



Application Notes for Configuring CenturyLink SIP Trunking with Avaya Aura® Communication Manager Evolution Server 6.0.1 and Avaya Aura® Session Border Controller 6.0 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server and an Avaya Aura® Session Border Controller, along with various Avaya endpoints.

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

1. Introduction

These Application Notes describe the steps required to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunking service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server and an Avaya Aura® Session Border Controller (SBC), along with various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to the CenturyLink 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

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various 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.
- 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, international, outbound toll-free, and operator (0).
- Codecs G.711MU and G.729A were tested but only codec G.711Mu is currently supported in the CenturyLink production environment.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).

Items not supported or not tested included the following:

- Inbound toll-free and emergency calls are supported but were not tested.
- T.38 Fax is not supported.

2.2. Test Results

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

- **Consultative Transfer:** When an enterprise phone attempts a consultative transfer out to the PSTN, the call will successfully transfer with two-way audio for roughly 10 seconds and then will disconnect. At the time these App Notes were being written, this issue was actively being worked for a resolution.
- **Off-net call forwarding:** When INVITE from the enterprise to CenturyLink for forwarding inbound call back to PSTN contains both Diversion and History-Info headers, CenturyLink would respond with "604 Does not exist anywhere" resulting failure of off-net call forward. This failure was addressed in the compliance test by turning off the History-Info header in the call-redirection INVITE from the enterprise.
- **EC500:** EC500 is the Communication Manager mobility feature which allows a user to have incoming calls ring the destination extension as well as a remote off-net number such as a mobile phone. When the INVITE from the enterprise to CenturyLink for the remote PSTN endpoint contains both Diversion and History-Info headers, CenturyLink would respond with "604 Does not exist anywhere" causing the EC500 call to fail. This failure was addressed in the compliance test by turning off the History-Info header in the call-redirection INVITE from the enterprise.
- **No Error Indication if No Matching Codec Offered:** If the Communication Manager SIP trunk is improperly configured to have no matching codecs with the service provider and an outbound call is placed, the service provider only returns a "100 Trying" response and no error indication. As a result, Communication Manager cancels the call when the Alternate Route Timer expires (generally 6 seconds by default).
- **Asynchronous DTMF payload header values are not supported:** CenturyLink 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. CenturyLink 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 as described in these Application Notes. This issue may occur in other call scenarios that were not tested.

2.3. Support

For technical support on CenturyLink SIP Trunking, contact CenturyLink using the **Support→Contact Us** links at www.centurylink.com, or by calling business customer support at 1-800-201-4102.

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Selecting the **Support Contact Options** link followed by **Maintenance Support** provides the *worldwide support directory* for Avaya Global Services. . Alternatively, in the United States, the phone number (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

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

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

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

Located at the edge of the enterprise is the Avaya Aura® SBC. It has a public side that connects to the external service provider network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flow through the Avaya Aura® SBC. In this way, the Avaya Aura® SBC can protect the enterprise against any SIP-based attacks. The Avaya Aura® SBC provides network address translation at both the IP and SIP layers.

Although Modular Messaging 5.2 was used for voicemail and to test DTMF, the installation and configuration of Modular Messaging is outside the scope of these Application Notes. For installation and configuration of Modular Messaging see reference [9] in **Section 10**.

For security reasons, any actual public IP addresses used in the configuration have been replaced throughout this document. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

