Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Border Controller with Qwest iQ® SIP Trunk (version 6.5) – 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) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Session Border Controller 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 Avaya Aura® Session Border Controller integration with Qwest iQ® SIP Trunk (version 6.5).

In the sample configuration, the Session Border Controller is used as an edge device between Avaya Communication Manager and Qwest-SIP Trunk. The Session Border Controller performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private IP addressing to IP addressing appropriate for the Qwest-SIP Trunk access method.

The Communication Manager and Session Border Controller are directly connected with a Communication Manager SIP trunk, Avaya Modular Messaging is also connected to the Communication Manager through a SIP trunk.

Qwest SIP Trunk 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 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 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.

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the Qwest SIP Trunking 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 Avaya Aura® Session Border Controller, 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 Session Border Controller, and subsequent redirection of inbound calls to Qwest-SIP Trunk.

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types.
  Phone types included H.323, digital, and analog telephones at the enterprise. Inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider. No SIP phones were tested because there was no SIP registrar in the configuration.

- 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

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™

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

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 a phone number and click "Speak to us now" and Customer Service will call the entered number, 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) 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 service provider 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 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 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 the Communication Manager to an endpoint and the endpoint wishes to use a different DTMF payload header value then was negotiated when the call was initially established. Qwest SIP Trunk 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, page 4 to 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 will send the call to the Avaya 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 Communication Manager loads: 5.2.1 SP9, 6.0.1 SP3, 6.2. Use of a 503 allows for a back-off time period and a retry by Qwest.

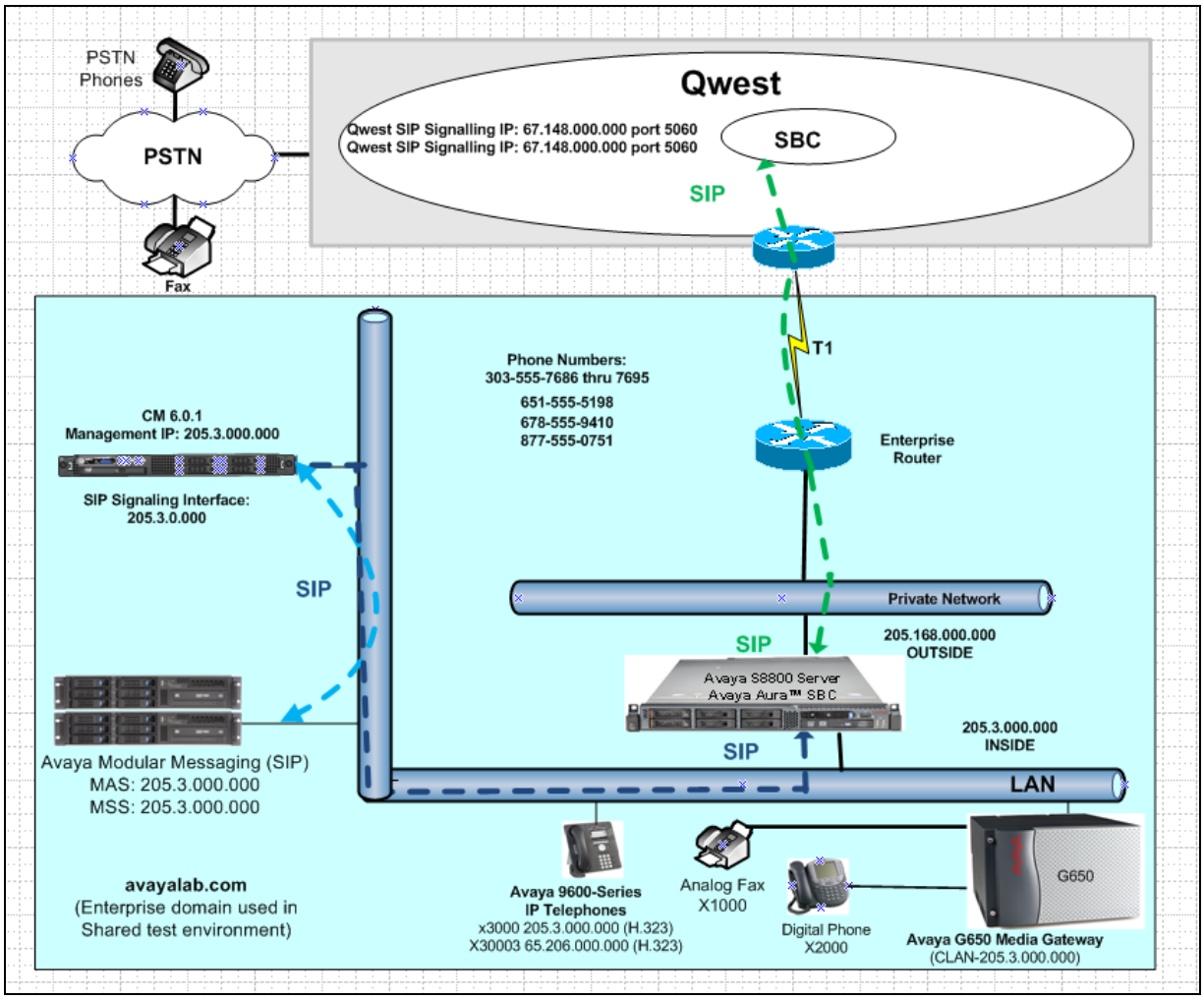
- **SIP Network REFER to an off-net extension is not supported**: When Communication Manager receives a PSTN call and tries to use a vector to automatically re-direct using a SIP REFER to another PSTN extension, the call will drop. Qwest SIP Trunk does not allow re-directs to/from non-Qwest PSTN numbers.

- **SIP REFER with transfer (consultative or blind) is not supported in Qwest iQ® SIP Trunk :** When an extension receives a call from a PSTN number and attempts to transfer (either consultative or blind) the call to another PSTN extension, 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 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 location connected via a T1 Internet connection to the Qwest iQ® SIP Trunk. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, an Avaya Aura® Session Border Controller provides NAT functionality and SIP header manipulation. The Session Border Controller receives traffic from 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

A separate trunk was created between Communication Manager and the Session Border Controller to carry the service provider traffic; this was done so that any trunk or codec setting

required by the service provider could be applied only to this trunk and not affect other enterprise traffic. In addition, this trunk carried both inbound and outbound traffic.

For inbound calls, the calls flow from the service provider to the Session Border Controller then to Communication Manager. 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 may be performed.

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

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
Avaya S8800 Server (Session Border Controller)	Avaya Aura® Session Border Controller Release 6.0 SBC Template SBCT 6.0.0.1.5
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 Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Qwest SIP Trunking. A SIP trunk is established between Communication Manager and the Avaya Aura® Session Border Controller for use by signaling traffic to and from Qwest SIP Trunk. It is

assumed the general installation of Communication Manager and Avaya G650 Media Gateway has been previously completed and is not discussed here.

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

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

          IP Attendant Consoles? 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 was used to refer calls to alternate destinations using SIP NCR (Network Call Redirect). Vector variables were used to include User-User Information (UUI) with the referred calls.

