Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.0.1 and Acme Packet 4250 Net-Net Session Director 6.2.0 with Qwest iQ® SIP Trunk (version 6.5.7R1) – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Qwest iQ® SIP Trunk (version 6.5.7R1) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.0.1 and Acme Packet 4250 Net-Net Session Director 6.2.0 with various Avaya endpoints.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solutions and Interoperability Test Lab, utilizing Qwest SIP Trunk Services.

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager 6.0.1 and Acme Packet 4250 Net-Net Session Director 6.2.0 (Acme Packet 4250) integration with Qwest iQ® SIP Trunk (version 6.5.7R1).

In the sample configuration, the Acme Packet 4250 is used as an edge device between Avaya Customer Premise Equipment (CPE) and the Qwest-SIP Trunk. The Acme Packet 4250 performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the Qwest-SIP Trunk access method. The Acme Packet 4250 connects to the service provider through one physical interface but with two different virtual connections. One to a SIP switch termination called East and one to a SIP switch called West. The Acme Packet 4250 is configured to round-robin between these two locations. Having multiple far-end destinations required that some SIP header manipulations be entered into the Acme Packet 4250. If there was one location, just the far-end IP address could be listed on the Avaya Aura® Communication Manager SIP signaling group, however because Qwest iQ® SIP Trunk (version 6.5.7R1) sends the IP address in SIP messages and we have two far-end destinations, we used header manipulations.

The Avaya Aura® Communication Manager and Acme Packet 4250 are directly connected with two Avaya Aura® Communication Manager SIP trunks (one to a Control LAN (CLAN) and one to the Processor Ethernet (PROCR) interface), Avaya Modular Messaging is also connected to the Avaya Aura® Communication Manager through a SIP trunk.

Qwest SIP Trunk service is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

Qwest SIP Trunk service will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE). SIP Trunk service will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

While this solution was tested with the ACME packet 4250, which is end-of-sale, the 3800 and 4500 are available with similar software and similar functionality and would be an appropriate substitute.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Qwest SIP Trunk service via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Avaya Aura® Communication Manager, the Acme Packet 4250, and various Avaya endpoints.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows to / from Communication Manager 6.0.1 and the Acme Packet 4250, and subsequent redirection of inbound calls to Qwest-SIP Trunk. The items below were covered in the compliance test:

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types.
  Phone types included H.323, digital, and analog telephones at the enterprise. Since there was not a Session Manager or SIP Enablement Server (SES) in the test configuration, no SIP phones were used during the testing. Inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types.
  Phone types included H.323, digital, and analog telephones at the enterprise. Outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client). Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X® Communicator also supports two Voice Over IP (VoIP) protocols: H.323 and SIP. Only the H.323 version of Communicator was tested.
- Various call types including: local, long distance, emergency, international, outbound toll-free, operator (0) and 0+ dialing.
- Codecs G.711MU, G.729A, and G.729AB were tested.
- DTMF transmission using RFC 2833.
- T.38 Fax
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- All trunks busy scenarios
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).
- Network re-direct using REFER
- Round Robin on outgoing calls to PSTN – East and West SIP gateways
- Round Robin on incoming calls to the CLAN and PROCR

2.2. Support

2.2.1. Avaya

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

2.2.2. CenturyLink™

Century**Link** acquired Qwest in April 2011. Over time Qwest branded services and web sites may be renamed by Century**Link.**

For technical support on the Qwest iQ SIP Trunk services, contact Customer Service at http://www.qwest.com/business/products/products-and-services/voip-adv-voice/sip-trunk.html Enter your phone number and click "Speak to us now" and Customer Service will call you or select the "Email us" link to send an e-mail inquiry or click "Contact a rep" and fill in the request information.

2.3. Test Results / Known Limitations

Interoperability testing of Qwest iQ SIP Trunk (version 6.5.7R1) was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **No Error Indication if No Matching Codec Offered on Inbound Calls**: If the Communication Manager SIP trunk is improperly configured to have no matching codec with the service provider and an inbound call is placed, the enterprise only returns a "488 Not Acceptable Here" response and the caller will hear a fast busy after 30 seconds. Codecs are normally agreed to upon turn-up so this condition should be discovered at that time.

- **No Error Indication if No Matching Codec Offered on Outbound Calls**: If the Communication Manager SIP trunk is improperly configured to have no matching codec with the service provider and an outbound call is placed, the service provider only returns a "487 Request Terminated" response. The caller will hear a fast busy and the called party will hear one ring before the call is terminated. Codecs are normally agreed to upon turn-up so this condition should be discovered at that time.

- **No Support for G.729B:** Qwest SIP Trunk service does not support G.729B codec.

- **Calling Party Number (PSTN transfers)**: The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/Qwest SIP Trunk solution. It is listed here simply as an observation.

- **Asynchronous DTMF payload header values are not supported**: Qwest SIP Trunk service does not support the use of a different DTMF payload header value in each direction of a single call. This may occur if the media is re-directed from Communication Manager to an endpoint and the endpoint wishes to use a different DTMF payload header value than was negotiated when the call was initially established. Qwest SIP Trunk service will send a re-INVITE to force the DTMF

payload header value to be the same in each direction. In response, Communication Manager will send a re-INVITE to force the DTMF payload header value back to the original asynchronous values which allow the DTMF payload header value to be the same end-to-end in the same direction (even though the values are different in each direction). These re-INVITEs continue for several minutes before one side gives up and tears down the call. This issue manifested itself in two separate call scenarios during the compliance test described below. This issue may occur in other call scenarios that were not tested.

- **An inbound call from the PSTN to an enterprise Avaya phone that is transferred back to the PSTN unattended will drop after several minutes**. This is because Qwest SIP Trunk uses a value of 100 for the DTMF payload header value and the Communication Manager uses a value of 127 by default. This scenario can be avoided by setting the "Telephone Event Payload Type" on the trunk group form, page 4, to a value of 100.
- **An inbound call from the PSTN to Avaya phone that is transferred back to the PSTN using an attended transfer will drop after several minutes.** This is the same scenario as described above except for attended and the corrective action is the same.

- **All Trunks Busy will ring from 7 – 40 seconds before fast busy**: When all Communication Manager trunk group members are busy, the caller will hear ringing for anywhere from 7 seconds to 40 seconds before finally hearing a fast busy. Qwest SIP Trunk service will send the call to Communication Manager and it will erroneously return a "403 Forbidden" instead of a "503 Service Unavailable". The workaround for this is to upgrade to one of the following loads: CM 5.2.1 SP9, CM 6.0.1 SP3, CM 6.2. Use of a 503 allows for a back-off time period and a retry by Qwest.

- **SIP Network REFER off-net is not supported**: When Communication Manager receives a PSTN call and tries to use a vector to automatically re-direct using a SIP REFER to another PSTN destination, the call will drop. Qwest SIP Trunk service does not allow re-directs to/from non-Qwest PSTN numbers.