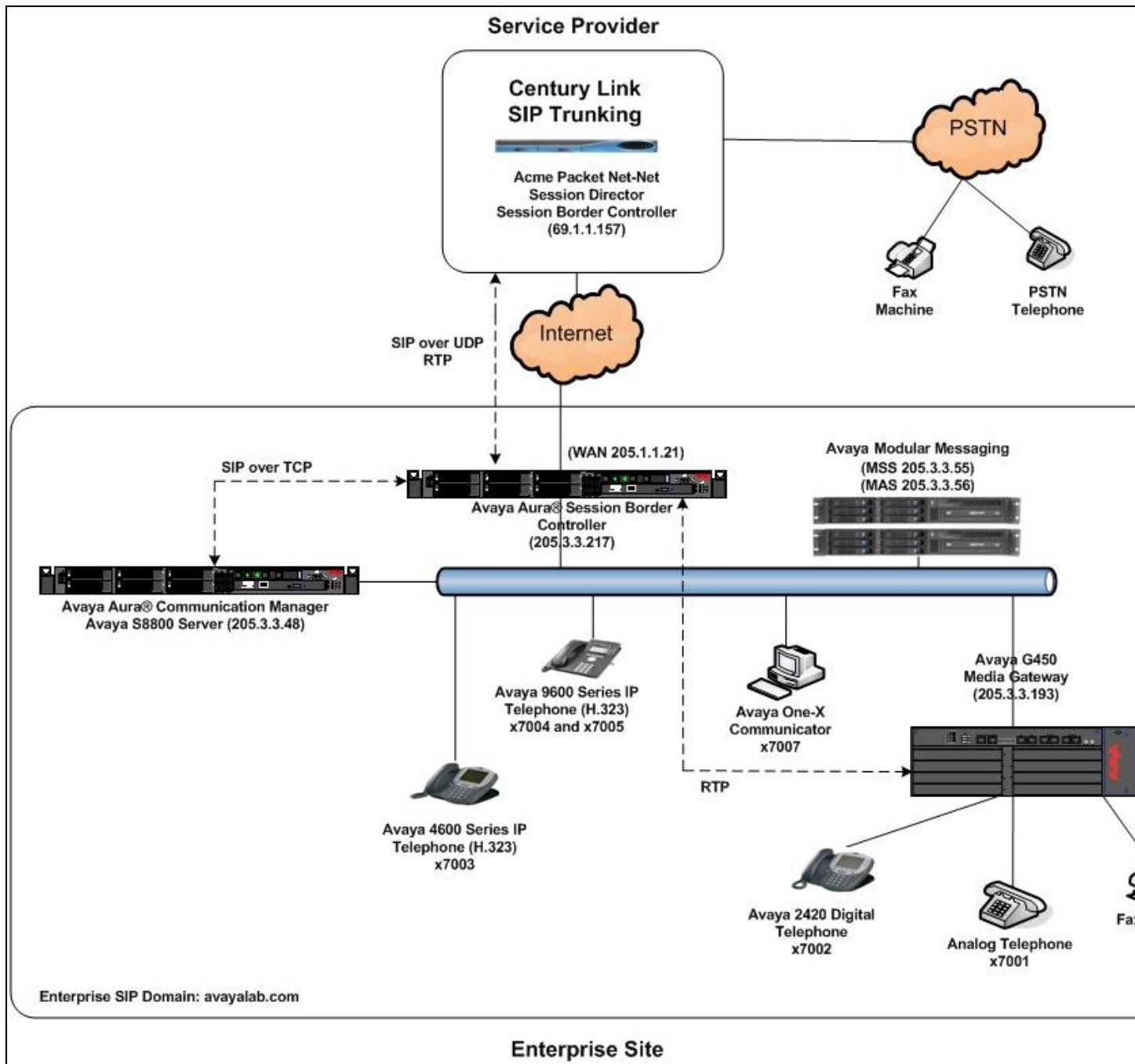


Figure 1: Avaya IP Telephony Network using CenturyLink SIP Trunking

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

For inbound calls, the calls flow from the service provider network to the Avaya Aura® SBC and then to Avaya Aura® Communication Manager. Once the call arrives at Avaya Aura® Communication Manager further incoming call treatment, such as incoming digit translations and class of service restrictions, may be performed.

Outbound calls to the PSTN are first processed by Avaya Aura® Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Avaya Aura® Communication Manager selects the proper SIP trunk, the call is routed to the Avaya Aura® SBC. From the Avaya Aura® SBC, any necessary Header Manipulations are executed and the call is sent to the CenturyLink SIP Trunking service.

For the compliance test, the enterprise sent 11 digits in the destination headers (e.g., Request-URI and To headers) and sent 10 digits in the source headers (e.g., From, Contact, and P-Asserted-Identity headers). CenturyLink sent 10 digits in both the source and destination headers.

