectively disable media shuffling on the SIP trunk. This was needed as a workaround to the one way audio path problem described in **Section 2.2**.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Enable Layer 3 Test** to ***y***. This will enable Communication Manager to send periodic SIP OPTIONS to the 3820 Net-Net SBC to monitor the status of the SIP trunk.
- Default values may be used for all other fields.

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

 Group Number: 4             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



   Near-end Node Name: procr                   Far-end Node Name: Acme_s1p0
 Near-end Listen Port: 5060                  Far-end Listen Port: 5060
                                          Far-end Network Region: 4
                                     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? n
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
        Enable Layer 3 Test? y
                                                    Alternate Route Timer(sec): 6
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group **4** was configured using the parameters highlighted below.

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

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

Group Number: 4                  Group Type: sip          CDR Reports: y
  Group Name: Wind Telecom                     COR: 1      TN: 1      TAC: 604
   Direction: two-way      Outgoing Display? n
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                      Signaling Group: 4
                                                    Number of Members: 6
```

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

```
change trunk-group 3                                            Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

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

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

On **Page 3**, set the **Numbering Format** field to ***public.*** 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.

```
change trunk-group 3                                            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
```

On **Page 4**, set the values as highlighted below:

- Set the **Network Call Redirection** field to ***n***. By setting this, Communication Manager will not send REFER headers for calls that are transferred back to the PSTN. See **Section 2.2** for more information.
- Set the **Send Diversion Header** field to ***y***. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.
- Set **Support Request History** fields to ***n***.
- Set the **Telephone Event Payload Type** to ***101***.
- Set **Convert 180 to 183 for Early Media** to ***y***.
- Default values were used for all other fields.

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

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


                        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
                                             Enable Q-SIP? n
```

5.8. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (**Section 5.7**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. DID numbers are provided by the SIP service provider. Each DID number is assigned in this table to one enterprise internal extension or Vector Directory Numbers (VDNs), and they are used to authenticate the caller. In the sample configuration, 3 DID numbers were assigned for testing. These 3 numbers were mapped to 3 extensions, 3001 to 3003. These 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 1                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext             Trk       CPN             CPN
Len Code            Grp(s)    Prefix          Len
                                                     Total Administered: 15
 4  2                                          4        Maximum Entries: 9999
 4  3                                          4
 4  3001            4         8291111234       10    Note: If an entry applies to
 4  3002            4         8291111235       10    a SIP connection to Avaya
 4  3003            4         8291111236       10    Aura(R) Session Manager,
                                                     the resulting number must
                                                     be a complete E.164 number.
```

5.9. Inbound Routing

DID numbers received from Wind Telecom can be mapped to internal extensions or Vector Directory Numbers (VDNs) on the enterprise, using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt** command to create an entry for each DID.

```
change inc-call-handling-trmt trunk-group 4                     Page   1 of  30
                      INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk   10 8291111234        10  3001
 public-ntwrk   10 8291111235        10  3002
 public-ntwrk   10 8291111236        10  3003
 public-ntwrk
 public-ntwrk
```

5.10. **Outbound Routing**

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

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

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

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

```
change feature-access-codes                                    Page   1 of  11
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: #1
                       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:      All:          Deactivation:
   Call Forwarding Enhanced Status:      Act:          Deactivation:
```

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 **4** which contains the SIP trunk group 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
    011                      10   18    4         intl           n
    1305                     11   11    4         fnpa           n
    1786                     11   11    4         fnpa           n
    1954                     11   11    4         fnpa           n
    829                      10   10    4         hnpa           n
                                                                 n
```

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern **4** 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 **4** was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: **1** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance numbers in the North American Numbering Plan (NANP).
- **LAR**: ***next***

```
change route-pattern 4                                          Page   1 of   3
                    Pattern Number: 4    Pattern Name: CM-Acme
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 4    0       1                                                       n   user
 2:                                                                      n   user
 3:                                                                      n   user
 4:                                                                      n   user
 5:                                                                      n   user
 6:                                                                      n   user

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

6. Configure Acme Packet 3820 Net-Net Session Border Controller

In the sample configuration, the Acme Packet 3820 Net-Net SBC is used as the edge device between the Avaya CPE and the public IP network. The following sections describe the configuration tasks required on the 3820 Net-Net SBC to connect to the Wind Telecom SIP Trunk service.

The following sections will not attempt to describe each component configuration in its entirety, but will show the most important settings required to support the reference configuration. The remaining parameters not mentioned here are generally the default values used by the SBC for that parameter. Consult the Acme Packet documentation for additional details on the administration of the 3820 Net-Net SBC.

The resulting 3820 Net-Net SBC complete configuration file is shown in **Appendix A**.
Over the next following sections, screenshots with relevant segments of the configuration file will be shown to illustrate some of the settings implemented.