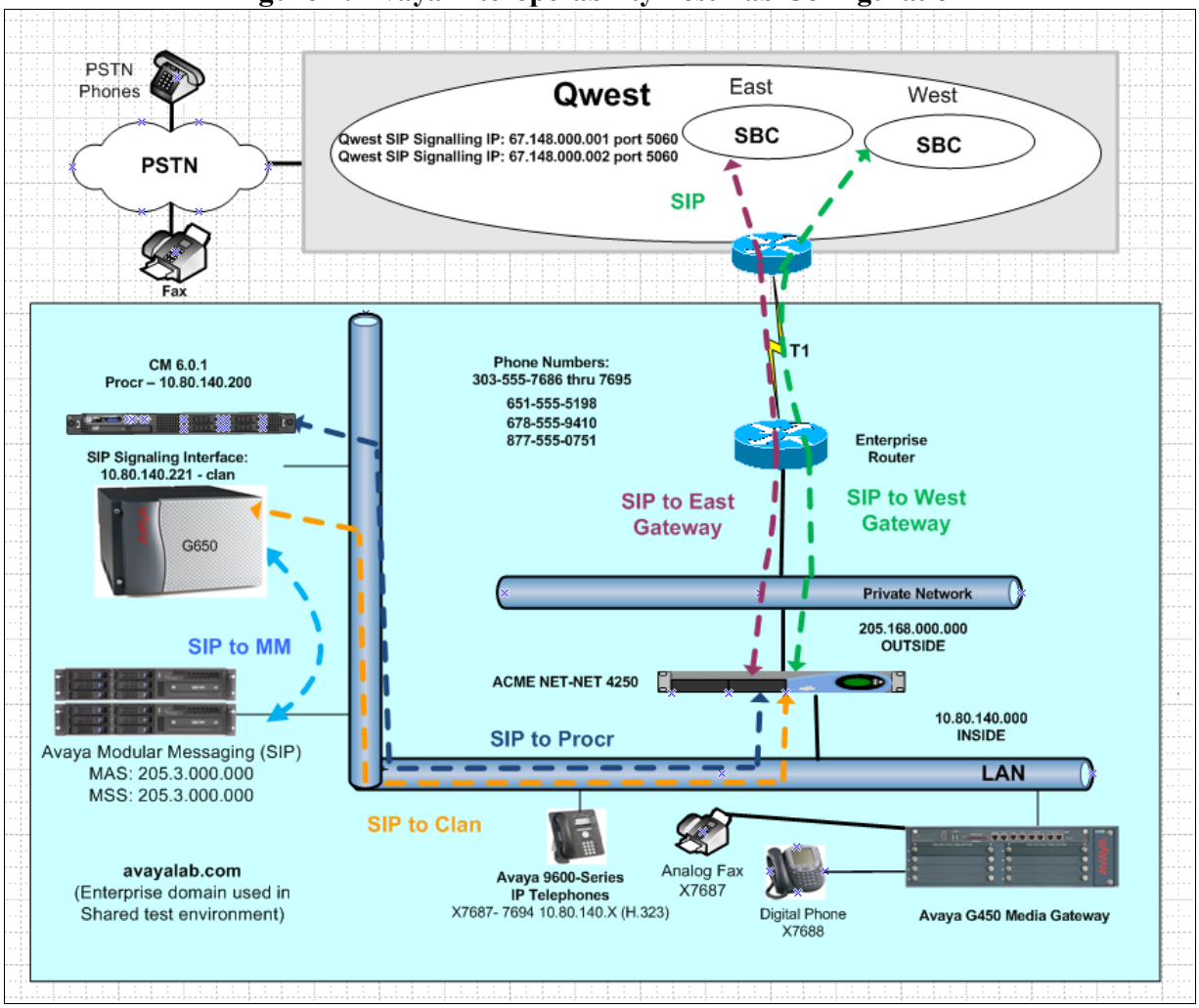
- **SIP REFER with transfer (consultative or blind) is not supported in Qwest iQ® SIP Trunk service (version 6.5.7R1):** When an extension receives a call from a PSTN number and attempts to transfer (either consultative or blind) the call to another PSTN destination, the call will initially connect and then will be dropped as soon as the transfer is completed on the enterprise user's side. This is addressed in a future Qwest iQ® SIP Trunk release, meanwhile the work-around is to have the **Network Call Redirection** field set to "n" on page 4 of the trunk group form, refer to section 5.7.

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE enterprise location connected via a T1 Internet connection to the Qwest iQ® SIP Trunks to East and West servers. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Acme Packet 4250 provides

NAT functionality and SIP header manipulation. The Acme Packet 4250 receives traffic from the Qwest iQ® SIP Trunk on port 5060 and sends traffic to the Qwest iQ® SIP Trunk using destination port 5060, using the UDP protocol.

Figure 1: Avaya Interoperability Test Lab Configuration



3.1. Interoperability Compliance Testing

Two separate trunks were created between Communication Manager and the Acme Packet 4250 to carry the service provider traffic; one to the CLAN in a G650 gateway and one to the PROCR of the server. These trunks carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the Acme Packet 4250 then to Communication Manager after header manipulation. Communication Manager uses the

configured dial patterns and routing policies to determine the recipient and any further incoming call treatment, such as incoming digit translations and class of service restrictions.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to the Acme Packet 4250. The Acme Packet 4250 forwards the call to a Qwest SIP Trunk after header manipulation.

4. Equipment and Software Validated

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

Equipment:	Software:
Avaya S8510 Server (Communication Manager)	Avaya Aura® Communication Manager Release 6.0.1 load 510.1
G650 Gateway TN2312BP (IPSI) TN2602AP (MedPro) TN799DP (CLAN) TN2224B (Digital Line Card) TN793B (Analog Line Card)	 HW36 FW 51 HW28 FW55 HW16 FW38 HW12 HW6
G450 Gateway	FW 30.12.1
Acme Packet 4250 Net-Net Session Director	Firmware SC6.2.0 MR-6 GA (Build 832)
Avaya Modular Messaging (Application Server)	Avaya Modular Messaging (MAS) 5.2 Service Pack 5 Patch 1
Avaya Modular Messaging (Storage Server)	Avaya Modular Messaging (MSS) 5.2, Build 5.2-11.0
Avaya 9600-Series Telephones (H.323)	Release 030909 - H.323 - 4625 Release 3.0 – H.323 -9630 Release 6.0 - H.323 - 9608, 9621
Avaya One-X Communicator (H.323)	Release 6.0.1.16-SP1-25226
Avaya 2400-Series and 6400-Series Digital Telephones	N/A

5. Configure Communication Manager

This section describes the procedure for configuring Avaya Aura® Communication Manager for Qwest SIP Trunk service. Two SIP trunks are established between Avaya Aura® Communication Manager and the Acme Packet 4250 for use by signaling traffic to and from the Qwest SIP Trunk service. It is assumed the general installation of Avaya Aura® Communication Manager and the Avaya G650 / G450 Media Gateways has been previously completed and is not discussed here.

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

brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **24000** SIP trunks are available and **257** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 6
             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: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                   Maximum Administered SIP Trunks: 24000 257
  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   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

On **Page 3** of the **System-Parameters Customer-Options** form, verify that **ARS** is enabled.

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

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

On **Page 4** of the **System-Parameters Customer-Options** form, verify that **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging will be required for the call flows, verify that the **ISDN/SIP Network Call Redirection** feature is enabled.

```
 display system-parameters customer-options                          Page   4 of  11
                                OPTIONAL FEATURES

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

On **Page 6** of the **System-Parameters Customer-Options** form, verify that any required call center features are enabled. In the sample configuration, vectoring is used to refer calls to alternate destinations using SIP NCR (Network Call Redirect). Vector variables are used to include User-User Information (UUI) with the referred calls.

```
display system-parameters customer-options                Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 6.0

                                ACD? y                          Reason Codes? y
                       BCMS (Basic)? y                Service Level Maximizer? n
         BCMS/VuStats Service Level? y              Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                  Business Advocate? n               Service Observing (VDNs)? y
                    Call Work Codes? y                                Timed ACW? y
      DTMF Feedback Signals For VRU? y                    Vectoring (Basic)? y
                  Dynamic Advocate? n                  Vectoring (Prompting)? y
       Expert Agent Selection (EAS)? y              Vectoring (G3V4 Enhanced)? y
                           EAS-PHD? y               Vectoring (3.0 Enhanced)? y
                  Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
               Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                      Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y                   Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y                Vectoring (Variables)? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System Features

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

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

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

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

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

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

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the CLAN of the G650 gateway, the PROCR interface of the Avaya Server running Communication Manager and for the Acme Packet 4250 inside interface. These node names will be needed for defining the service provider signaling group in **Section 5.6**.

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                IP Address
Acme-Inside           10.80.140.254
Gateway1              10.80.140.1
Gateway254            10.80.140.254
MM                    10.80.140.56
MedPro1A03            10.80.140.222
MedPro1A04            10.80.140.223
clan                  10.80.140.221
default               0.0.0.0
procr                 10.80.140.200
```

The output for the **list registered-ip stations** shows that IP endpoint registrations are split between the **PROCR** and the **CLAN**.

```
 list registered-ip-stations
                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
7687          9630      IP_Phone    y  10.80.140.55
              1         3.0020         10.80.140.200
7689          9620      IP_Phone    y  10.80.140.51
              1         6.0000         10.80.140.200
7690          9630      IP_Phone    y  10.80.140.52
              1         6.0000         10.80.140.221
7691          9630      IP_Phone    y  10.80.140.53
              1         6.0000         10.80.140.200
7692          9650      IP_Phone    y  10.80.140.54
              1         3.0020         10.80.140.221
7694          4625      IP_Phone    y  10.80.140.56
              1         2.9010         10.80.140.200
```

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, codecs G.729A and G.711MU were tested using ip-codec-set 1. To use these codecs, enter ***G.711MU*** and ***G.729A*** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields. Silence suppression is normally set to **n** and packet size is standard at **20ms**.

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

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

On **Page 2**, set the **Fax Mode** to ***T.38-standard*** for fax support.

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

                               Allow Direct-IP Multimedia? n

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

5.5. IP Network Region

You can create a separate IP network region for the service provider trunk if desired. This allows for separate codecs 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 1 was chosen for the service provider trunk. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

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

```
change ip-network-region 1                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avayalab.com
    Name: Enterprise
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 34
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        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 in region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 1 will be used for calls in region 1 (both calls to the service provider and calls within the enterprise side).

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

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Acme Packet 4250 for use by the service provider trunks. These signaling groups are used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling groups 4 and 5 were used for this purpose and were configured using the parameters highlighted below.