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:

ENBLOC DIALING PARAMETERS
   Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the clan of the Avaya S8510 Server running Communication Manager and for the Session Border Controller. 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
AuraSBC-Inside          205.3.0.1
Gateway1                205.3.0.1
Gateway254              205.3.0.254
MM                      205.3.0.56
MedPro1A03              205.3.0.222
MedPro1A04              205.3.0.223
clan                    205.3.0.221
default                 0.0.0.0
procr                   205.3.0.200
```

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.729A*** and ***G.711MU*** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields. 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.***

```
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

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP-network-region 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 (the service provider region) and region 1 (the enterprise side). Creating this table entry for ip network region 1 will automatically create a complementary table entry on the ip network region 1 form for destination region 1.

```
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 Session Border Controller for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 3 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Set the **Transport Method** to the recommended default value of ***tls*** (Transport Layer Security). 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 Session Border Controller.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). 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***. This node name maps to the IP address of the clan in the G650 gateway as defined in the **node-names ip** screen shot in section 5.3.
- Set the **Far-end Node Name** to ***AuraSBC-inside***. This node name maps to the IP address of the Session Border Controller 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).
- 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.

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

 Group Number: 1              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: AuraSBC-Inside
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                         Far-end Network Region: 1

Far-end Domain: 67.148.000.000
                                              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 group 3 was configured using the parameters highlighted below.

- Set the **Group Type** field to ***sip***.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to ***public-ntwrk***.
- Set **Member Assignment Method** to ***auto***.
- Set the **Signaling Group** to the signaling group 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 1                                            Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC: *101
   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: 1
                                                      Number of Members: 20
```

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 ***900*** seconds was used.

```
change trunk-group 1                                          Page   2 of  21
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto
                                        Redirect On OPTIM Failure: 20000

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

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

On **Page 4**, set the **Network Call Redirection** field to n. Set the **Send Diversion Header** field to ***y***. This field provides 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 1                                          Page   4 of  21
                              PROTOCOL VARIATIONS

                       Mark Users as Phone? y
             Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                  Network Call Redirection? n
                     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 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
   #           3   fac
```

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

```
change feature-access-codes                                    Page   1 of  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
   Call Forwarding Enhanced Status: 112    Act: 113    Deactivation: 114
                        Call Park Access Code: 125
                      Call Pickup Access Code: 126
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
```

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 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
    10xxx011              15   23   deny      intl         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 2 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*** This is the routing preference for **Look Ahead Routing**.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: toAuraSBC
                                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: 1    0       1                                                   n   user
 2: 3    0       1                                                   n   user
 3:                                                                  n   user
 4:                                                                  n   user
 5:                                                                  n   user
 6:                                                                  n   user

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

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. 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 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. In Section 2.3, Test Results / Known Limitations, Qwest SIP Trunk does not support SIP-NCR to an off-net PSTN number and therefore we suggest that **Network Call Redirection** (trunk-group page 4) be turned off to support blind transfers and conference calls. SIP NCR is allowed for internal call redirection to another internal extension and this section is describing how to configure that. However, **Network Call Redirection** would have to be turned on and would then affect call transfers.

5.9.1. 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. A corresponding detailed verification is provided in **Section 8.1**. In this example, the inbound toll-free call is routed to VDN 3999 shown in the following screen. The originally dialed service provider Toll Free number may be mapped to VDN 3999 by the incoming call handling treatment for the inbound trunk group (described in **section 5.10** below).

```
display vdn 3999                                          Page   1 of   3
                          VECTOR DIRECTORY NUMBER

                            Extension: 3999
                                 Name*: Qwest Call Center
                          Destination: Vector Number        2
                  Attendant Vectoring? n
                 Meet-me Conferencing? n
                   Allow VDN Override? n
                                  COR: 1
```

VDN 3999 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 **route-to number** (step 5) includes **~r3036267690** where the number 303-626-7690 is an internal destination. This step causes a REFER message to be sent where the Refer-To header includes **13035557690** 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 #    Refer the call to the PSTN destination
05 route-to     number ~r3035557690     with cov n if unconditionally
06 #    If Refer fails, play announcement and disconnect
07 disconnect   after announcement 3997
```

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 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 **8778620755 to extension 3003**.

```
change inc-call-handling-trmt trunk-group 1                    Page   1 of  30
                     INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    10 8775550755       10  3003
 public-ntwrk    10 3035557686       10  1000
 public-ntwrk    10 3035557687       10  1001
 public-ntwrk    10 3035557688       10  2000
 public-ntwrk    10 3035557689       10  3000
 public-ntwrk    10 3035557690       10  3001
 public-ntwrk    10 3035557691       10  3002
 public-ntwrk    10 3035557692       10  3003
 public-ntwrk    10 3035557693       10  3999
 public-ntwrk    10 3035557694       10  3005
 public-ntwrk    10 6515555198       10  3000
 public-ntwrk    10 6785559410       10  2000
 public-ntwrk    10 8775550751       10  3003
```

5.11. Modular Messaging Hunt Group

Although not specifically related to Qwest SIP Trunk, 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 Avaya Modular Messaging

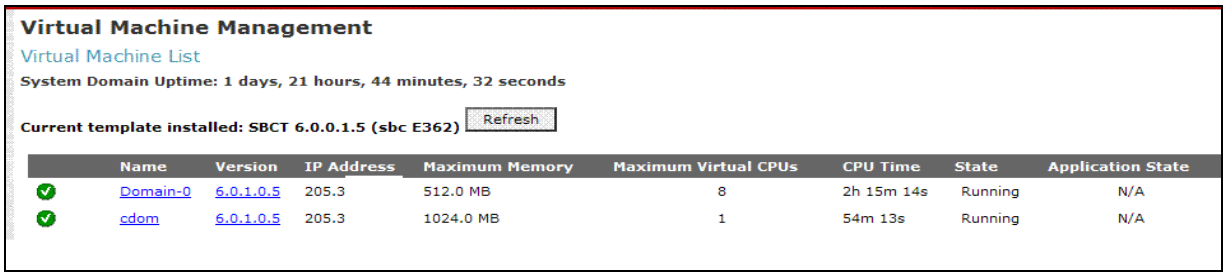
Although not specifically related to Qwest SIP Trunk, this section shows the AAR routing for the number used in the hunt group in the previous section. The bold row shows that calls to the number 7999, which is the Modular Messaging Group Extension for hunt group 99, will use **Route Pattern** 2.