The 3820 Net-Net SBC was configured using the Acme Packet CLI via a Putty SSH connection to the previously configured management port of the SBC. A serial connection to the console port is also supported. The following are the generic steps for configuring the 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 a **#**).
3. In superuser mode, type **configure terminal** to enter configure mode. The prompt will change to **(configure)#**.
4. Type the name of the element that will be configured (e.g., **system**).
5. Type the name of the sub-element, if any (e.g., **phy-interface**).
6. Type the name of the parameter followed by its value (e.g., **name s0p0**).
7. When all required parameters of the sub-element have been entered, type **done**.
8. Type **exit** as many times as needed to return to the **configure** prompt.
9. Repeat steps 4-8 to configure all the elements. When finished, exit the configuration mode by typing **exit** until returned to the superuser prompt.
10. Type **save-configuration** to save the configuration.
11. Type **activate-configuration** to activate the configuration.

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

6.1. Physical Interfaces

There are 4 physical interfaces in the back of the 3820 Net-Net SBC for the use of signaling and media traffic. They are labeled using slot (0/1) and port (0/1) numbers in the chassis. For the reference configuration, interface **s0p0** was used to connect the SBC to the public network, while **s1p0** was used to connect to the private enterprise network.

Enter **system → phy-interface** at the configure level to create the physical interfaces to the public and the private sides of the SBC. Set the parameters as highlighted on the screen below.

- Enter a descriptive **name** for the interface.
- Set **operation-type** to **Media**.
- Enter the **port** and **slot** of the interface.
- Set the **duplex-mode** to **FULL**.
- Set the **speed** to **100**.

```
phy-interface
        name                            s0p0
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@192.168.10.150
        last-modified-date              2013-01-23 12:40:35
phy-interface
        name                            s1p0
        operation-type                  Media
        port                            0
        slot                            1
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@192.168.10.150
        last-modified-date              2013-02-12 15:33:56
```

6.2. Network Interfaces

Network interfaces are logical elements containing configuration parameters that are associated to the physical interfaces created previously. Enter **system → network-interface** at the configure level to create the physical interfaces for the public and the private sides of the SBC. Set the following parameters.

- Enter the **name** of the interface. This must be the same name as the physical interface to which it corresponds, created in **Section 6.1**.
- Enter an appropriate **description**.
- Enter the **ip-address**, **netmask** and **gateway** assigned to the interface.
- Since in the reference configuration only one IP address is assigned to each interface, set **hip-ip-list** and **icmp-address** to the same **ip-address** value entered above.

The screen below shows the Network Interface created for the public network.

```
network-interface
        name                            s0p0
        sub-port-id                     0
        description                     Service-Provider
        hostname
        ip-address                      172.16.157.140
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.192
        gateway                         172.16.157.129
        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                     172.16.157.140
        ftp-address
        icmp-address                    172.16.157.140
        snmp-address
        telnet-address
        ssh-address
        signaling-mtu                   0
        last-modified-by                admin@192.168.10.150
        last-modified-date              2013-01-23 13:00:08
```

The screen below shows the Network Interface created for the private enterprise network.

```
network-interface
        name                            s1p0
        sub-port-id                     0
        description                     Private-Network
        hostname
        ip-address                      192.168.10.52
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.0
        gateway                         192.168.10.254
        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                     192.168.10.52
        ftp-address
        icmp-address                    192.168.10.52
        snmp-address
        telnet-address
        ssh-address
        signaling-mtu                   0
        last-modified-by                admin@192.168.10.150
        last-modified-date              2013-01-23 13:06:02
```

6.3. Realms

Realms are logical definitions of networks used as a basis for determining egress and ingress associations between physical and network interfaces, as well as the application of SIP header manipulation rules and other policies. Enter **media-manager → realm-config** at the configure level to create the realms for the public and the private sides of the SBC. Set the following parameters.

- Set an **identifier.** This is later used in the configuration to associate the realm to other parameters.
- Enter an appropriate **description**.
- Enter the **network-interface** associated with this realm**.**
- For the public side realm only, for the **out-manipulationid** parameter enter **Outbound_HMRs.** This is the name of the sip manipulation, defined in **Section 6.10** later in this document, which will be applied to all outbound traffic to the service provider.

Realm for the outside public network.

```
realm-config
        identifier                          Carrier
        description                         ServiceProvider
        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
        qos-enable                          disabled
        generate-UDP-checksum               disabled
        max-bandwidth                       0
        fallback-bandwidth                  0
        max-priority-bandwidth              0
        max-latency                         0
        max-jitter                          0
        max-packet-loss                     0
        observ-window-size                  0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough                disabled
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid                  Outbound_HMRs
        manipulation-string
        manipulation-pattern
```

Realm for the private network:

```
realm-config
        identifier                          Enterprise
        description                         Private-Network
        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
        qos-enable                          disabled
        generate-UDP-checksum               disabled
```

On the screens above, note the **sub-port-id 0** after the colon in the **network-interfaces**. Since VLANs were not used, the default value **0** was automatically added to the configuration, and it was not required to be explicitly configured by the user.