NOTE: Qwest SIP Trunk uses an IP address in the SIP URI field of the SIP messages that it sends/receives. Avaya Best Practices also recommend that the **Far-end Domain** be populated for additional security. Since the configuration contains two SIP service provider far ends (East and West) and two endpoints to round-robin , ***qwest.com*** will be used in the **Far-end Domain** field. This means that the Acme Packet 4250 will be used to manipulate the header of all messages coming in and going out. If this field is left blank (**Far-end Domain) (**not recommended**),** or there was only one far-end (an IP address could be used in the **Far-end Domain)**, or if the service provider sent a domain name (ex. qwest.com) in the SIP URI instead of an IP address, this manipulation would not be necessary. The header manipulation in Section 6.12 called NatIp will change the P-Asserted Identity on inbound calls from an IP address to the domain of qwest.com and the header maniuplation called NatURI will change the SIP URI to/from an IP address to/from the domain qwest.com for outbound calls.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). For ease of troubleshooting during testing, part of the compliance test was conducted with the **Transport Method** set to ***tcp***. The transport method specified here is used between the Communication Manager and the Acme Packet 4250.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP/UDP the well-known port value is 5060). The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to ***5060***.
- Set the **Near-end Node Name** to ***clan*** *or* ***procr***. This node name maps to the IP address of the CLAN in the G650 gateway or the PROCR as defined in the **node-names ip** screen shot in **section 5.3**.

- Set the **Far-end Node Name** to ***Acme-inside***. This node name maps to the IP address of Acme Packet 4250 Inside interface as defined in the **node-names-ip** screen shot in section 5.3.
- Set the **Far-end Network Region** to the IP network region for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the domain of the enterprise (usually an IP Address or a domain name). For the compliance test **qwest.com** was used (see note above).
- Set **Direct IP-IP Audio Connections** to ***y***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set **Initial IP-IP Direct Media** to ***n***. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. Both Direct and Initial IP-IP Direct Media need to be set as indicated for Early Media to be Enabled.
- Set the **DTMF over IP** field to ***rtp-payload***. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to ***15***. This defines the number of seconds the that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

Signaling group from the ***CLAN*** interface.

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

 Group Number: 4              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                          SIP Enabled LSP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: Others

   Near-end Node Name: clan                 Far-end Node Name: ACME-Inside
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                          Far-end Network Region: 1

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

Signaling group from the ***PROCR*** interface.-

```
change signaling-group 5                                        Page   1 of   1
                              SIGNALING GROUP

 Group Number: 5             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                        SIP Enabled LSP? 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-Inside
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                          Far-end Network Region: 1

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

5.7. 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 groups 4 and 5 were configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- 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: OUTSIDE CALL                COR: 1        TN: 1        TAC: *104
   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: 10
```

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

Group Number: 5                    Group Type: sip           CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC: *109
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 5
                                                   Number of Members: 10
```

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

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

```
change trunk-group 5                                          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 4**, set the **Network Call Redirection** field and the **Send Diversion Header** field to ***y***. These fields provide additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Telephone Event Payload Type** to ***100***, the value preferred by Qwest SIP Trunk.

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

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                 Network Call Redirection? y
                    Send Diversion Header? y
                  Support Request History? y
             Telephone Event Payload Type: 100


       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

5.8. 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** and of length **1** as a feature access code (**fac**).

```
change dialplan analysis                                      Page   1 of  12
                              DIAL PLAN ANALYSIS TABLE
                                    Location: all            Percent Full: 2
   Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
   String   Length Type     String   Length Type     String   Length Type
   1           3   fac
   10          4   ext
   2           4   ext
   3           4   ext
   7           3   fac
   7           4   ext
   8           4   ext
   9           1   fac
   *           3   fac
   *10         4   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  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: 137
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code: 160
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: 115
                       Answer Back Access Code: 116
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *88
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: 120    Deactivation: 121
Call Forwarding Activation Busy/DA: 122    All: 123    Deactivation: 124
```

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

```
change ars analysis 0                                          Page   1 of   2
                              ARS DIGIT ANALYSIS TABLE
                                     Location: all            Percent Full: 1
          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    0                     1    1     1        op           n
    0                     8    8     1        op           n
    0                     11   11    1        op           n
    00                    2    2     deny     op           n
    01                    9    17    deny     iop          n
    011                   10   18    1        intl         n
    101xxxx0              8    8     deny     op           n
    101xxxx0              18   18    deny     op           n
    101xxxx01             16   24    deny     iop          n
    101xxxx011            17   25    deny     intl         n
    101xxxx1              18   18    deny     fnpa         n
    10xxx0                6    6     deny     op           n
    10xxx0                16   16    deny     op           n
    10xxx01               14   22    deny     iop          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 1 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the SIP service provider. For the compliance test, trunk group 3 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level.
- **Pfx Mrk**: ***1*** The prefix mark (**Pfx Mrk**) of one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **LAR**: ***next***

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: toACME
                              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

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

5.9. Vector Directory Numbers (VDNs) and Vectors for SIP NCR

This section describes the basic commands used to configure Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke the Communication Manager SIP Network Call Redirection (NCR) functionality and also SIP "302 Temporarily Moved" messages. These Application Notes provide rudimentary vector definitions to demonstrate and test the SIP NCR and UUI functionalities. In general, call centers will use vector functionality that is more complex and tailored to individual needs. Call centers may also use customer hosts running applications used in conjunction with Application Enablement Services (AES) to define call routing and provide associated UUI. The definition and documentation of those complex applications and associated vectors are beyond the scope of these Application Notes.

5.9.1. Pre-answer Redirection to a PSTN Destination

This section provides an example configuration of a vector that will use pre-answer redirection to a PSTN destination. In this example, the inbound number 303-555-7693 is routed to VDN 3999 by the incoming call handling treatment for the inbound trunk group, shown in **Section 5.10**.

```
display vdn 3999                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER
                             Extension: 3999
                                 Name*: Call Center
                           Destination: Vector Number        3
                     Attendant Vectoring? n
                    Meet-me Conferencing? n
                      Allow VDN Override? n
                                     COR: 1
```

VDN 3999 is associated with vector 3, which is shown below. Vector 3 waits 2 seconds while hearing ringback (step 1) then transfers the call off-net (step 2) to a PSTN destination (**~r3035551856)**. Since the call is being transferred pre-answer, Communication Manager issues a **302 Temporarily Moved** in response. This message is then manipulated by the Acme Packet 4250 into an INVITE that is sent to the Service Provider as shown in **section 6.12.2**

```
display vector 3                                                Page   1 of   6
                                   CALL VECTOR

    Number: 3                Name: test
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 route-to     number ~r3035551856     with cov n if unconditionally
03 disconnect   after announcement 3997
```

5.9.2. Post-Answer Redirection to a PSTN Destination

This section provides an example configuration of a vector that will use post-answer redirection to a PSTN destination. In this example, the inbound toll-free call is routed to VDN 3991. The originally dialed service provider Toll Free number is mapped to VDN 3991 by the incoming call handling treatment for the inbound trunk group, shown in **Section 5.10**. SIP NCR to an off-net destination is not supported by Qwest as listed in Section 2.3 Test Results / Known Limitations. However, it is possible to use SIP NCR to forward to an internal location and is also displayed for completeness. To forward to an internal destination, the number **~r3035551890** could be replaced by **7690** or any valid extension number.

```
display vdn 3991                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER
                             Extension: 3991
                                 Name*: Qwest Call Center
                           Destination: Vector Number        2
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: internal
        Acceptable Service Level (sec): 20                    TN*: 1
                              Measured: internal
        Acceptable Service Level (sec): 20
```

VDN 3991 is associated with vector 2, which is shown below. Vector 2 plays an announcement and collects 5 digits (step 3) to answer the call. After the digit collection, the UUI to send is set with variable A (step 5), then the **route-to number** (step 7) includes **~r3035551890** where the number 303-555-1890 is a PSTN destination. This step causes a REFER message to be sent where the Refer-To header includes **13035551890** as the user portion.

```
display vector 2                                                Page   1 of   6
                                   CALL VECTOR

    Number: 2                 Name: PreAns Redirect
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 #    Collect 5 digits - which answers the call
03 collect      5    digits after announcement 3998     for none
04 #    Define a UUI variable to set with the redirection
05 set          A      = none   CATR  1234567890123456
06 #    Refer to PSTN
07 route-to     number ~r3035551890     with cov n if unconditionally
08 #    If Refer fails, play announcement and disconnect
09 disconnect   after announcement 3997
```

```
display variables                                               Page   1 of  39
                                VARIABLES FOR VECTORS

Var Description                   Type    Scope Length Start Assignment       VAC
A   test                          asaiuui L     16     1
B
```

5.10. Incoming Call Handling Treatment for Incoming Calls

In general, the "incoming call handling treatment" for a trunk group can be used to manipulate the digits received for an incoming call if necessary. The toll-free number sent by Qwest SIP Trunk service can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of toll-free number **8775550751** to extension **3991**.