```
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
```

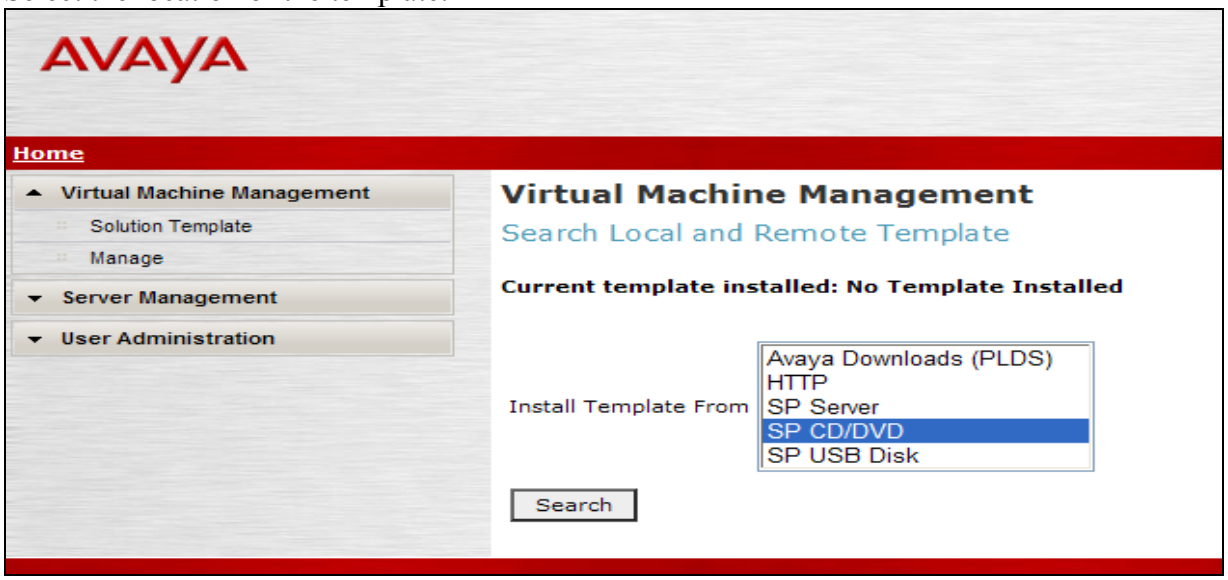
6. Avaya Aura® Session Border Controller Element Manager Configuration

6.1. Initial Installation

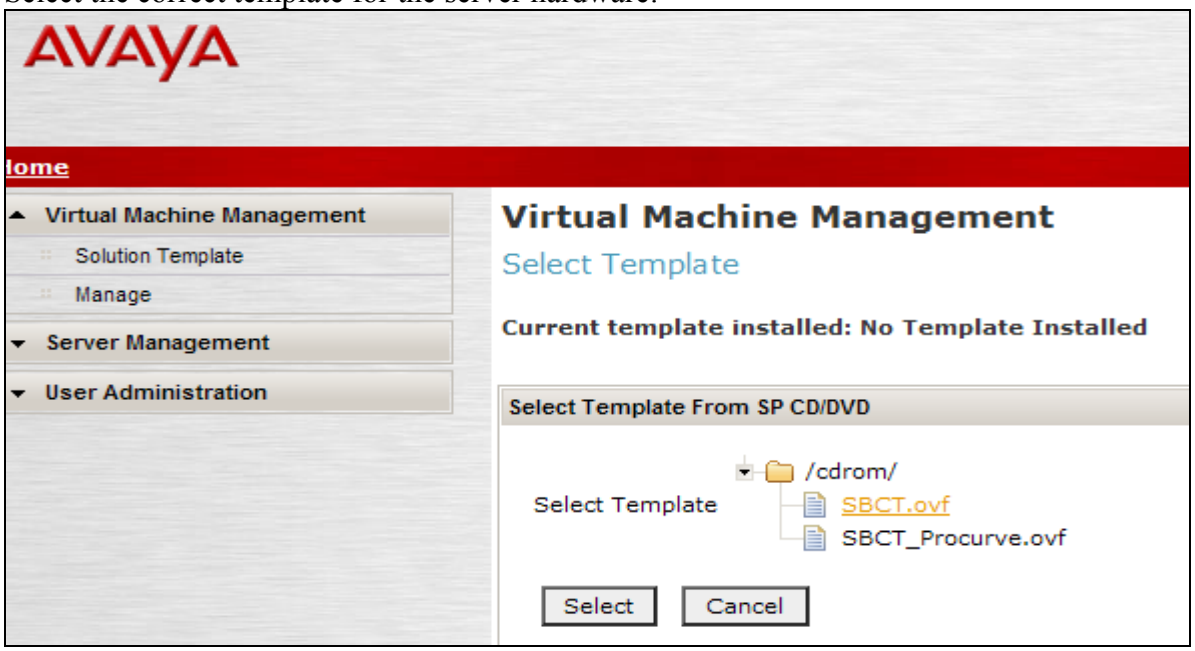
This section displays basic configuration of the Session Border Controller from the installation wizard. The initial configuration was completed by installing the Virtual Server Platform (VSP) 6.0.1.0.5 and then logging into the web interface of the server (cdom) address. This screen will verify the state of the dom-0 and cdom platforms (the State column below) and the Application State of the Session Border Controller after it has been installed.



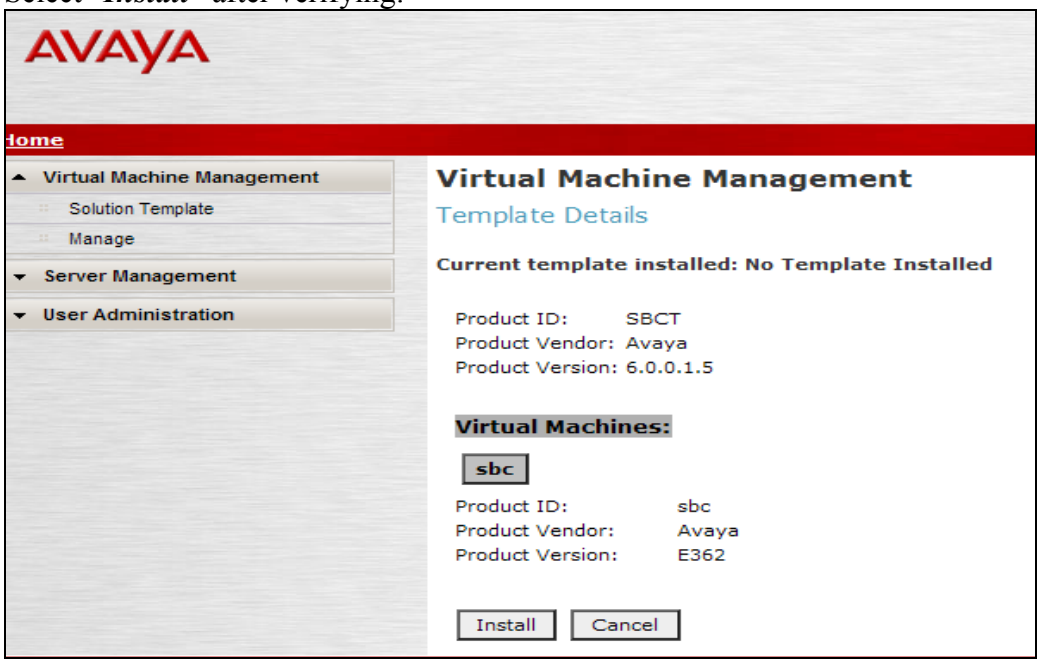
After Installation of VSP is complete open the web interface to the CDOM and go to **Virtual Machine Management→ Solution Template**
Select the location of the template:



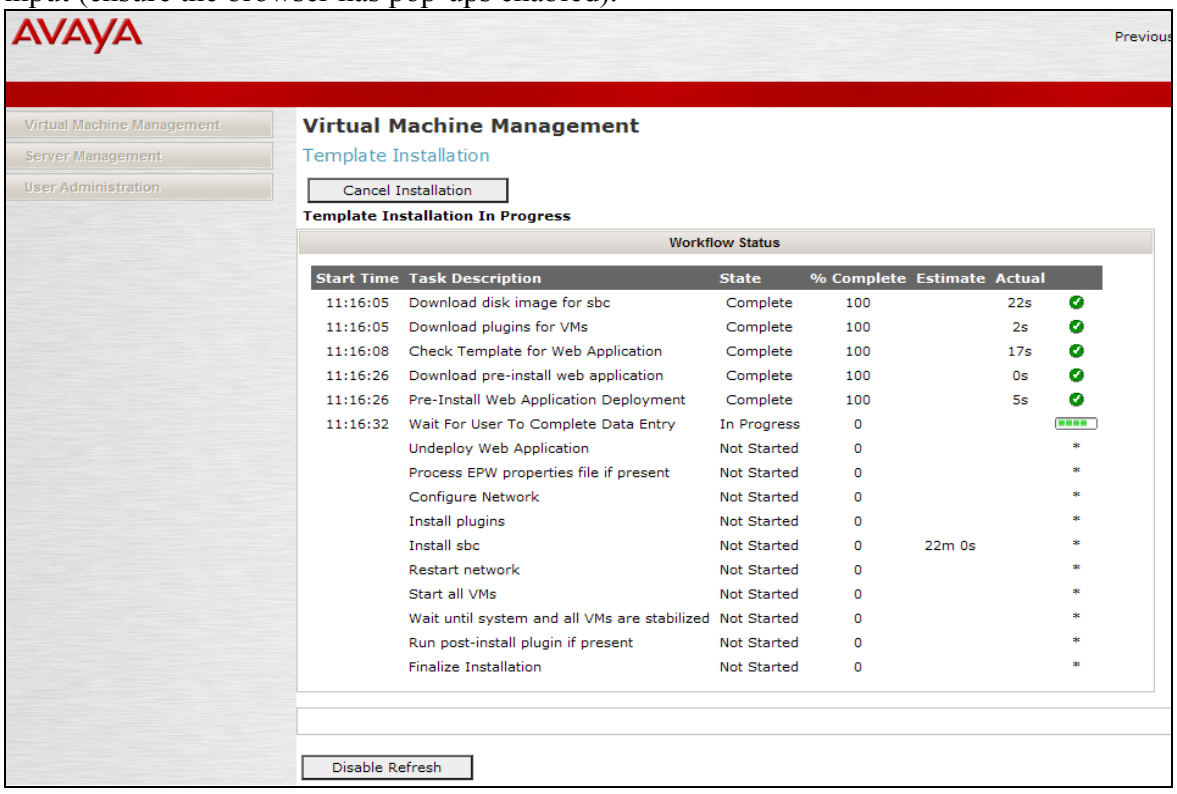
Select the correct template for the server hardware:



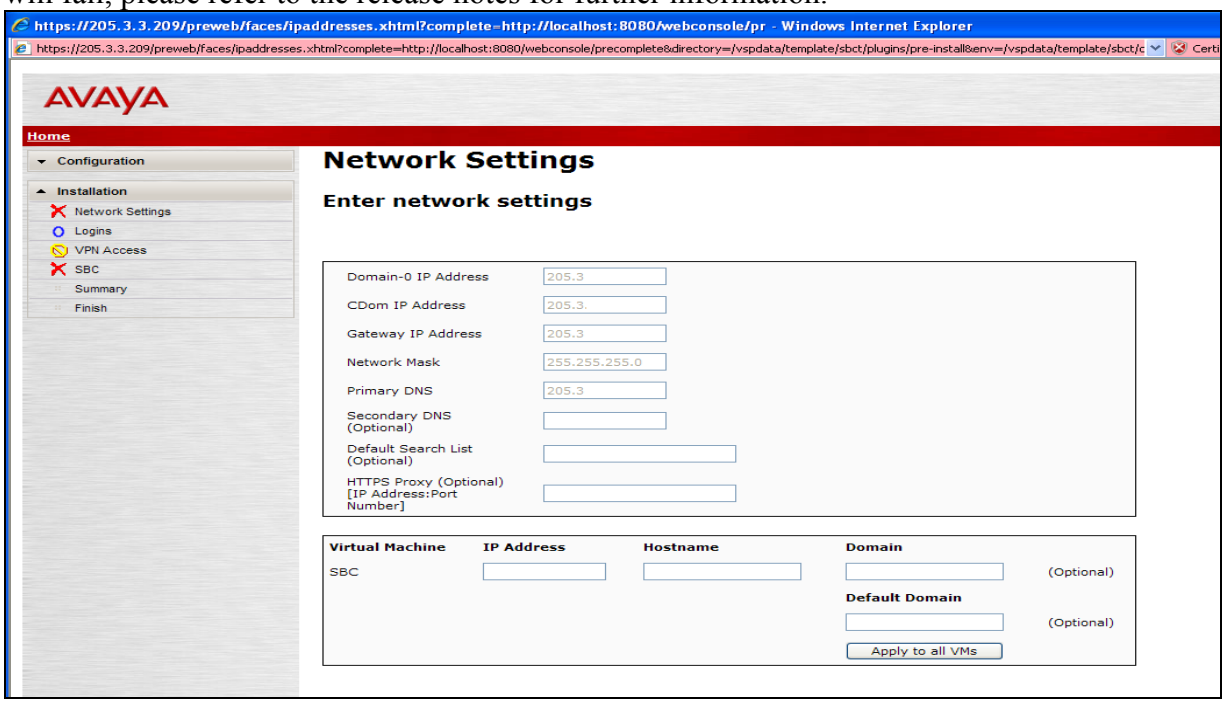
Select "***Install***" after verifying:



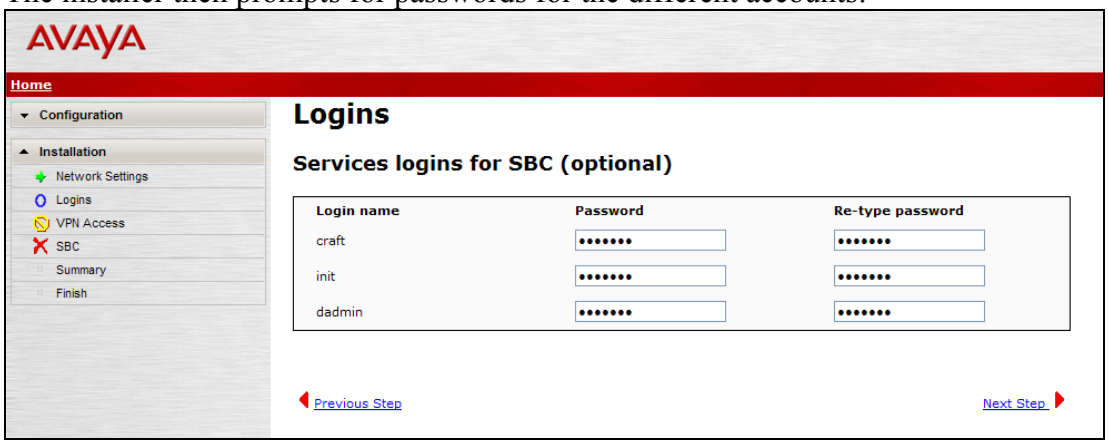
At this point, the installer will open a log that will show the progress of the installation. When the installer gets to "Wait for User to Complete Data Entry", another window will open for input (ensure the browser has pop-ups enabled).



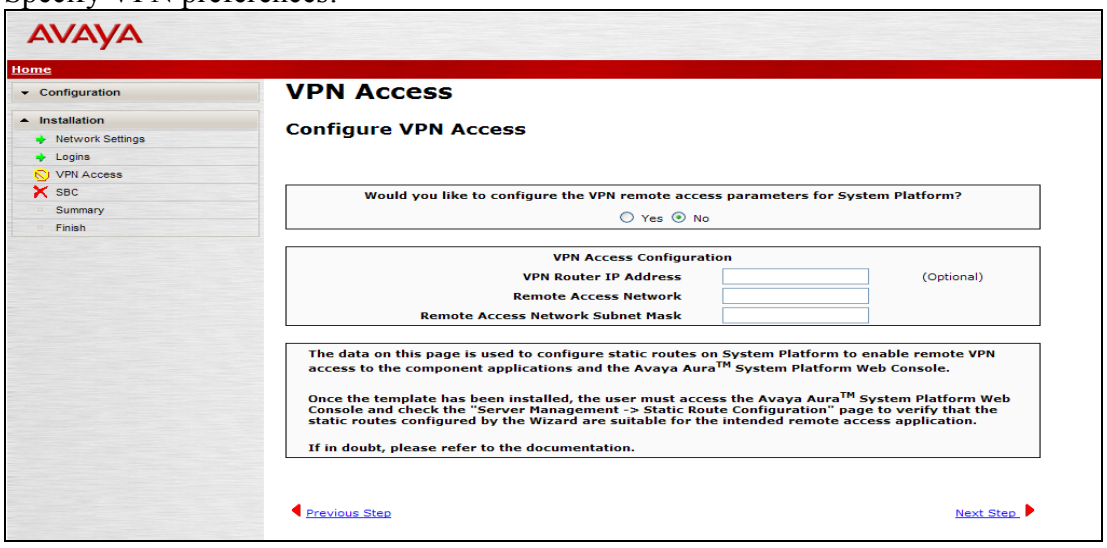
In this version the domain that is listed is **NOT** optional and must be populated or installation will fail, please refer to the release notes for further information.



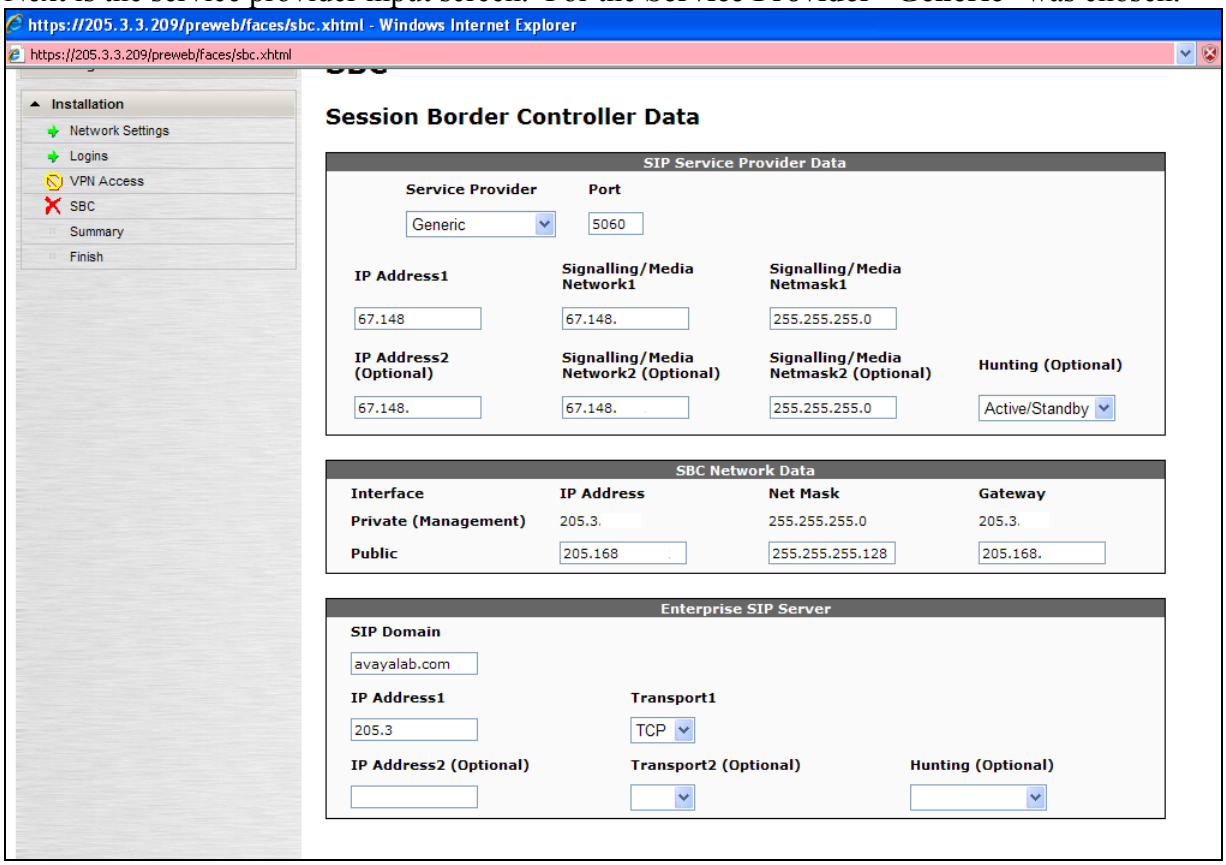
The installer then prompts for passwords for the different accounts:



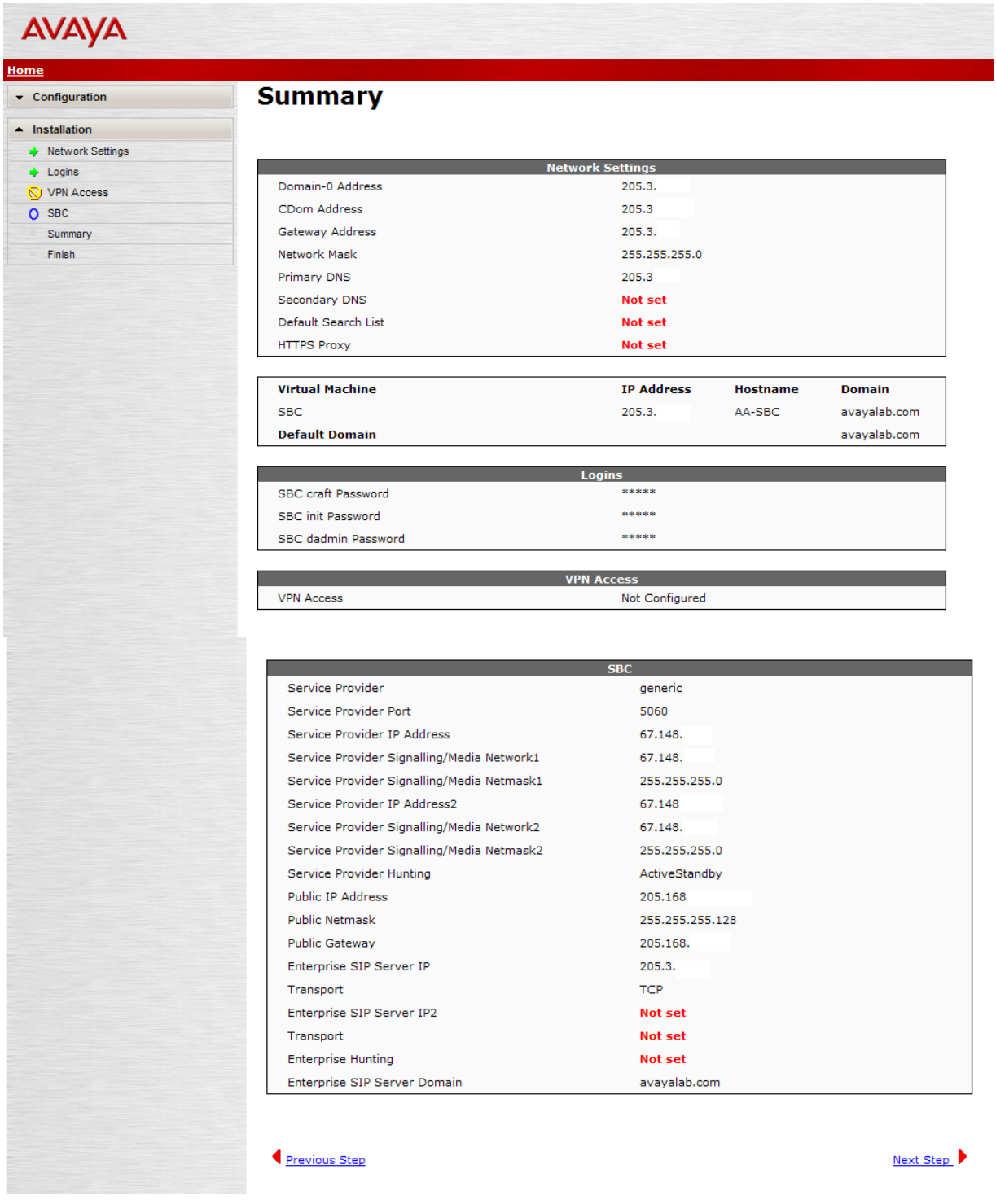
Specify VPN preferences:



Next is the service provider input screen. For the **Service Provider** "**Generic**" was chosen.



A summary of the input is displayed, confirm choices by clicking “Next Step”:



The progress page will re-appear as it continues the installation.

Template Installation

Template Installation Completed Successfully

Workflow Status

Start Time	Task Description	State	% Complete	Estimate	Actual
22:23:29	Download disk image for sbc	Complete	100		11m 20s
22:23:29	Download plugins for VMs	Complete	100		1m 21s
22:24:50	Check Template for Web Application	Complete	100		21s