6.4. Steering-Pools

Steering pools define sets of ports that are used for steering the media flows through the 3820 Net-Net SBC interfaces. Enter **media-manager → steering-pool** at the configure level to create the Steering-Pools for the public and the private sides of the SBC. Set the following parameters.

- Enter the **ip-address** of the network interface on the 3820 Net-Net SBC.
- Enter the **start-port** and **end-port** which define the range used for the media. For the compliance test, the range for the public network was specified by Wind Telecom (40000-60000). The Private side was made to match the port range specified in the IP-Network-Region in Communication Manager, of 2048-3329.
- Enter the **realm-id** of the associated realm defined in **Section 6.3**.

```
steering-pool
        ip-address                     192.168.10.52
        start-port                     2048
        end-port                       3329
        realm-id                       Enterprise
        network-interface
        last-modified-by               admin@192.168.10.150
        last-modified-date             2013-01-23 14:22:21
steering-pool
        ip-address                     172.16.157.140
        start-port                     40000
        end-port                       60000
        realm-id                       Carrier
        network-interface
        last-modified-by               admin@192.168.10.150
        last-modified-date             2013-01-23 14:20:25
```

6.5. Media-Manager

Verify that the media-manager process is enabled.

- Enter **media-manager → media-manager** at the configure level
- **Enter select → show**. Verify that the media-manager state is enabled, as shown on the screen below. If disabled, enable it by entering the **state enabled** command.

```
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
```

6.6. SIP Configuration

The **sip-config** element defines global system-wide SIP parameters in the 3820 Net-Net SBC. Enter **session-router → sip-config** at the configure level and set the following.

- Set **state** to **enabled**.
- Set **operation-mode** to **dialog**.
- Set **home-realm-id** to **Enterprise,** the realm corresponding to the private network.
- Set **nat-mode** to **None**.

```
sip-config
        state                               enabled
        operation-mode                      dialog
        dialog-transparency                 enabled
        home-realm-id                       Enterprise
        egress-realm-id
        nat-mode                            None
        registrar-domain
        registrar-host
```

6.7. SIP Interfaces

SIP interfaces are created to specify the IP addresses and ports in which the 3820 Net-Net SBC will listen for signaling traffic in both the inside and outside networks. Enter **session-router → sip-interface** at the configure level to configure the SIP interfaces for the private and public networks. Set the following parameters.

- Set **state** to **enabled**.
- Enter the **realm-id** of the associated realm for that interface.
- Under the **sip-port** sub-element, enter the **address**, **port** and **transport-protocol** for the interface. Note that the transport protocol for the outside interface to Wind Telecom is **UDP,** while on the inside interface to Communication Manager the transport protocol is **TCP**.
- For the **allow-anonymous** parameter, the value of **agents-only** is used on the public side. By setting this, SIP requests will only be accepted from session agents (as defined later in **Section 6.8**) on this interface. On the private side, the value of **all** is used. Thus, SIP requests will be accepted from any entity on this interface.
- Set **stop-recourse** to **401,407** (not shown).

The screen below shows the SIP interface on the public side of the 3830 Net-Net SBC.

```
sip-interface
        state                               enabled
        realm-id                            Carrier
        description
        sip-port
                address                             172.16.157.140
                port                                5060
                transport-protocol                  UDP
                tls-profile
                multi-home-addrs
                allow-anonymous                     agents-only
                ims-aka-profile
```

The SIP interface on the private network is shown below.

```
sip-interface
        state                                  enabled
        realm-id                               Enterprise
        description
        sip-port
                address                                192.168.10.52
                port                                   5060
                transport-protocol                     TCP
                tls-profile
                multi-home-addrs
                allow-anonymous                        all
                ims-aka-profile
```

6.8. Session-Agents

A session-agent defines an internal "next hop" signaling entity or peer for the SIP traffic. A realm is associated with a session-agent, to identify sessions coming from or going to that session-agent. SIP header manipulations can also be applied at the SIP agent level.

Enter **session-router → session-agent** at the configure level to define the session-agents for the service provider (on the outside network) and Communication Manager (on the inside network). Set the parameters as follows.

- Under **hostname** and **ip-address**, enter the IP address of the Wind Telecom's SIP proxy server or Communication manager signaling interface (**procr**), in each case.
- Set **port** to **5060**.
- Set **state** to **enabled**.
- Set the **app-protocol** to **SIP**.
- Set the **transport-method** for the service provider session agent to **UDP**, and **StaticTCP** for the inside session agent.
- Enter the **realm-id** of the associated realm for that session agent.
- Enter an appropriate **description**.
- Set **ping-method** to **OPTIONS;hops=0**. This setting specifies that SIP OPTIONS messages will be sent to verify the health of the connection to this session agent.
- Set the **ping-interval** to **180**. This value specifies the interval, in seconds, between OPTIONS messages sent to this session agent.
- Set **ping-send-mode** to **keep-alive**.