```
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 3035557693       10  3999
 public-ntwrk    10 6515555198       10  7693
 public-ntwrk    10 6785559410       10  7688
 public-ntwrk    10 8775550751       10  3991
 public-ntwrk    10 303555           6
```

5.11. Modular Messaging Hunt Group

Although not specifically related to Qwest SIP Trunk service, this section shows the hunt group used for access to Avaya Modular Messaging. In the sample configuration, users with voice mail have a coverage path containing **hunt group 99**. Users can dial extension **7999** to reach Modular Messaging (e.g., for message retrieval). The following screen shows **Page 1** of hunt-group 99.

```
display hunt-group 99                                          Page   1 of  60
                                   HUNT GROUP

            Group Number: 99                                 ACD? n
              Group Name: MM                               Queue? n
         Group Extension: 7999                           Vector? n
              Group Type: ucd-mia                 Coverage Path:
                      TN: 1           Night Service Destination:
                     COR: 1                     MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name
```

The following screen shows **Page 2** of **hunt-group 99**, which routes to the AAR access code ***88** and **Voice Mail Number 7999**.

```
display hunt-group 99                                          Page   2 of  60
                                   HUNT GROUP

                       Message Center: sip-adjunct

     Voice Mail Number        Voice Mail Handle         Routing Digits
                                                   (e.g., AAR/ARS Access Code)
     7999                     MM                        *88
```

5.12. AAR Routing to Modular Messaging

Although not specifically related to Qwest SIP Trunk service, this section shows the AAR routing for the number used in the hunt group in the previous section. The bold row shows that calls to the number **7999**, which is the Modular Messaging Group Extension for hunt group 99, will use **Route Pattern 2**.

```
change aar analysis 7                                          Page   1 of   2
                              AAR DIGIT ANALYSIS TABLE
                                     Location: all            Percent Full: 1
          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd

    7999                  4    4     2        unku         n
```

6. Acme Packet 4250 Configuration

6.1. Initial Installation

The following sections describe the provisioning of the Acme Packet 4250. Only the Acme Packet 4250 provisioning required for the reference configuration is described in these Application Notes. The full Acme Packet 4250 configuration file is shown in **Appendix A**.

The Acme Packet 4250 was configured using the Acme Packet 4250 CLI via a serial console port connection and via an IP connection once the system config/bootparams were completed. The following are the generic steps for configuring various elements.

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

Once the provisioning is complete, the configuration may be verified by entering the ***show running-config*** command.
The suggested order of configuration for Acme Packet 4250 elements are:

system-config
phy-interface
network-interface
media-manager
realm-config
steering-pool
sip-interface
sip-nat
sip-manipulation
session-agent
session-group
local-policy

6.2. System Config

The system configuration is the basic management information for the system, some fields are optional.

1. Enter **system → system-config**
2. Enter **hostname → ACME**
3. Enter **description → ACME_to_Qwest**
4. Enter **mib-system-name → ACME_to_Qwest**
5. Enter **default-gateway → 10.80.140.1**
6. Enter **cli-more → enabled**
7. Enter **done**
8. Enter **exit**

6.3. Physical Interfaces

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

6.3.1. Management Interface (wancom0)

1. Enter **system → phy-interface**
2. Enter **name → wancom0**
3. Enter **operation-type → Control**
4. Enter **port → 0**
5. Enter **slot → 2** **(This is on the rear of the box – not shown)**
6. Enter **done**
7. Enter **exit**

6.3.2. Public Interface

Create a phy-interface for the public side of the Acme Packet 4250.

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

6.3.3. Private Interface

Create a phy-interface for the private enterprise side of the Acme Packet 4250.

1. Enter **system → phy-interface**
2. Enter **name → s1p0**
3. Enter **operation-type → Media**
4. Enter **port → 0**
5. Enter **slot → 1**
6. Enter **duplex-mode → FULL**

7. Enter **speed → 100**
8. Enter **done**
9. Enter **exit**

6.4. Network Interfaces

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

6.4.1. Public Interface

Create a network-interface for the public side of the Acme Packet 4250.

1. Enter **system → network-interface**
2. Enter **name → s0p0**
3. Enter **ip-address → 205.1.1.112**
4. Enter **netmask → 255.255.255.128**
5. Enter **gateway → 205.1.1.1**
6. Enter **description → ToServiceProvider**
7. Enter **done**
8. Enter **exit**

6.4.2. Private Interface

Create a network-interface for the private enterprise side of the Acme Packet 4250.

1. Enter **system → network-interface**
2. Enter **name → s1p0**
3. Enter **ip-address → 10.80.140.254**
4. Enter **netmask → 255.255.255.0**
5. Enter **gateway → 10.80.140.1**
6. Enter **description → ToAvaya**
7. Enter **done**
8. Enter **exit**

6.5. Media-Manager

Verify that the media-manager process is enabled.

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

6.6. Realms

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

6.6.1. Outside Realm

Create a realm for the external network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → Outside**
3. Enter **network-interfaces → s0p0:0**
4. Enter **out-manipulationid →NatIpOutside (This will be defined in Section 6.11)**
5. Enter **done**
6. Enter **exit**

6.6.2. Inside Realm

Create a realm for the internal network.

1. Enter **media-manager → realm-config**
2. Enter **identifier → Inside**
3. Enter **network-interfaces → s1p0:0**
4. Enter **in-manipulationid →Fix302 (This will be defined in Section 6.11)**
5. Enter **out-manipulationid →NatIp (This will be defined in Section 6.11)**
6. Enter **done**
7. Enter **exit**

6.7. Steering-Pools

Steering pools define sets of ports that are used for steering media flows thru the Acme Packet 4250.

6.7.1. Outside Steering-Pool

Create a steering-pool for the outside network. The start-port and end-port values should specify a range acceptable to the Qwest SIP Trunk.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 205.1.1.112**
3. Enter **start-port → 8000**
4. Enter **end-port → 39998**
5. Enter **realm-id → Outside**
6. Enter **done**
7. Enter **exit**

6.7.2. Inside Steering-Pool

Create a steering-pool for the inside network. The start-port and end-port values should specify a range acceptable to the internal enterprise network and include the port range used by Communication Manager. For the compliance test, a wide range was selected that included the default port range that Communication Manager uses as shown on the ip-network-region form in **Section 5.5**.

1. Enter **media-manager → steering-pool**
2. Enter **ip-address → 10.80.140.254**
3. Enter **start-port → 2048**
4. Enter **end-port → 8001**
5. Enter **realm-id → Inside**
6. Enter **done**
7. Enter **exit**

6.8. SIP Configuration

This command sets the values for the Acme Packet 4250 SIP operating parameters. The home-realm defines the SIP daemon location, and the egress-realm is the realm that will be used to send a request if a realm is not specified elsewhere.

1. Enter **session-router → sip-config**
2. Enter **state → enabled**
3. Enter **operation-mode → dialog**
4. Enter **home-realm-id → Inside**
5. Enter **egress-realm-id → Inside**
6. Enter **options → max-udp-length=0 (You must have this or you will get errors about the packet size being too large.)**
7. Enter **done**
8. Enter **exit**

6.9. SIP Interfaces

The SIP interface defines the SIP signaling interface (IP address and port) on the Acme Packet 4250. SIP header manipulations can be applied at the SIP interface level.

6.9.1. Outside SIP Interface

Create a sip-interface for the outside network.

1. Enter **session-router → sip-interface**
2. Enter **state → enabled**
3. Enter **realm-id → Outside**
4. Enter **sip-port**
    a. Enter **address → 205.168.000.000**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → UDP**
    d. Enter **allow-anonymous → all**
    e. Enter **done**
    f. Enter **exit**
5. Enter **stop-recurse → 401,407**
6. Enter **rfc2833-payload →100 (This is the Qwest defined payload type)**
7. Enter **done**
8. Enter **exit**

6.9.2. Inside SIP Interface

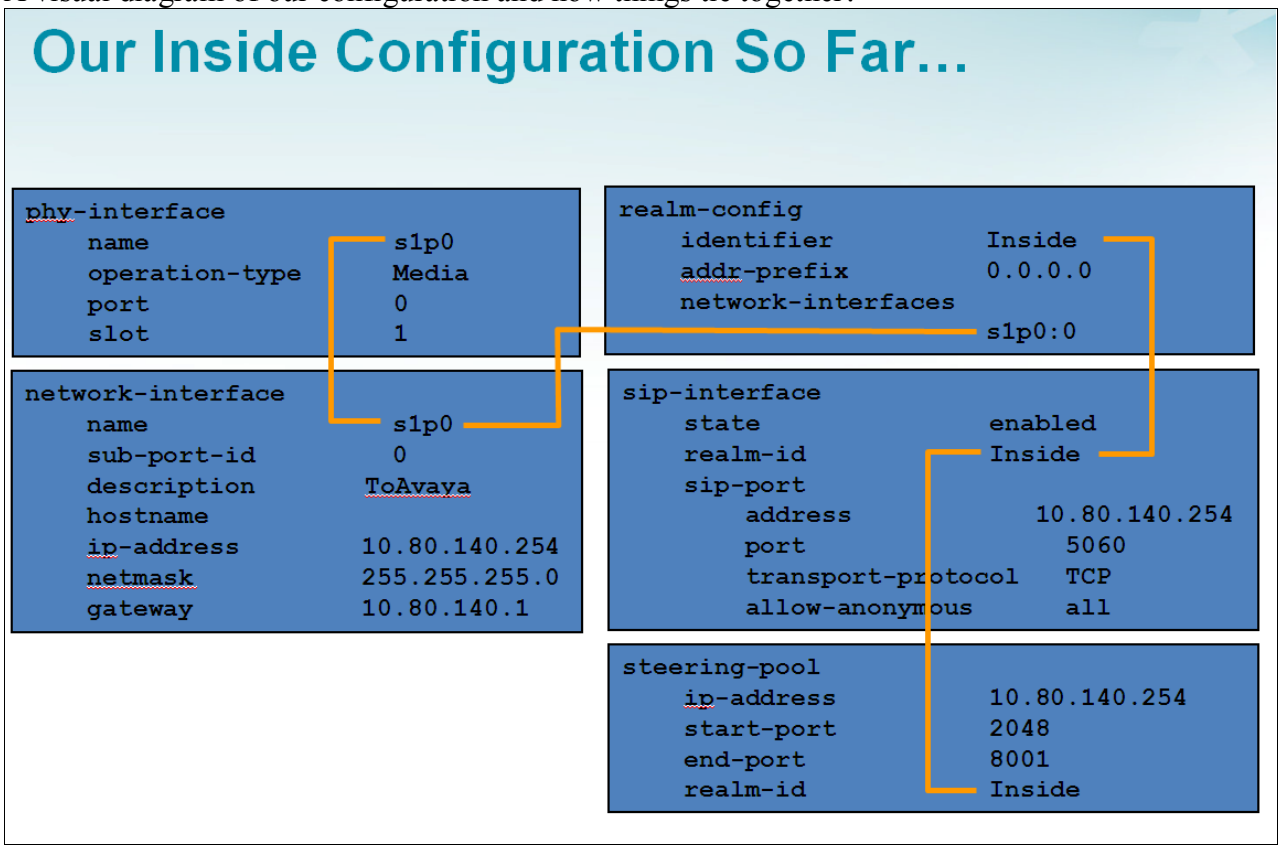
Create a sip-interface for the inside network.

1. Enter **session-router → sip-interface**
2. Enter **state → enabled**
3. Enter **realm-id → Inside**
4. Enter **sip-port**
    a. Enter **address → 10.80.140.254**
    b. Enter **port → 5060**
    c. Enter **transport-protocol → TCP**

d. Enter **allow-anonymous → all**
e. Enter **done**
f. Enter **exit**

5. Enter **stop-recurse → 401,407**
6. Enter **rfc2833-payload →100** **(This is the Qwest defined payload type)**
7. Enter **done**
8. Enter **exit**

A visual diagram of our configuration and how things tie together:



6.10. Session-Agents and Session Agent Groups (SAG)

A session-agent defines the "next hop" signaling entity for SIP traffic. A realm is associated with a session-agent to identify sessions coming from or going to the session-agent. A session-agent is defined for the service provider (outside) and Communication Manager (inside). SIP header manipulations can be applied at the session-agent level. SAGs can also be defined for multiple connections and then a strategy for using multiple connections.

6.10.1. Outside Session-Agent

For this configuration there are two service provider gateways, East and West. The strategy that is being implemented is a Round-Robin; to do this two outside session agents will be used. The **hostname** and **ip-address** will be the address of the service provider SIP gateway.

Create a session-agent for the outside network location 1 (East).

1. Enter **session-router → session-agent**
2. Enter **hostname → 67.148.000.1**
3. Enter **ip-address → 67.148.000.1**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP**
8. Enter **realm-id → Outside**
9. Enter **description → East**
10. Enter **ping-method → OPTIONS;hops=70**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **done**
14. Enter **exit**

Create a session-agent for the outside network location 2 (West).

1. Enter **session-router → session-agent**
2. Enter **hostname → 67.148.000.2**
3. Enter **ip-address → 67.148.000.2**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP**
8. Enter **realm-id → Outside**
9. Enter **description → West**
10. Enter **ping-method → OPTIONS;hops=70**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **done**
14. Enter **exit**

6.10.2. Inside Session-Agent

Create a session-agent for the inside network. In this configuration we will have two session agents because we have created two SIP trunks on the Communication Manager, one that terminates on the CLAN and one that terminates on the PROCR interface.

Create a session-agent for the inside clan.

1. Enter **session-router → session-agent**
2. Enter **hostname → 10.80.140.221**
3. Enter **ip-address → 10.80.140.221**
4. Enter **port → 5060**
5. Enter **transport-method → UDP+TCP**
6. Enter **realm-id → Inside**
7. Enter **description → clan**

8. Enter **ping-method → OPTIONS;hops=70**
9. Enter **ping-interval → 60**
10. Enter **ping-send-mode → keep-alive**
11. Enter **done**
12. Enter **exit**

Create a session-agent for the inside procr.

1. Enter **session-router → session-agent**
2. Enter **hostname → 10.80.140.200**
3. Enter **ip-address → 10.80.140.200**
4. Enter **port → 5060**
5. Enter **state → enabled**
6. Enter **app-protocol → SIP**
7. Enter **transport-method → UDP+TCP**
8. Enter **realm-id → Inside**
9. Enter **description → procr**
10. Enter **ping-method → OPTIONS;hops=70**
11. Enter **ping-interval → 60**
12. Enter **ping-send-mode → keep-alive**
13. Enter **done**
14. Enter **exit**

6.10.3. Outside Session Agent Group

The outside session-agent group will allow the calls to round-robin between the East and West locations. If you only have one location to forward call traffic to, you do not need a SAG. This will be applied to the local policy in **section 6.11**.

1. Enter **session-router → session-group**
2. Enter **group-name → Outside_group**
3. Enter **description → Outside_group**
4. Enter **state →enabled**
5. Enter **app-protocol → SIP**
6. Enter **strategy → Round-Robin**
7. Enter **dest → "67.148.000.001 67.148.000.002"**
8. Enter **done**
9. Enter **exit**

6.10.4. Inside Session Agent Group

The inside session-agent group will allow calls to round-robin between the CLAN and PROCR interfaces. If you only have one location to forward call traffic to, you do not need a SAG. This will be applied to the local policy in **section 6.11**.

1. Enter **session-router → session-group**
2. Enter **group-name → Inside_group**
3. Enter **description → Inside_group**
4. Enter **state →enabled**

5. Enter **app-protocol → SIP**
6. Enter **strategy → Round-Robin**
7. Enter **dest → "10.80.140.200 10.80.140.221"**
8. Enter **done**
9. Enter **exit**

6.11. Local Policies

Local policies allow SIP requests from the **Inside** realm to be routed to the service provider session agent in the **Outside** realm, and vice-versa.

6.11.1. Inside to Outside

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

1. Enter **session-router → local-policy**
2. Enter **from-address → ***
3. Enter **to-address → ***
4. Enter **source-realm → Inside**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → SAG:Outside_group (Defined above in section 6.10.3)**
    b. Enter **realm → Outside**
    c. Enter **app-protocol → SIP**
    d. Enter **state → enabled**
    e. Enter **done**
    f. Enter **exit**
7. Enter **done**
8. Enter **exit**

6.11.2. Outside to Inside

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

1. Enter **session-router → local-policy**
2. Enter **from-address → ***
3. Enter **to-address → ***
4. Enter **source-realm → Outside**
5. Enter **state → enabled**
6. Enter **policy-attributes**
    a. Enter **next-hop → SAG:Inside_Group (Defined above in section 6.10.4)**
    b. Enter **realm → Inside**
    c. Enter **app-protocol → SIP**
    d. Enter **state → enabled**
    e. Enter **done**
    f. Enter **exit**
7. Enter **done**
8. Enter **exit**

6.12. SIP Header Manipulations

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

ACME PACKET 4250 to Communication Manager:

- NatIp –SIP header manipulation rule (HMR) on P-Asserted-Identity for traffic to Communication Manager that changes the Service Provider IP address in the URI-HOST to the domain of **qwest.com**. This domain was added to Communication Manager signaling groups created in **Section 5.6.**

ACME PACKET 4250 to Service Provider

- NatIpOutside – A SIP HMR on traffic from Communication Manager to the Service Provider that changes the URI-HOST from **qwest.com** to the Remote IP address and also changes the REFER from **qwest.com** to the remote IP address.
- Fix302 – SIP HMR that takes a 302 message (Moved Temporarily) and changes it into an INVITE to the Service Provider to the new location. This rule is necessary for any vectors that re-direct inbound calls pre-answer, as covered in **Section 5.9.1**.

6.12.1. Acme Packet 4250 to Communication Manager

The following SIP HMR is applied from traffic coming from the Acme Packet 4250 to Communication Manager. We are modifying the URI-HOST in the P-Asserted Identity Header from an IP Address to the domain of qwest.com to match the signaling group created in **Section 5.6**.

Before Change:

```
⊟ P-Asserted-Identity: "AVAYA INC      " <sip:303   1910@67.148.    :5060>
    SIP Display info: "AVAYA INC      "
  ⊟ SIP PAI Address: sip:303   1910@67.148.    :5060
      SIP PAI User Part: 303   .1910
      SIP PAI Host Part: 67.148.
      SIP PAI Host Port: 5060
```

After Change:

```
⊟ P-Asserted-Identity: "AVAYA INC      " <sip:303    .910@qwest.com:5060>
    SIP Display info: "AVAYA INC      "
  ⊟ SIP PAI Address: sip:303   1910@qwest.com:5060
      SIP PAI User Part: 303   1910
      SIP PAI Host Part: qwest.com
      SIP PAI Host Port: 5060
```

6.12.1.1 Change PAI from IP Address to Domain

To create this SIP HMR:

1. Enter **session-router → sip-manipulation**
2. Enter **name → NatIp**
3. Enter **header-rule**
4. Enter **name → natPAI**

5. Enter **header-name → P-Asserted-Identity**
6. Enter **action → manipulate**
7. Enter **comparison-type → case-sensitive**
8. Enter **msg-type → request**
9. Enter **methods → ACK, BYE,CANCEL,INVITE,REFER**
10. Enter **element-rule**
    a. Enter **name → natPAIhost**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **new-value→qwest.com**
    g. Enter **done**
    h. Enter **exit**
11. Enter **done**
12. Enter **exit**

6.12.2. Acme Packet 4250 to Service Provider

The following set of SIP HMRs are applied to traffic from the Acme Packet 4250 to the Qwest iQ® SIP Trunk gateway. Communication Manager is sending outbound calls with a domain of qwest.com since that is what is listed on the signaling group form, and that needs to be changed to an IP address.

6.12.2.1 Change URI to IP Address

To create this set of SIP HMRs:

1. Enter **session-router → sip-manipulation**
2. Enter **name → NatIpOutside**
3. Enter **header-rule**
4. Enter **name → natUri**
5. Enter **header-name → request-uri**
6. Enter **action → manipulate**
7. Enter **comparison-type → case-sensitive**
8. Enter **msg-type → any**
9. Enter **methods →ACK,BYE,CANCEL,INVITE,REFER**
10. Enter **element-rule**
    a. Enter **name → natUriHost**
    b. Enter **type → uri-host**
    c. Enter **action → replace**
    d. Enter **match-val-type → any**
    e. Enter **comparison-type → case-sensitive**
    f. Enter **match-value →qwest.com**
    g. Enter **new-value→$REMOTE_IP**
    h. Enter **done**
    i. Enter exit
11. Enter **done**

12. Enter **exit**

6.12.2.2 Change 302 Messages to Invites

This rule will take a "302 Temporarily Moved" message and automatically turn it into an INVITE. This will allow redirection of an incoming call that has not been answered to be forwarded to another PSTN location. This is done with a vector using the **~r** redirect listed in **Section 5.9.1**.

1. Enter **session-router → sip-manipulation**
2. Enter **name → Fix302**
3. Enter **header-rule**
4. Enter **name → mod302**
5. Enter **header-name → Contact**
6. Enter **action → manipulate**
7. Enter **comparison-type → case-sensitive**
8. Enter **msg-type → reply**
9. Enter **methods → INVITE**
10. Enter **element-rule**
    i. Enter **name → replaceName**
    j. Enter **type → uri-host**
    k. Enter **action → find-replace-all**
    l. Enter **match-val-type → any**
    m. Enter **comparison-type → case-sensitive**
    n. Enter **match-value →qwest.com**
    o. Enter **new-value→$LOCAL_IP**
    p. Enter **done**
    q. Enter **exit**
11. Enter **done**
12. Enter **exit**

7. Qwest iQ SIP Trunk Configuration

To use the Qwest iQ SIP Trunk Service, a customer must request service. The process can be started by accessing the corporate web site at www.qwest.com and requesting information via the online sales links or telephone numbers.

8. Verification Steps

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

8.1. Acme Packet 4250 Verification

This section illustrates verifications using the Acme Packet 4250 CLI and Wireshark to illustrate key SIP messaging.

8.1.1. Acme Packet 4250 show commands

Verify the version on the system:

```
ACME_SP# show version
ACME PACKET 4250Net-Net 4250 Firmware SC6.2.0 MR-6 GA (Build 832)
Build Date=04/07/11
```

Verify licensing:

```
ACME_SP# show features
Total session capacity: 250
Enabled features:
        250 sessions, SIP, H323, ACP, Routing, Load Balancing,
        High Availability, PAC
```

Verify the Interfaces:

```
ACME_SP# show virtual-interfaces
intf phy-name vlan  ip-addr          realm     type
0/0  s0p0     0     205.168.000.000  Outside   sip-port
1/0  s1p0     0     10.80.140.254    Inside    sip-port
```

Verify Routes:

```
ACME_SP# show routes
Destination/Pfx    Gateway         Flags    RefCnt Use     Proto Tos I/f

0.0.0.0/0          10.80.140.1       2010003  0      0           1   0 sp0
10.80.140.0/24     10.80.140.254     2000101  4      0           2   0 sp0
127.0.0.1          127.0.0.1         2200005  101    11226       2   0 lo0
135.000.000.000/16 135.000.000.000   2000101  3      0           2   0 wancom0
10.80.140.200        10.80.140.2     2000017  0      0           4   0 sp0
10.80.140.221        10.80.140.2     2000017  0      0           4   0 sp0
```

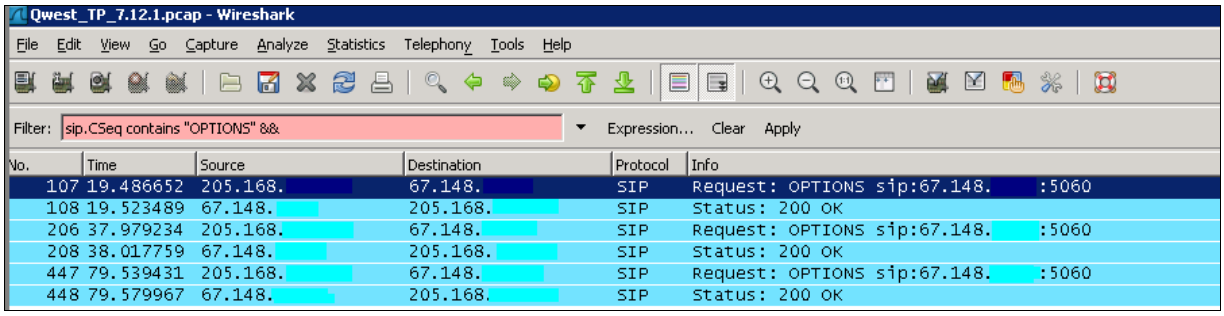
Verify alarms:

```
ACME_SP# display-alarms
2 alarms to show
ID      Task    Severity        First Occurred          Last Occurred
131091  467079408       4       2011-05-10 14:34:11     2011-05-10 14:34:11
Count   Description
1       Slot 0 Port 0 DOWN

131101  467079408       4       2011-05-10 14:34:17     2011-05-10 14:34:17
Count   Description
1       health score is at 50 (under threshold of 60)
```

8.1.2. Verify Acme Packet 4250 Connectivity to Qwest SIP Trunk

Verify that your SIP trunks from the Acme Packet 4250 (205.1.1.112) to Qwest SIP Trunk service (67.148.x.x) are up and communicating with SIP OPTION messages and 200 OK responses.



8.1.3. Verify Acme Packet 4250 Connectivity to Communication Manager

Verify that your signaling group / trunk group between the Communication Manager and the Acme Packet 4250 are up by using **status signaling group #** and **status trunk-group #.**

```
status signaling-group 4
                        STATUS SIGNALING GROUP
        Group ID: 1
      Group Type: sip
     Group State: in-service
```

```
status trunk 4                                                    Page   1
                            TRUNK GROUP STATUS
Member    Port      Service State      Mtce Connected Ports
                                       Busy
0001/001 T00001    in-service/idle    no
0001/002 T00002    in-service/idle    no
```

8.2. Communication Manager Verifications

8.2.1. Example Incoming Call from PSTN via Qwest SIP Trunk

DID and incoming toll-free calls arrive from Qwest SIP Trunk service at the Acme Packet 4250, which sends the call to Communication Manager in a round-robin between trunks 4 and 5, and signaling groups 4 and 5, respectively.

The following abridged Communication Manager "list trace" trace output shows a call incoming on trunk group 5. The PSTN telephone dialed 303-555-7691. The "***incoming-call-handling-trmt trunk-group 5***" form maps the incoming number to an extension of a Communication Manager telephone (x7691). Extension 7691 is an IP Telephone with IP Address 10.80.140.53 in Region 1. Initially, the G650 Media Gateway MedPro (10.80.140.222) is used, but as can be seen in the final trace output, once the call is answered the final RTP media path is "ip-direct" from the IP Telephone (10.80.140.53) to the "inside" of the Acme Packet 4250(10.80.140.254).

NOTE: In Communication Manager Release 6, the tracing prints the Communication Manager Release version at the start of the trace, and intersperses the SIP messaging with the Communication Manager processing.