22:25:12	Download pre-install web application	Complete	100		37s
22:25:50	Pre-Install Web Application Deployment	Complete	100		2s
22:25:52	Wait For User To Complete Data Entry	Complete	100		4m 34s
22:30:27	Undeploy Web Application	Complete	100		1s
22:30:29	Process EPW properties file if present	Complete	100		33s
22:31:03	Configure Network	Complete	100		6s
22:31:09	Install plugins	Complete	100		4s
22:34:50	Install sbc	Complete	100		5m 12s
22:40:02	Restart network	Complete	100		21s
22:40:24	Start all VMs	Complete	100		13s
22:40:37	Wait until system and all VMs are stabilized	Complete	100		41s
22:41:19	Run post-install plugin if present - SBC:Creating SBC Configuration File - SBC:Checking ssh connection to SBC - SBC:Connecting to SBC web service - SBC:Copying configuration file to SBC - SBC:Merging SBC configuration - SBC:Saving SBC configuration file - SBC:Restarting SBC - SBC:Waiting for two minutes - SBC:Checking ssh connection to SBC - SBC:Connecting to SBC web service - SBC:Reading SBC configuration - SBC:Adding user admin - SBC:Adding user cust - SBC:Adding user init - SBC:Adding user craft - SBC:Adding user dadmin - SBC:Loading users - SBC:Saving SBC configuration file - SBC:Restarting SBC - main:**Wizard completed successfully**	Complete	100		3m 10s
22:44:30	Finalize Installation	Complete	100		17s

Once the installation is completed, verify all application statuses:

Virtual Machine Management

Virtual Machine List

System Domain Uptime: 1 days, 21 hours, 44 minutes, 32 seconds

Current template installed: SBCT 6.0.0.1.5 (sbc E362) Refresh

	Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
	Domain-0	6.0.1.0.5	205.3	512.0 MB	8	2h 15m 14s	Running	N/A
	cdom	6.0.1.0.5	205.3	1024.0 MB	1	54m 13s	Running	N/A
	sbc	E362	205.3	4.0 GB	4	4h 40m 49s	Running	Running

Please refer to Session Border Controller installation manuals and appropriate release notes for further assistance. Also note, this version of the Session Border Controller is the first to require the license file be loaded via WebLM.

6.2. Configuration File

The GUI installation wizard prompted for IP addresses, port numbers, domains, etc. and then created the initial configuration file for the Session Border Controller. This configuration file is listed below and has been appended, but the configured fields are shown.