The screen below shows the session agent representing the Wind Telecom SIP Trunk service proxy server.

```
session-agent
        hostname                               10.10.169.16
        ip-address                             10.10.169.16
        port                                   5060
        state                                  enabled
        app-protocol                           SIP
        app-type
        transport-method                       UDP
        realm-id                               Carrier
        egress-realm-id
        description                            Service-Provider
        carriers
        allow-next-hop-lp                      enabled
        constraints                            disabled
        max-sessions                           0
        max-inbound-sessions                   0
        max-outbound-sessions                  0
        max-burst-rate                         0
        max-inbound-burst-rate                 0
        max-outbound-burst-rate                0
        max-sustain-rate                       0
        max-inbound-sustain-rate               0
        max-outbound-sustain-rate              0
        min-seizures                           5
        min-asr                                0
        time-to-resume                         0
        ttr-no-response                        0
        in-service-period                      0
        burst-rate-window                      0
        sustain-rate-window                    0
        req-uri-carrier-mode                   None
        proxy-mode
        redirect-action
        loose-routing                          enabled
        send-media-session                     enabled
        response-map
        ping-method                            OPTIONS;hops=0
        ping-interval                          180
        ping-send-mode                         keep-alive
        ping-all-addresses                     disabled
        ping-in-service-response-codes
```

The screen below shows the session agent for Communication Manager.

```
session-agent
        hostname                        192.168.10.12
        ip-address                      192.168.10.12
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                StaticTCP
        realm-id                        Enterprise
        egress-realm-id
        description                     Communication-Manager
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   180
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
```

6.9. Local Policies

Local policies control the forwarding of SIP requests from the **Enterprise** realm to the service provider session agent in the **Carrier** realm, and vice-versa. Enter **session-router → local-policy** at the configure level and set the following.

- Set the **from-address** and **to-address** to *, indicating that the policy allows any origin and destination IP address.
- Enter the **source-realm** where the SIP requests are originated, in each case.
- Enter an appropriate **description**.
- Set **state** to **enabled**.
- Under the **policy-attibute** sub-element, set **next-hop** to the IP address of the session agent and the associated **realm** where all SIP requests should be forwarded on this policy. Set **terminate-recursion** to **enabled**, **app-protocol** to **SIP** and **state** to **enabled**.

The screen below shows the local policy for SIP requests originating from the **Enterprise** realm, being forwarded to the session agent corresponding to the Wind Telecom SIP proxy server, on the **Carrier** realm.

```
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       Enterprise
        description                    CM-to-Service-Provider
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@192.168.10.150
        last-modified-date             2013-01-23 15:48:29
        policy-attribute
                next-hop                       10.10.169.16
                realm                          Carrier
                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
```

The screen below shows the local policy for SIP requests originating from the **Carrier** realm, being forwarded to the session agent corresponding to Communication Manager, on the **Enterprise** realm.

```
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        Carrier
        description                     Service-Provider-to-CM
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@192.168.10.150
        last-modified-date              2013-01-25 12:57:08
        policy-attribute
                next-hop                        192.168.10.12
                realm                           Enterprise
                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
```

6.10. SIP Manipulation

SIP manipulations specify rules for the modification of the contents of SIP headers. They can be assigned at different levels in the configuration. During the compliance test, a SIP manipulation named **Outbound_HMRs** was created. This was applied to the realm for the outside public network, as previously seen in **Section 6.3**.

To create the SIP manipulation, enter **session-router → sip-manipulation** at the configure level. Enter an appropriate **name** and **description**.

```
sip-manipulation
        name                            Outbound_HMRs
        description                     Change_host_Remove_Alert_Info
        split-headers
        join-headers
```

Two types of header manipulation rules (HMR) were defined as part of this SIP Manipulation:

- SIP URI host manipulation. These HMRs will prevent local domains and IP addresses present in the host part of the SIP URIs originating in the Enterprise from being propagated to the outside network. Source headers like From, PAI and Diversion headers will have their host part being populated with the outside IP address of the 3820 Net-Net SBC (**$LOCAL_IP**). Destination headers like To and Refer-To will have their URI host set to the IP address of the session agent representing the service provider SIP proxy **($REMOTE_IP**).
- Header removal. The Alert-Info header sent in SIP messages from Communication Manager contains private IP addresses or SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries. Since this header was not used by Wind Telecom, it was removed (deleted).

Enter **header-rule** at the **(sip-manipulation)#** prompt to create the header rule to replace the host of the SIP URI in the From header, containing the enterprise domain, with the IP address of the outside interface of the 3820 Net-Net SBC. Set the parameters as highlighted on the screen below.

```
header-rule
    name                                From
    header-name                         From
    action                              manipulate
    comparison-type                     case-insensitive
    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-insensitive
        match-value
        new-value                           $LOCAL_IP
```

Similar headers rules were created to replace the host in the To, PAI, Diversion and Refer-to headers with the local or remote IP address for each case. See the configuration file in **Appendix A** for complete details.