```
list trace tac *109                                                    Page   1
                                LIST TRACE
time            data
15:27:27 TRACE STARTED 05/20/2011 CM Release String cold-00.1.510.1-defsw1107371
15:27:47 SIP<INVITE sip:3035557691@10.80.140.200:5060 SIP/2.0
15:27:47     active trunk-group 5 member 1  cid 0x5a
15:27:47 SIP>SIP/2.0 180 Ringing
15:27:47     dial 7691
15:27:47     ring station    7691 cid 0x5a
15:27:47     G711MU ss:off ps:20
             rgn:1 [10.80.140.53]:2662
             rgn:1 [10.80.140.222]:3048
15:27:47     G711MU ss:off ps:20
             rgn:1 [10.80.140.254]:16454
             rgn:1 [10.80.140.222]:3032
15:27:47     xoip options: fax:T38 modem:off tty:US  uid:0x5021d
             xoip ip: [10.80.140.222]:3032
15:27:47 SIP<PRACK sip:10.80.140.200;transport=tcp SIP/2.0
15:27:47 SIP>SIP/2.0 200 OK
15:27:51 SIP>SIP/2.0 200 OK
15:27:51     active station    7691 cid 0x5a
15:27:51 SIP<ACK sip:10.80.140.200;transport=tcp SIP/2.0
15:27:51 SIP>INVITE sip:3035551910@10.80.140.254:5060;transport=
15:27:51 SIP>tcp SIP/2.0
15:27:51 SIP<SIP/2.0 100 Trying
15:27:51 SIP<SIP/2.0 200 OK
15:27:51 SIP>ACK sip:3035551910@10.80.140.254:5060;transport=tcp
15:27:51 SIP> SIP/2.0
15:27:51     G711MU ss:off ps:20
             rgn:1 [10.80.140.254]:16454
             rgn:1 [10.80.140.53]:2662
15:27:51     G711MU ss:off ps:20
             rgn:1 [10.80.140.53]:2662
             rgn:1 [10.80.140.254]:16454
15:29:19 SIP<BYE sip:10.80.140.200;transport=tcp SIP/2.0
15:29:19 SIP>SIP/2.0 200 OK
15:29:19     idle trunk-group 5 member 1  cid 0x5a
```

The following screen shows **Page 2** of the output of the command "***status trunk 5/1***" (Trunk 5, Member 1. One of the active call endpoints) command pertaining to the same call. Note the signaling using port 5060 between Communication Manager and the Acme packet 4250. Note the media is "ip-direct" from the IP Telephone (10.80.140.53) to the inside IP Address of the Acme Packet 4250(10.80.140.254) using G.711MU.

```
status trunk 5/1                                                Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                                Port
   Near-end:  10.80.140.200                             : 5060
    Far-end:  10.80.140.254                           : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:           H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                          Codec Type: G.711MU
   Audio      IP Address                                Port
   Near-end:  10.80.140.53                           : 2662
    Far-end:  10.80.140.254                          : 16454
```

```
status trunk 5/1                                                Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00541
T00541:TX:10.80.140.254:16454/g711u/20ms
S00012:RX:10.80.140.53:2662/g711u/20ms
```

1. Verify your communication from the Acme Packet 4250 (205.1.1.112) to Qwest SIP Trunk service (67.148.000.000) are up and communicating with SIP OPTION messages and 200 OK responses **Section 8.1.2**.
2. Verify that your signaling group / trunk group between the Communication Manager and Acme Packet 4250 are up by using ***status signaling group*** # and ***status trunk-group*** # **Section 8.1.3**.
3. 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.
4. 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.
5. Verify that the user on the PSTN can end an active call by hanging up.
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.

8.3. Troubleshooting:

1. Communication Manager:
   - **list trace station** <extension number> - Traces calls to and from a specific station.
   - **list trace tac** <trunk access code number> - Traces calls over a specific trunk group.
   - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
   - **status trunk** <trunk access code number> - Displays trunk group information.
   - **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.
2. ACME PACKET 4250
   - **show running-config –** Displays the current config

- **show prom-info all** – Displays the all prom information including serial number, hardware revision, manufacturing date, part numbers and more
- **show sipd sessions all** – Will display all of the active SIP sessions that are currently traversing the SBC, including the To, From, Call-ID.
- **show support-info -** Outputs all of the system level info, including hardware specifics, licensing info, current call volume, etc.
- **show health -** For a redundant system will give a status of synchronized processes and an overview of failover history
- **show sipd invite -** Will display a chart of all recent SIP requests and responses
- **display-alarms -** Alarm log output of recent and current alarms
- **show logfile sipmsg.log -** Will output the contents of the sipmsg.log without having to FTP this file off the SBC

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and an Acme Packet 4250 to Qwest SIP Trunk service. Qwest SIP Trunk service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Qwest SIP Trunk service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Qwest SIP Trunk service passed compliance testing. Please refer to **Section 2.3** for any exceptions or workarounds.

10. References

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

[1] *Administering Avaya Aura® Communication Manager*, May 2009, Document Number 03-300509.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* May 2009, *D*ocument Number 555-245-205.

[3]

[4] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x,* February 2010, Document Number 16-601443.

[5] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.

[6] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.

[7] *Avaya one-X® Communicator Getting Started, November 2009.*

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

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

[10] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

[11] Acme Packet Support (login required): http://www.acmepacket.com/support.htm

Appendix A: Acme Packet 4250 Configuration File

```
ACME_SP# show config
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        Inside
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 14:06:04
        policy-attribute
                next-hop                        SAG:Outside_group
                realm                           Outside
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol                    SIP
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        Outside
        description
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 13:58:38
        policy-attribute
                next-hop                        SAG:Inside_group
                realm                           Inside
                action                          none
```

```
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol                   SIP
                state                          enabled
                methods
                media-profiles
                lookup                         single
                next-key
                eloc-str-lkup                  disabled
                eloc-str-match

media-manager
        state                           enabled
        latching                        enabled
        flow-time-limit                 86400
        initial-guard-timer             300
        subsq-guard-timer               300
        tcp-flow-time-limit             86400
        tcp-initial-guard-timer         300
        tcp-subsq-guard-timer           300
        tcp-number-of-ports-per-flow    2
        hnt-rtcp                        disabled
        algd-log-level                  NOTICE
        mbcd-log-level                  NOTICE
        red-flow-port                   1985
        red-mgcp-port                   1986
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        media-policing                  enabled
        max-signaling-bandwidth         10000000
        max-untrusted-signaling         100
        min-untrusted-signaling         30
        app-signaling-bandwidth         0
        tolerance-window                30
        rtcp-rate-limit                 0
        trap-on-demote-to-deny          enabled
        min-media-allocation            32000
        min-trusted-allocation          1000
        deny-allocation                 1000
        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@console
        last-modified-date              2011-04-13 09:11:58
network-interface
```

```
        name                            s0p0
        sub-port-id                     0
        description                     ToServiceProvider
        hostname
        ip-address                      205.168.000.000
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         205.168.000.000
        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
        ftp-address
        icmp-address
        snmp-address
        telnet-address
        ssh-address
        last-modified-by
        last-modified-date              2011-04-11 14:01:15
network-interface
        name                            s1p0
        sub-port-id                     0
        description                     ToAvaya
        hostname
        ip-address                      10.80.140.254
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.0
        gateway                         10.80.140.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     10.80.140.254
        ftp-address
        icmp-address                    10.80.140.254
        snmp-address
        telnet-address
```

```
        ssh-address
        last-modified-by
        last-modified-date              2011-04-12 10:13:49
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
        last-modified-date              2011-04-11 12:09:48
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
        last-modified-date              2011-04-11 12:10:57
phy-interface
        name                            wancom0
        operation-type                  Control
        port                            0
        slot                            2
        virtual-mac
        wancom-health-score             50
        overload-protection             disabled
        last-modified-by
        last-modified-date              2011-04-12 10:40:07
realm-config
        identifier                      Outside
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        s0p0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        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
in-translationid
out-translationid
in-manipulationid
out-manipulationid            NatIpOutside
manipulation-string
manipulation-pattern
class-profile
average-rate-limit            0
access-control-trust-level    none
invalid-signal-threshold      0
maximum-signal-threshold      0
untrusted-signal-threshold    0
nat-trust-threshold           0
deny-period                   30
ext-policy-svr
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
dyn-refer-term                disabled
codec-policy
codec-manip-in-realm          disabled
constraint-name
call-recording-server-id
stun-enable                   disabled
stun-server-ip                0.0.0.0
stun-server-port              3478
stun-changed-ip               0.0.0.0
stun-changed-port             3479
match-media-profiles
qos-constraint
sip-profile
sip-isup-profile
block-rtcp                    disabled
```