```
#
#  Copyright (c) 2004-2010  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 15:15:21 Thu 2011-04-07
#
config cluster
 config box 1
  set hostname AA-SBC.avayalab.com
  set timezone America/Denver
  set name AA-SBC.avayalab.com
  set identifier 00:ca:fe:41:41:30
  config interface eth0
   config ip inside
    set ip-address static 205.3.000.000/24
    config ssh
    return
    config snmp
     set trap-target 205.3.000.000 162
    return
    config web
    return
    config web-service
     set protocol https 8443
     set authentication certificate "vsp\tls\certificate ws-cert"
    return
    config sip
     set udp-port 5060 "" "" any 0
     set tcp-port 5060 "" "" any 0
     set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
    return
     config routing
     config route Default
      set gateway 205.5.000.000
     return
     config route Static0
      set destination network 192.11.13.4/30
      set gateway 205.3.0.0
     return
     config route Static1
      set admin disabled
     return
```

```
    return
   return
  return
  config interface eth2
   config ip outside
    set ip-address static 205.168.000.000/25
    config sip
     set udp-port 5060 "" "" any 0
    return
    config media-ports
    return
    config routing
     config route Default
      set admin disabled
     return
     config route external-sip-media-1
      set destination network 67.148.000.000/28
      set gateway 205.168.1.1
     return
    return
    config kernel-filter
     config allow-rule allow-sip-udp-from-peer-1
      set destination-port 5060
      set source-address/mask 67.148.000.000/28
      set protocol udp
     return
     config deny-rule deny-all-sip
      set destination-port 5060
     return
    return
   return
  return
  config cli
   set prompt AA-SBC.avayalab.com
  return
 return
return
config vsp
 set admin enabled
 config default-session-config
  config media
   set anchor enabled
   set rtp-stats enabled
  return
  config sip-directive
   set directive allow
  return
  config log-alert
   set apply-to-methods-for-filtered-logs
  return
  config third-party-call-control
   set admin enabled
   set handle-refer-locally disabled
  return
 return
 config tls
```