The screen below shows the **Alert_Info** header rule created. Note that in this case the **action** is set to **delete** the header.

```
header-rule
    name                                Alert_Info
    header-name                         Alert-Info
    action                              delete
    comparison-type                     case-insensitive
    msg-type                            any
    methods
    match-value
    new-value
```

7. Wind Telecom SIP Trunk Service Configuration

To use the Wind Telecom SIP Trunk Service, a customer must request the service from Wind Telecom using the established sales and provisioning processes. The customer will need to provide Wind Telecom with the public IP address used to reach the 3820 Net-Net SBC at the enterprise. Wind Telecom will provide the customer with the necessary information to configure the SIP connection from the enterprise site to the Wind Telecom network, including:

- IP address of the Wind Telecom SIP proxy.
- Supported codecs.
- DID numbers.
- Transport protocol.
- Port numbers used for signaling and media.

This information is used to complete the configuration of Communication Manager and the 3820 Net-Net SBC discussed in the previous sections.

8. Verification and Troubleshooting

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

Verification Steps:

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

Troubleshooting:

1. Communication Manager:
    - **list trace station** <extension number>
      Traces calls to and from a specific station.
    - **list trace tac** <trunk access code number>
      Trace calls over a specific trunk group.
    - **status signaling-group** <signaling group number>
      Displays signaling group service state.
    - **status trunk** <trunk group number>
      Displays trunk group service state.
    - **status station** <extension number>
      Displays signaling and media information for an active call on a specific station.

2. Acme Packet 3820 Net-Net SBC:
    - **show sipd agents**
      Display the service state of SIP session agents, as well as additional information, like inbound, outbound and latency statistics.

There are multiple logs and tools that can be used on the 3820 Net-Net SBC to assist in troubleshooting and to evaluate the performance of the SBC in general. Consult the Acme Packet documentation for more information.

9. Conclusion

The Wind Telecom SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. It provides businesses with a flexible, cost-saving alternative to traditional hardwired telephony trunks.

These Application Notes describe the configuration necessary to connect the service above to Avaya Aura® Communication Manager R6.2 and the Acme Packet 3820 Net-Net Session Border Controller.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the exception of the observations/limitations described in **Section 2.2.**

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 6.2, December 2012, Document Number 03-300509.
[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.2, December 2012, Document Number 555-245-205.
[3] *Acme Packet Net-Net 4000 ACLI Configuration Guide*, Release S-Cx6.4.0, January 2013, Document Number 400-0061-64.
[4] *Acme Packet Net-Net 4000 Maintenance and Troubleshooting Guide*. Release S-Cx6.4.0, December 2012, Document Number 400-0063-64.
[5] *Administering Avaya one-X® Communicator*, October 2011.
[6] *Using Avaya one-X® Communicator, Release 6.1*, October 2011.
[7] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/.