```
        hide-egress-media-update       disabled
        last-modified-by               admin@10.80.140.50
        last-modified-date             2011-04-28 10:00:07
realm-config
        identifier                     Inside
        description
        addr-prefix                    0.0.0.0
        network-interfaces
                                       s1p0:0
        mm-in-realm                    enabled
        mm-in-network                  enabled
        mm-same-ip                     enabled
        mm-in-system                   enabled
        bw-cac-non-mm                  disabled
        msm-release                    disabled
        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
        in-translationid
        out-translationid
        in-manipulationid              Fix302
        out-manipulationid             NatIp
        manipulation-string
        manipulation-pattern
        class-profile
        average-rate-limit             0
        access-control-trust-level     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        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
        dyn-refer-term                  disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        sip-profile
        sip-isup-profile
        block-rtcp                      disabled
        hide-egress-media-update        disabled
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-28 17:01:59
session-agent
        hostname                        67.148.000.001
        ip-address                      67.148.000.001
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        Outside
        egress-realm-id
        description                     East
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
```

```
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=70
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        enabled
        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                 100
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 11:53:01


session-agent
        hostname                        10.80.140.221
        ip-address                      10.80.140.221
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP+TCP
        realm-id                        Inside
        egress-realm-id
        description                     clan
        carriers
```

```
allow-next-hop-lp              enabled
constraints                    disabled
max-sessions                   0
max-inbound-sessions           0
max-outbound-sessions          0
max-burst-rate                 0
max-inbound-burst-rate         0
max-outbound-burst-rate        0
max-sustain-rate               0
max-inbound-sustain-rate       0
max-outbound-sustain-rate      0
min-seizures                   5
min-asr                        0
time-to-resume                 0
ttr-no-response                0
in-service-period              0
burst-rate-window              0
sustain-rate-window            0
req-uri-carrier-mode           None
proxy-mode
redirect-action
loose-routing                  enabled
send-media-session             enabled
response-map
ping-method                    OPTIONS;hops=70
ping-interval                  60
ping-send-mode                 keep-alive
ping-all-addresses             disabled
ping-in-service-response-codes
out-service-response-codes
media-profiles
in-translationid
out-translationid
trust-me                       enabled
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                100
codec-policy
enforcement-profile
refer-call-transfer            disabled
reuse-connections              NONE
tcp-keepalive                  none
```

```
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 14:10:02

session-agent
        hostname                        67.148.000.002
        ip-address                      67.148.000.002
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        Outside
        egress-realm-id
        description                     West
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=70
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-all-addresses              disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
```

```
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        sip-profile
        sip-isup-profile
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-28 10:16:10

session-agent
        hostname                        10.80.140.200
        ip-address                      10.80.140.200
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP+TCP
        realm-id                        Inside
        egress-realm-id
        description                     procr
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
```

```
        burst-rate-window              0
        sustain-rate-window            0
        req-uri-carrier-mode           None
        proxy-mode
        redirect-action
        loose-routing                  enabled
        send-media-session             enabled
        response-map
        ping-method                    OPTIONS;hops=70
        ping-interval                  60
        ping-send-mode                 keep-alive
        ping-all-addresses             disabled
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                       disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                    disabled
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        p-asserted-id
        trunk-group
        max-register-sustain-rate      0
        early-media-allow
        invalidate-registrations       disabled
        rfc2833-mode                   none
        rfc2833-payload                0
        codec-policy
        enforcement-profile
        refer-call-transfer            disabled
        reuse-connections              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        sip-profile
        sip-isup-profile
        last-modified-by               admin@10.80.140.50
        last-modified-date             2011-04-27 14:10:18

session-group
        group-name                     Outside_group
        description                    Outside_gr
        state                          enabled
        app-protocol                   SIP
        strategy                       RoundRobin
        dest
                                       67.148.000.001
```

```
                                        67.148.000.002
        trunk-group
        sag-recursion                   disabled
        stop-sag-recurse                401,407
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-29 09:41:42

session-group
        group-name                      Inside_group
        description                     Inside_gr
        state                           enabled
        app-protocol                    SIP
        strategy                        RoundRobin
        dest
                                        10.80.140.200
                                        10.80.140.221
        trunk-group
        sag-recursion                   disabled
        stop-sag-recurse                401,407
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 14:11:57

sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             enabled
        home-realm-id                   Inside
        egress-realm-id                 Inside
        nat-mode                        None
        registrar-domain
        registrar-host
        registrar-port                  5060
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        add-reason-header               disabled
        sip-message-len                 0
        enum-sag-match                  disabled
        extra-method-stats              disabled
        registration-cache-limit        0
```

```
        register-use-to-for-lp         disabled
        options                        max-udp-length=0
        refer-src-routing              disabled
        add-ucid-header                disabled
        proxy-sub-events
        pass-gruu-contact              disabled
        sag-lookup-on-redirect         disabled
        set-disconnect-time-on-bye     disabled
        last-modified-by               admin@10.80.140.50
        last-modified-date             2011-04-27 11:31:00
sip-interface
        state                          enabled
        realm-id                       Inside
        description
        sip-port
                address                        10.80.140.254
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
```

```
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
        rfc2833-payload                100
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by               admin@10.80.140.50
        last-modified-date             2011-04-27 11:31:23
sip-interface
        state                          enabled
        realm-id                       Outside
        description
        sip-port
                address                        205.168.000.000
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
```

```
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        manipulation-pattern
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode  pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
        implicit-service-route          disabled
        rfc2833-payload                 100
        rfc2833-mode                    transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                 disabled
        enforcement-profile
        route-unauthorized-calls
        tcp-keepalive                   none
        add-sdp-invite                  disabled
        add-sdp-profiles
        sip-profile
        sip-isup-profile
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 11:31:38
sip-manipulation
        name                            NatIp
        description
        split-headers
        join-headers
        header-rule
                name                            natPAI
                header-name                     P-Asserted-Identity
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        request
                methods                         ACK,BYE,CANCEL,INVITE,REFER
                match-value
                new-value
                element-rule
                        name                            natPAIhost
```

```
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       qwest.com
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-28 09:34:30
sip-manipulation
        name                            NatIpOutside
        description
        split-headers
        join-headers
        header-rule
                name                            natURI
                header-name                     request-uri
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        any
                methods                         ACK,BYE,CANCEL,INVITE,REFER
                match-value
                new-value
                element-rule
                        name                            natUriHost
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value                     qwest.com
                        new-value                       $REMOTE_IP
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-28 17:01:32

sip-manipulation
        name                            Fix302
        description
        split-headers
        join-headers
        header-rule
                name                            mod302
                header-name                     Contact
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        reply
                methods                         INVITE
                match-value
                new-value
                element-rule
                        name                            replaceName
                        parameter-name
                        type                            uri-host
                        action                          find-replace-all
                        match-val-type                  any
                        comparison-type                 case-sensitive
```

```
                        match-value                     qwest.com
                        new-value                       $LOCAL_IP
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-28 16:57:06
steering-pool
        ip-address                      205.168.000.000
        start-port                      8000
        end-port                        39998
        realm-id                        Outside
        network-interface
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 11:32:20
steering-pool
        ip-address                      10.80.140.254
        start-port                      2048
        end-port                        8001
        realm-id                        Inside
        network-interface
        last-modified-by                admin@10.80.140.50
        last-modified-date              2011-04-27 11:33:44
system-config
        hostname                        ACME
        description                     ACME_to_Qwest
        location
        mib-system-contact
        mib-system-name                 ACME_to_Qwest
        mib-system-location
        snmp-enabled                    enabled
        enable-snmp-auth-traps          enabled
        enable-snmp-syslog-notify       enabled
        enable-snmp-monitor-traps       enabled
        enable-env-monitor-traps        disabled
        snmp-syslog-his-table-length    1
        snmp-syslog-level               DEBUG
        system-log-level                DEBUG
        syslog-server
                address                         10.80.140.50
                port                            514
                facility                        4
        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                  disabled
        log-filter                      all
```

```
default-gateway                 10.80.140.1
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                        enabled
terminal-height                 24
debug-timeout                   0
trap-event-lifetime             0
cleanup-time-of-day             00:00
last-modified-by                admin@10.80.140.50
last-modified-date              2011-04-27 13:34:23
```

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.