```
 config default-ca
  set ca-file /cxc/certs/sipca.pem
 return
 config certificate ws-cert
  set certificate-file /cxc/certs/ws.cert
 return
 config certificate aasbc.p12
  set certificate-file /cxc/certs/aasbc.p12
  set passphrase-tag aasbc-cert-tag
 return
return
config session-config-pool
 config entry ToTelco
  config to-uri-specification
   set host next-hop
   set user-param keep
  return
  config from-uri-specification
   set host local-ip
   set user-param keep
  return
  config request-uri-specification
   set host next-hop
   set user-param keep
  return
  config p-asserted-identity-uri-specification
   set host local-ip
   set user-param keep
  return
  config forking-settings
   set outbound-arbiter-rule weighted-round-robin
  return
  config header-settings
  return
 return
 config entry ToPBX
  config to-uri-specification
   set host next-hop-domain
  return
  config request-uri-specification
   set host next-hop-domain
  return
  config header-settings
  return
 return
 config entry Discard
  config sip-directive
  return
 return
return
config dial-plan
 config route Default
  set priority 500
  set location-match-preferred exclusive
  set session-config vsp\session-config-pool\entry Discard
 return
```

```
  config source-route FromTelco
   set peer server "vsp\enterprise\servers\sip-gateway PBX"
   set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
   set peer server "vsp\enterprise\servers\sip-gateway Telco"
   set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
 return
 config enterprise
  config servers
   config sip-gateway PBX
    set domain avayalab.com
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
    config server-pool
     config server PBX1
      set host 205.3.000.000
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set failover-detection ping
    set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
    config server-pool
     config server Telco1
      set host 67.148.000.000
     return
    return
   return
  return
 return
 config dns
  config resolver
   config server 205.3.000.000
   return
  return
 return
 config settings
  set read-header-max 8191
 return
return
config external-services
return
config preferences
 config gui-preferences
  set enum-strings DatabaseName spotlite
  set enum-strings SIPSourceHeader Refer-to
 return
return
config permissions read-only
  set config view
  set actions disabled
```

```
 return
 config users
  config user admin
   set password
0x0062cbb6cbe2cad687396c595c8460dba0ea4dc0a39c09dc77475f6be3
   set permissions access\permissions superuser
  return
  config user cust
   set password
0x00c7e90a870789f8cfcbbeb59233fac1a36075cbd8013a9a5acceaa387
   set permissions access\permissions read-only
  return
  config user init
   set password
0x0094cf691d6888e6b02f413213093a7585c31fa1624682b766a60f24de
   set permissions access\permissions superuser
  return
  config user craft
   set password
0x00eeb7c06047a5f92e29fff123b971cd57ec0dd0768d7bf072c911bc70
   set permissions access\permissions superuser
  return
  config user dadmin
   set password
0x00107d0dc0bb643d5f4c1043175f8ecf01924b7812bd530c54ac1e97be
   set permissions access\permissions read-only
  return
 return
return