Appendix A
Acme Packet 3820 Net-Net SBC Configuration File

```
ACME3800# show run
local-policy
      from-address
                                     *
      to-address
                                     *
      source-realm
                                     Enterprise
      description                    CM-to-Service-Provider
      activate-time                  N/A
      deactivate-time                N/A
      state                          enabled
      policy-priority                none
      last-modified-by               admin@192.168.10.150
      last-modified-date             2013-01-23 15:48:29
      policy-attribute
            next-hop                       10.10.169.16
            realm                          Carrier
            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
                                     Carrier
      description                    Service-Provider-to-CM
      activate-time                  N/A
      deactivate-time                N/A
      state                          enabled
      policy-priority                none
      last-modified-by               admin@192.168.10.150
      last-modified-date             2013-01-25 12:57:08
      policy-attribute
            next-hop                       192.168.10.12
            realm                          Enterprise
            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        775880
      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
      syslog-on-demote-to-deny       disabled
      trap-on-demote-to-untrusted    disabled
      syslog-on-demote-to-untrusted  disabled
      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@192.168.10.150
      last-modified-date             2011-06-01 16:08:35
network-interface
      name                           s0p0
      sub-port-id                    0
      description                    Service-Provider
      hostname
      ip-address                     172.16.157.140
      pri-utility-addr
      sec-utility-addr
      netmask                        255.255.255.192
      gateway                        172.16.157.129
      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                   172.16.157.140
      ftp-address
        icmp-address                  172.16.157.140
      snmp-address
      telnet-address
      ssh-address
      signaling-mtu                 0
      last-modified-by              admin@192.168.10.150
      last-modified-date            2013-01-23 13:00:08
network-interface
      name                          s1p0
      sub-port-id                   0
      description                   Private-Network
      hostname
      ip-address                    192.168.10.52
      pri-utility-addr
      sec-utility-addr
      netmask                       255.255.255.0
      gateway                       192.168.10.254
      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                   192.168.10.52
      ftp-address
        icmp-address                  192.168.10.52
      snmp-address
      telnet-address
      ssh-address
      signaling-mtu                 0
      last-modified-by              admin@192.168.10.150
      last-modified-date            2013-01-23 13:06:02
phy-interface
      name                          s0p0
      operation-type                Media
      port                          0
      slot                          0
      virtual-mac
      admin-state                   enabled
      auto-negotiation              enabled
      duplex-mode                   FULL
      speed                         100
      overload-protection           disabled
      last-modified-by              admin@192.168.10.150
      last-modified-date            2013-01-23 12:40:35
phy-interface
      name                          s1p0
      operation-type                Media
      port                          0
```

```
        slot                            1
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        overload-protection             disabled
        last-modified-by                admin@192.168.10.150
        last-modified-date              2013-02-12 15:33:56
realm-config
        identifier                      Carrier
        description                     ServiceProvider
        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
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough            disabled
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid              Outbound_HMRs
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit              0
        access-control-trust-level      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        cac-failure-threshold           0
        untrust-cac-failure-threshold   0
        ext-policy-svr
        diam-e2-address-realm
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
```

```
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        refer-notify-provisional        none
        dyn-refer-term                  disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        xnq-state                       xnq-unknown
        hairpin-id                      0
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        tcp-media-profile
        subscription-id-type            END_USER_NONE
        last-modified-by                admin@192.168.10.150
        last-modified-date              2013-01-25 12:19:28
realm-config
        identifier                      Enterprise
        description                     Private-Network
        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
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
        media-sec-policy
        srtp-msm-passthrough            disabled
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
```

```
      manipulation-pattern
      class-profile
      average-rate-limit              0
      access-control-trust-level      none
      invalid-signal-threshold        0
      maximum-signal-threshold        0
      untrusted-signal-threshold      0
      nat-trust-threshold             0
      deny-period                     30
      cac-failure-threshold           0
      untrust-cac-failure-threshold   0
      ext-policy-svr
      diam-e2-address-realm
      symmetric-latching              disabled
      pai-strip                       disabled
      trunk-context
      early-media-allow
      enforcement-profile
      additional-prefixes
      restricted-latching             none
      restriction-mask                32
      accounting-enable               enabled
      user-cac-mode                   none
      user-cac-bandwidth              0
      user-cac-sessions               0
      icmp-detect-multiplier          0
      icmp-advertisement-interval     0
      icmp-target-ip
      monthly-minutes                 0
      net-management-control          disabled
      delay-media-update              disabled
      refer-call-transfer             disabled
      refer-notify-provisional        none
      dyn-refer-term                  disabled
      codec-policy
      codec-manip-in-realm            disabled
      constraint-name
      call-recording-server-id
      xnq-state                       xnq-unknown
      hairpin-id                      0
      stun-enable                     disabled
      stun-server-ip                  0.0.0.0
      stun-server-port                3478
      stun-changed-ip                 0.0.0.0
      stun-changed-port               3479
      match-media-profiles
      qos-constraint
      sip-profile
      sip-isup-profile
      block-rtcp                      disabled
      hide-egress-media-update        disabled
      tcp-media-profile
      subscription-id-type            END_USER_NONE
      last-modified-by                admin@192.168.10.150
      last-modified-date              2013-01-25 12:25:06
session-agent
      hostname                        10.10.169.16
      ip-address                      10.10.169.16
      port                            5060
      state                           enabled
      app-protocol                    SIP
      app-type
      transport-method                UDP
```

```
realm-id                        Carrier
egress-realm-id
description                     Service-Provider
carriers
allow-next-hop-lp               enabled
constraints                     disabled
max-sessions                    0
max-inbound-sessions            0
max-outbound-sessions           0
max-burst-rate                  0
max-inbound-burst-rate          0
max-outbound-burst-rate         0
max-sustain-rate                0
max-inbound-sustain-rate        0
max-outbound-sustain-rate       0
min-seizures                    5
min-asr                         0
time-to-resume                  0
ttr-no-response                 0
in-service-period               0
burst-rate-window               0
sustain-rate-window             0
req-uri-carrier-mode            None
proxy-mode
redirect-action
loose-routing                   enabled
send-media-session              enabled
response-map
ping-method                     OPTIONS;hops=0
ping-interval                   180
ping-send-mode                  keep-alive
ping-all-addresses              disabled
ping-in-service-response-codes
out-service-response-codes
load-balance-dns-query          hunt
media-profiles
in-translationid
out-translationid
trust-me                        disabled
request-uri-headers
stop-recurse
local-response-map
ping-to-user-part
ping-from-user-part
li-trust-me                     disabled
in-manipulationid
out-manipulationid
manipulation-string
manipulation-pattern
p-asserted-id
trunk-group
max-register-sustain-rate       0
early-media-allow
invalidate-registrations        disabled
rfc2833-mode                    none
rfc2833-payload                 0
codec-policy
enforcement-profile
refer-call-transfer             disabled
refer-notify-provisional        none
reuse-connections               NONE
tcp-keepalive                   none
tcp-reconn-interval             0
```

```
      max-register-burst-rate        0
      register-burst-window          0
      sip-profile
      sip-isup-profile
      kpml-interworking              inherit
      last-modified-by               admin@192.168.10.150
      last-modified-date             2013-01-25 13:37:53
session-agent
      hostname                       192.168.10.12
      ip-address                     192.168.10.12
      port                           5060
      state                          enabled
      app-protocol                   SIP
      app-type
      transport-method               StaticTCP
      realm-id                       Enterprise
      egress-realm-id
      description                    Communication-Manager
      carriers
      allow-next-hop-lp              enabled
      constraints                    disabled
      max-sessions                   0
      max-inbound-sessions           0
      max-outbound-sessions          0
      max-burst-rate                 0
      max-inbound-burst-rate         0
      max-outbound-burst-rate        0
      max-sustain-rate               0
      max-inbound-sustain-rate       0
      max-outbound-sustain-rate      0
      min-seizures                   5
      min-asr                        0
      time-to-resume                 0
      ttr-no-response                0
      in-service-period              0
      burst-rate-window              0
      sustain-rate-window            0
      req-uri-carrier-mode           None
      proxy-mode
      redirect-action
      loose-routing                  enabled
      send-media-session             enabled
      response-map
      ping-method                    OPTIONS;hops=0
      ping-interval                  180
      ping-send-mode                 keep-alive
      ping-all-addresses             disabled
      ping-in-service-response-codes
      out-service-response-codes
      load-balance-dns-query         hunt
      media-profiles
      in-translationid
      out-translationid
      trust-me                       disabled
      request-uri-headers
      stop-recurse
      local-response-map
      ping-to-user-part
      ping-from-user-part
      li-trust-me                    disabled
      in-manipulationid
      out-manipulationid
      manipulation-string
```

```
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        refer-notify-provisional       none
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        kpml-interworking              inherit
        last-modified-by               admin@192.168.10.150
        last-modified-date             2013-01-23 15:39:55
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  Enterprise
        egress-realm-id
        nat-mode                       None
        registrar-domain
        registrar-host
        registrar-port                 0
        register-service-route         always
        init-timer                     500
        max-timer                      4000
        trans-expire                   32
        initial-inv-trans-expire       0
        invite-expire                  180
        inactive-dynamic-conn          32
        enforcement-profile
        pac-method
        pac-interval                   10
        pac-strategy                   PropDist
        pac-load-weight                1
        pac-session-weight             1
        pac-route-weight               1
        pac-callid-lifetime            600
        pac-user-lifetime              3600
        red-sip-port                   1988
        red-max-trans                  10000
        red-sync-start-time            5000
        red-sync-comp-time             1000
        add-reason-header              disabled
        sip-message-len                4096
        enum-sag-match                 disabled
        extra-method-stats             disabled
        extra-enum-stats               disabled
        registration-cache-limit       0
        register-use-to-for-lp         disabled
        refer-src-routing              disabled
        add-ucid-header                disabled
        proxy-sub-events
        allow-pani-for-trusted-only    disabled
```

```
      pass-gruu-contact              disabled
      sag-lookup-on-redirect         disabled
      set-disconnect-time-on-bye     disabled
      msrp-delayed-bye-timer         15
      last-modified-by               admin@192.168.10.150
      last-modified-date             2013-01-23 15:17:45
sip-interface
      state                          enabled
      realm-id                       Carrier
      description
      sip-port
            address                        172.16.157.140
            port                           5060
            transport-protocol             UDP
            tls-profile
            multi-home-addrs
            allow-anonymous                agents-only
            ims-aka-profile
      carriers
      trans-expire                   0
      initial-inv-trans-expire       0
      invite-expire                  0
      max-redirect-contacts          0
      proxy-mode
      redirect-action
      contact-mode                   none
      nat-traversal                  none
      nat-interval                   30
      tcp-nat-interval               90
      registration-caching           disabled
      min-reg-expire                 300
      registration-interval          3600
      route-to-registrar             disabled
      secured-network                disabled
      teluri-scheme                  disabled
      uri-fqdn-domain
      trust-mode                     all
      max-nat-interval               3600
      nat-int-increment              10
      nat-test-increment             30
      sip-dynamic-hnt                disabled
      stop-recurse                   401,407
      port-map-start                 0
      port-map-end                   0
      in-manipulationid
      out-manipulationid
      manipulation-string
      manipulation-pattern
      sip-ims-feature                disabled
      subscribe-reg-event            disabled
      operator-identifier
      anonymous-priority             none
      max-incoming-conns             0
      per-src-ip-max-incoming-conns  0
      inactive-conn-timeout          0
      untrusted-conn-timeout         0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode           pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
```

```
      term-tgrp-mode                 none
      implicit-service-route         disabled
      rfc2833-payload                101
      rfc2833-mode                   transparent