config features
return
```

7. Qwest iQ SIP Trunking 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.

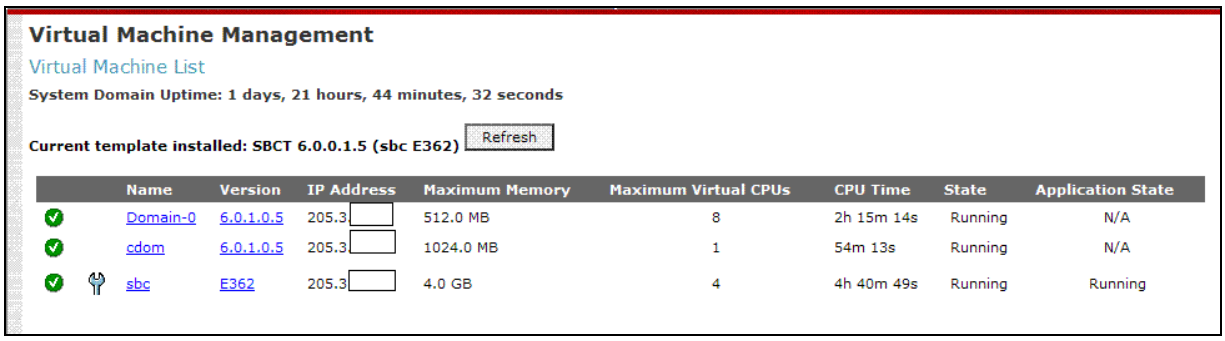
8. Verification Steps

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. Avaya Aura® Session Border Controller Verification

This section illustrates verifications using the Session Border Controller and Wireshark to illustrate key SIP messaging.

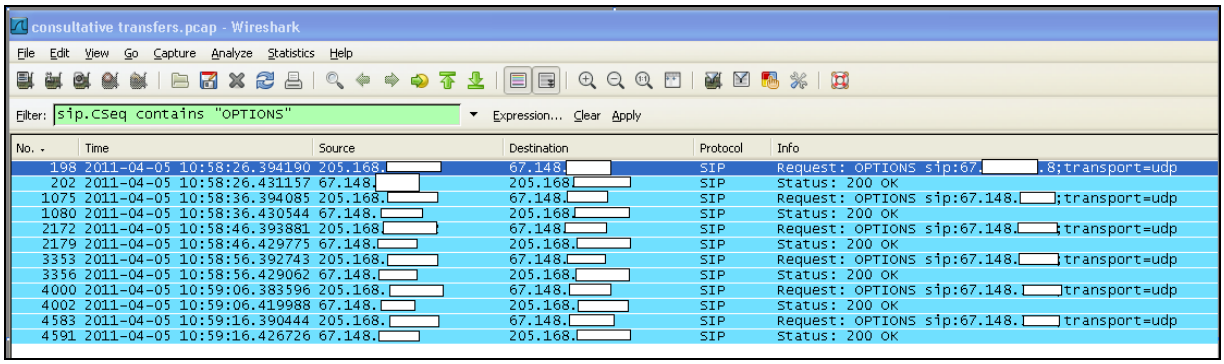
This section contains verification steps that may be performed using the Session Border Controller. The status of the virtual machines can be checked via the System Platform Console Domain of the server. The following screen, available via the Virtual Machine Management link in the console domain, shows the "**Running**" State of the Session Border Controller.



Click on the wrench icon to the left of the name "sbc" to access the element manager user interface of the Session Border Controller.

8.1.1. Verify Connectivity to Qwest SIP Trunk

Using Wireshark, verify that entity links from the Session Border Controller (205.168.x.x) to Qwest SIP Trunk (67.148.x.x) are communicating with SIP OPTION messages and 200 OK responses.



8.1.2. Verify Connectivity to Communication Manager

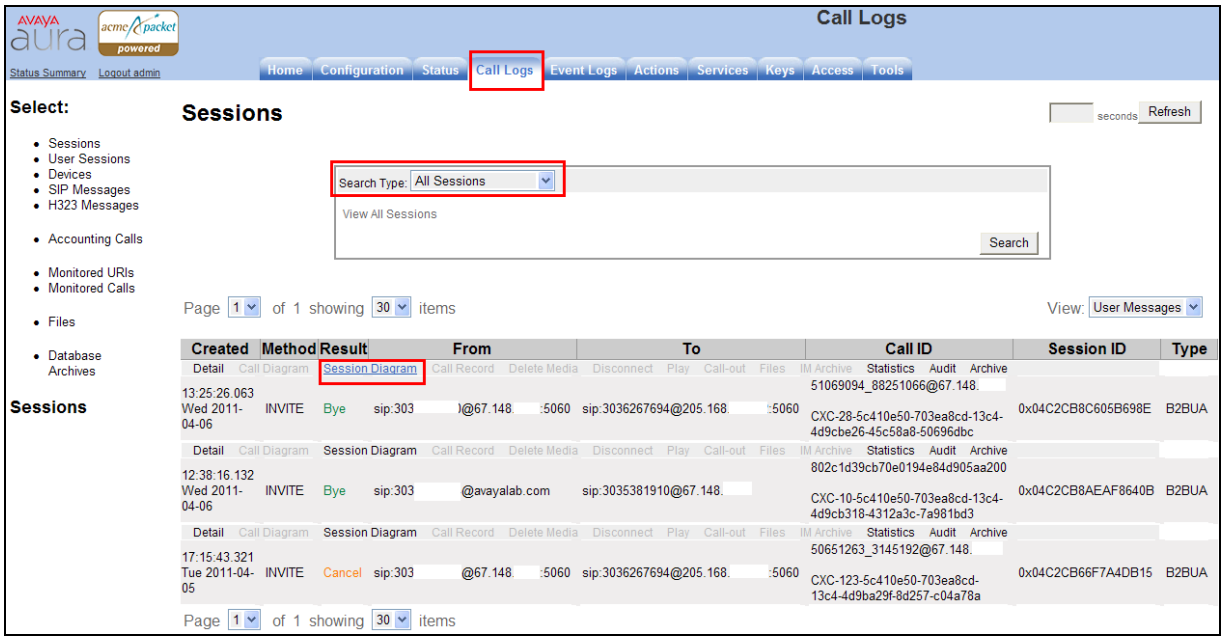
Verify that the signaling group / trunk group between the Communication Manager and Session Border Controller are up by using the **status signaling group #** and **status trunk-group** commands**.**

```
status signaling-group 1
                          STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

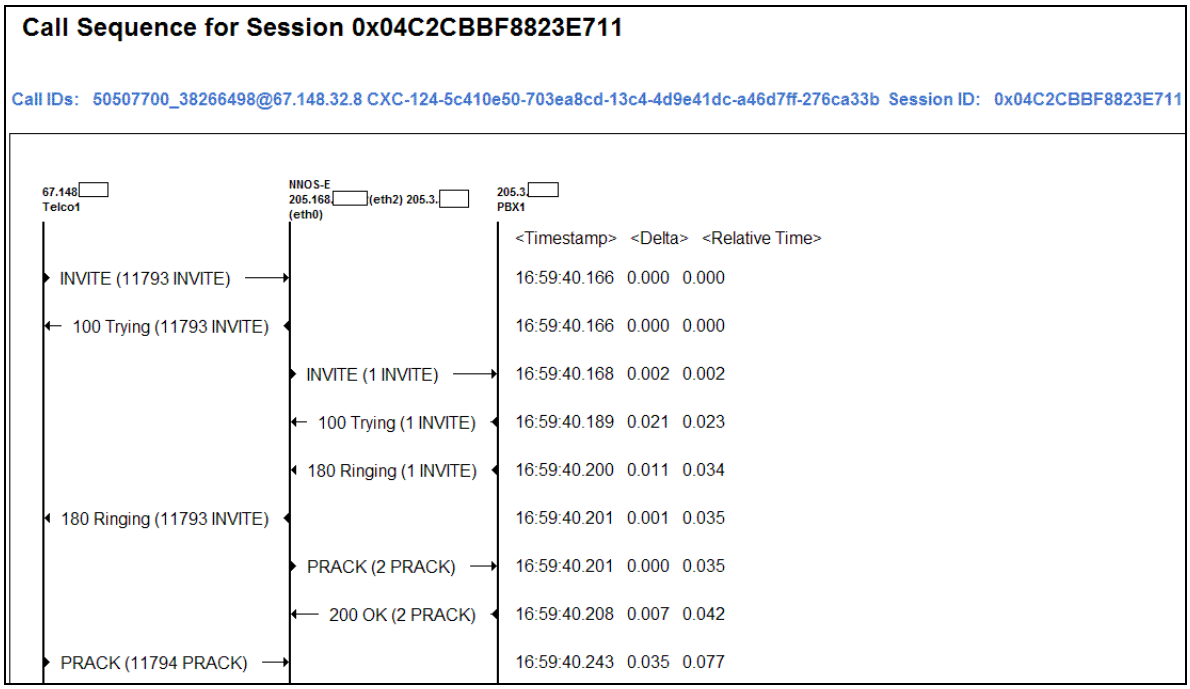
```
status trunk 1                                                    Page    1
                                TRUNK GROUP STATUS

Member    Port      Service State       Mtce Connected Ports
                                        Busy
0001/001  T00001    in-service/idle     no
0001/002  T00002    in-service/idle     no
0001/003  T00013    in-service/idle     no
0001/004  T00014    in-service/idle     no
0001/005  T00015    in-service/idle     no
0001/006  T00016    in-service/idle     no
0001/007  T00017    in-service/idle     no
```