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                disabled
      enforcement-profile
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      sip-profile
      sip-isup-profile
      tcp-conn-dereg                 0
      register-keep-alive            none
      kpml-interworking              disabled
      tunnel-name
      msrp-delay-egress-bye          disabled
      send-380-response
      session-timer-profile
      last-modified-by               admin@192.168.10.150
      last-modified-date             2013-01-23 15:29:44
sip-interface
      state                          enabled
      realm-id                       Enterprise
      description
      sip-port
            address                        192.168.10.52
            port                           5060
            transport-protocol             TCP
            tls-profile
            multi-home-addrs
            allow-anonymous                all
            ims-aka-profile
      carriers
      trans-expire                   0
      initial-inv-trans-expire       0
      invite-expire                  0
      max-redirect-contacts          0
      proxy-mode
      redirect-action
      contact-mode                   none
      nat-traversal                  none
      nat-interval                   30
      tcp-nat-interval               90
      registration-caching           disabled
      min-reg-expire                 300
      registration-interval          3600
      route-to-registrar             disabled
      secured-network                disabled
      teluri-scheme                  disabled
      uri-fqdn-domain
      trust-mode                     all
      max-nat-interval               3600
      nat-int-increment              10
      nat-test-increment             30
      sip-dynamic-hnt                disabled
      stop-recurse                   401,407
      port-map-start                 0
      port-map-end                   0
      in-manipulationid
```

```
      out-manipulationid
      manipulation-string
      manipulation-pattern
      sip-ims-feature                disabled
      subscribe-reg-event            disabled
      operator-identifier
      anonymous-priority             none
      max-incoming-conns             0
      per-src-ip-max-incoming-conns  0
      inactive-conn-timeout          0
      untrusted-conn-timeout         0
      network-id
      ext-policy-server
      default-location-string
      charging-vector-mode           pass
      charging-function-address-mode pass
      ccf-address
      ecf-address
      term-tgrp-mode                 none
      implicit-service-route         disabled
      rfc2833-payload                101
      rfc2833-mode                   transparent
      constraint-name
      response-map
      local-response-map
      ims-aka-feature                disabled
      enforcement-profile
      route-unauthorized-calls
      tcp-keepalive                  none
      add-sdp-invite                 disabled
      add-sdp-profiles
      sip-profile
      sip-isup-profile
      tcp-conn-dereg                 0
      register-keep-alive            none
      kpml-interworking              disabled
      tunnel-name
      msrp-delay-egress-bye          disabled
      send-380-response
      session-timer-profile
      last-modified-by               admin@192.168.10.150
      last-modified-date             2013-01-23 15:28:59
sip-manipulation
      name                           Outbound_HMRs
      description                    Change_host_Remove_Alert_Info
      split-headers
      join-headers
      header-rule
            name                           From
            header-name                    From
            action                         manipulate
            comparison-type                case-insensitive
            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-insensitive
```

```
            match-value
            new-value                       $LOCAL_IP
      header-rule
         name                          To
         header-name                   To
         action                        manipulate
         comparison-type               case-insensitive
         msg-type                      request
         methods
         match-value
         new-value
         element-rule
            name                            To
            parameter-name
            type                            uri-host
            action                          replace
            match-val-type                  any
            comparison-type                 case-insensitive
            match-value
            new-value                       $REMOTE_IP
      header-rule
         name                          P_Asserted_Identity
         header-name                   P-Asserted-Identity
         action                        manipulate
         comparison-type               case-sensitive
         msg-type                      request
         methods
         match-value
         new-value
         element-rule
            name                            P_Asserted_Identity
            parameter-name
            type                            uri-host
            action                          replace
            match-val-type                  any
            comparison-type                 case-insensitive
            match-value
            new-value                       $LOCAL_IP
      header-rule
         name                          Diversion
         header-name                   Diversion
         action                        manipulate
         comparison-type               case-insensitive
         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-insensitive
            match-value
            new-value                       $LOCAL_IP
      header-rule
         name                          Refer
         header-name                   Refer-To
         action                        manipulate
         comparison-type               case-insensitive
         msg-type                      request
         methods
```

```
            match-value
            new-value
            element-rule
                  name                              Refer
                  parameter-name
                  type                              uri-host
                  action                            replace
                  match-val-type                    any
                  comparison-type                   case-insensitive
                  match-value
                  new-value                         $REMOTE_IP
      header-rule
            name                              Alert_Info
            header-name                       Alert-Info
            action                            delete
            comparison-type                   case-insensitive
            msg-type                          any
            methods
            match-value
            new-value
      last-modified-by                  admin@192.168.10.150
      last-modified-date                2013-01-25 12:18:00
steering-pool
      ip-address                        192.168.10.52
      start-port                        2048
      end-port                          3329
      realm-id                          Enterprise
      network-interface
      last-modified-by                  admin@192.168.10.150
      last-modified-date                2013-01-23 14:22:21
steering-pool
      ip-address                        172.16.157.140
      start-port                        40000
      end-port                          60000
      realm-id                          Carrier
      network-interface
      last-modified-by                  admin@192.168.10.150
      last-modified-date                2013-01-23 14:20:25
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                 0.0.0.0
      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-signaling-mtu              1500
      ipv4-signaling-mtu              1500
      cleanup-time-of-day             00:00
      snmp-engine-id-suffix
      snmp-agent-mode                 v1v2
      last-modified-by                admin@192.168.10.150
      last-modified-date              2011-05-27 20:11:35
task done
```

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.