8.1.3. Session Border Controller Call Logs

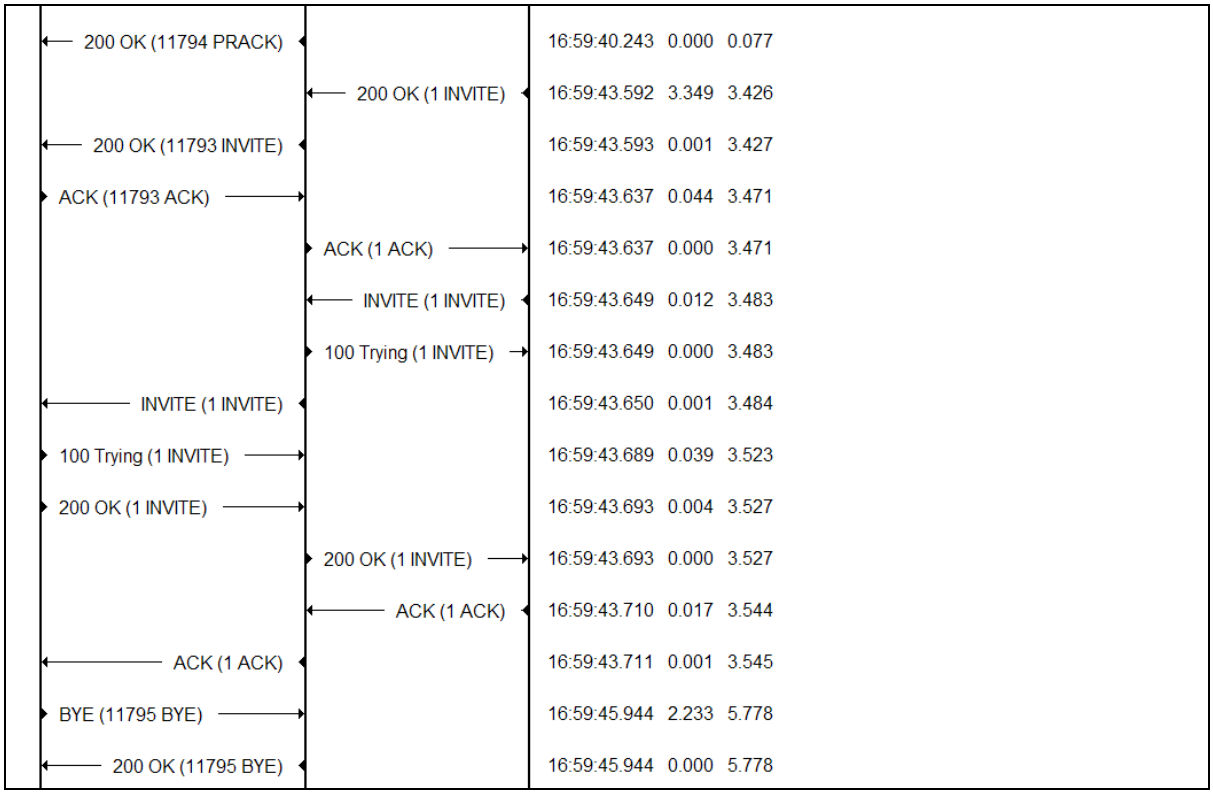
Call Log Ladder Diagrams visually displays the call flow between the service provider, the Session Border Controller and Communication Manager. To view this diagram, log into the web interface on the Session Border Controller, navigate to **Call Logs,** in **Search Type:** Enter **All Sessions** or Filter appropriately **Session Diagram** (for the appropriate call)**.**



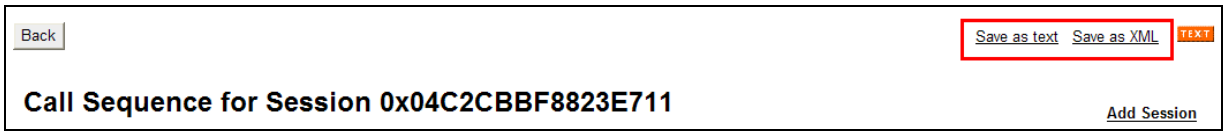
The following screen shows a portion of the ladder diagram for an inbound call. Note that the activity for both the inside private and outside public side of the Session Border Controller can be seen.



Scroll down to continue the ladder diagram. The following screen shows the portion of the ladder diagram for a call that is answered by a Communication Manager and released on the PSTN/Qwest SIP Trunk side.



At the top right of the screen, the session may be saved as a text or XML file. If the session is saved as an XML file, using the **Save as XML** link, the xml file can be provided to support personnel that can open the session on another Session Border Controller for analysis.



8.2. Communication Manager and Wireshark Verifications

8.2.1. Example Incoming Call from PSTN via Qwest SIP Trunk

DID and incoming toll-free calls arrive from Qwest SIP Trunk at the Session Border Controller, which sends the call to Communication Manager on trunk 1 signaling group 1.

The following abridged Communication Manager "**list trace**" trace output shows a call incoming on trunk group1. The PSTN telephone dialed 303-555-7694. The "***inc-call-handling-trmt trunk-group 1***" maps the incoming number to an extension of a Communication Manager telephone (x3005). Extension 3005 is an IP Telephone with IP Address 205.3.123.333 in Region 1. Initially, the G650 Media Gateway (205.3.123.111) 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 (205.3.123.333) to the "inside" of the Session Border Controller (205.3.123.222).

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 *101                                                    Page   1
                                LIST TRACE
time            data

16:24:22 TRACE STARTED 04/07/2011 CM Release String cold-00.1.510.1
16:25:07 SIP<INVITE sip:3035557694@avayalab.com:5060 SIP/2.0
16:25:07     active trunk-group 1 member 1  cid 0x208
16:25:07 SIP>SIP/2.0 180 Ringing
16:25:07     dial 3005
16:25:07     ring station    3005 cid 0x208
16:25:07     G711MU ss:off ps:20
             rgn:1 [205.3.123.222]:7306
             rgn:1 [205.3.123.111]:7672
16:25:07     G711MU ss:off ps:20
             rgn:1 [205.3.123.333]:23512
             rgn:1 [205.3.123.222]:7648
16:25:07     xoip options: fax:PT modem:off tty:US  uid:0x50001
             xoip ip: [205.3.3.222]:7648
16:25:07 SIP<PRACK sip:3035557694@avayalab.com:5060 SIP/2.0
16:25:09 SIP>SIP/2.0 200 OK
16:25:09     active station    3005 cid 0x208
16:25:09 SIP<ACK sip:3035557694@avayalab.com:5060 SIP/2.0
16:25:09 SIP>INVITE sip:3035551910@67.148.000.000:5060;transport=tc
16:25:09 SIP>p;maddr=205.3.3.208 SIP/2.0
16:25:09 SIP<SIP/2.0 100 Trying
16:25:09 SIP<SIP/2.0 200 OK
16:25:09 SIP>ACK sip:3035551910@67.148.000.000:5060;transport=tcp;m
16:25:09 SIP>addr=205.3.3.208 SIP/2.0
16:25:09     G711MU ss:off ps:20
```

The following screen shows **Page 2** of the output of the "***status trunk 1/1***" command pertaining to the same call. Note the signaling using port 5060 between Communication Manager and the Session Border Controller. Note the media is "**ip-direct**" from the IP Telephone (205.3.3.235) to the inside IP Address of the Session Border Controller (205.3.3.208) using G.711.

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

Near-end Signaling Loc: 01A0217
  Signaling   IP Address                              Port
   Near-end:  205.3.3.221                           : 5060
    Far-end:  205.3.3.208                           : 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:  205.3.3.235                           : 7306
    Far-end:  205.3.3.208                           : 23512
```

```
status trunk 1/1                                                    Page   3 of   3
                        SRC PORT TO DEST PORT TALKPATH
src port: T00001
T00001:TX:205.3.3.208:23512/g711u/20ms
S00010:RX:205.3.3.235:7306/g711u/20ms
```

Verification Steps:

1. Verify that entity links from the Session Border Controller (205.168.000.000) to Qwest SIP Trunk (67.148.000.000) are up and communicating with SIP OPTION messages and 200 OK responses.
2. Verify that the signaling group / trunk group between the Communication Manager and Session Border Controller are up by using ***status signaling group*** # and ***status trunk-group*** #.
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.

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. Session Border Controller
    - **Virtual Server Platform status page**
    - **Session Border Controller initial status page**
    - **Call logs from the ladder diagrams**

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and Avaya Aura® Session Border Controller to Qwest SIP Trunking. Qwest SIP Trunking passed compliance testing. Please refer to **Section 2.2** for any observations 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 2011, Document Number 03-603628.
[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* August 2010, *D*ocument Number 555-245-205.
[3] *Installing Avaya Aura® SBC System Administration Guide*, 2010.
[4] *Administering Avaya Aura® Session Services Configuration Guide,* 2010.
[5] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x,* February 2010, Document Number 16-601443.
[6] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.
[7] *Avaya one-X® Deskphone H323 Administrator Guide Release 6.1,* May 2011, Document Number 16-300698.
[8] *Avaya one-X® Communicator Getting Started, November 2009.*
[9] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/
[10] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/
[11] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

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.