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on an Avaya S8800 Server	6.0.1 (R016x.00.1.510.1) (System Platform 6.0.2.0.5)
Avaya Aura® Session Border Controller running on an Avaya S8800 Server	6.0 Version E362P1 (Build 47121) (System Platform 6.0.1.0.5)
Avaya G450 Media Gateway	30.14.0
Avaya 4610SW IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 9620 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1.1
Avaya one-X® Communicator (H.323)	6.0.0.26
Avaya 2420 Digital Telephone	n/a
Avaya Analog Telephone	n/a
Modular Messaging: <ul style="list-style-type: none"> • MAS • MSS 	5.2 SP5 5.2 SP5
CenturyLink SIP Trunking Solution Components	
Component	Release
Acme Packet Net-Net Session Border Controller	6.1
BroadSoft Softswitch	R17 sp1
Sonus Media Gateway	V07.02.05R000

Table 1: Equipment and Software Tested

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Avaya Aura® Communication Manager for CenturyLink SIP Trunking. A SIP trunk is established between Avaya Aura® Communication Manager and the Avaya Aura® SBC for use by signaling traffic to and from CenturyLink. It is assumed that the basic installation tasks for Avaya Aura® Communication Manager, the Avaya G450 Media Gateway, and the Avaya Aura® SBC have been previously completed and are 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 58 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 3
      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 58
Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
  Maximum Number of DS1 Boards with Echo Cancellation: 522 0
      Maximum TN2501 VAL Boards: 128 0
      Maximum Media Gateway VAL Sources: 250 1
  Maximum TN2602 Boards with 80 VoIP Channels: 128 0
  Maximum TN2602 Boards with 320 VoIP Channels: 128 0
  Maximum Number of Expanded Meet-me Conference Ports: 300 0

(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:
      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 Avaya S8800 Server running Communication Manager (*procr*) and for the inside IP address of the Avaya Aura® SBC. 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
AA-SBC            205.3.3.217
ASM61               205.3.3.204
Acme                205.3.3.3
MM                205.3.3.56
SMGR61             205.3.3.203
default             0.0.0.0
procr            205.3.3.48
procr6             ::
```

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls within the enterprise. For the compliance test, codecs G.711MU and G.729A 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 order of preference. Default values can be used for all other fields.

```
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** to support T.38 faxing *within* the enterprise.

```
change ip-codec-set 1                                   Page 2 of 2
                                                    IP Codec Set
Allow Direct-IP Multimedia? n
FAX                Mode          Redundancy
t.38-standard    0
Modem              off           0
TDD/TTY           US            3
Clear-channel     n            0    Clear-channel n    0
```

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 3. To use these codecs, enter **G.729A** and **G.711MU** in the **Audio Codec** column of the table in order of preference. Default values can be used for all other fields.

```
change ip-codec-set 3                                     Page 1 of 2

                                IP Codec Set

Codec Set: 3

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

On **Page 2**, set the **Fax Mode** to **off** since T.38 faxing is not currently supported by CenturyLink’s SIP Trunking service.

```
change ip-codec-set 3                                     Page 2 of 2

                                IP Codec Set

                                Allow Direct-IP Multimedia? n

FAX      Mode      Redundancy
Modem      off         0
TDD/TTY    US         3
```

5.5. IP Network Regions

Create an IP-Network-Region for devices within the enterprise. For the compliance test, IP-network-region 1 was chosen for the enterprise. 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. In this case **Enterprise** was used.
- 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 for the enterprise 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: 1           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? n
    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5           AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Peer Detection Enabled? y Peer Server: Others

```

On **Page 4**, define the IP codec set to be used for traffic between region 3 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 3. 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 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for ip network region 1 will automatically create a complementary table entry on the ip network region 3 form for destination region 1. This complementary table entry can be viewed using the **display ip-network-region 3** command and navigating to **Page 4**.

```

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
2
3      3      y      NoLimit                                n      t
4

```

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 3 was chosen for the service provider trunk. Use the **change ip-network-region 3** command to configure region 3 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain or IP address of the service providers SBC or SIP proxy. In this configuration, an IP address of the service provider SBC, **69.1.1.157**, was used. This appears in the Host portion of the “From” header of SIP messages originating from this IP region.

- Enter a descriptive name in the **Name** field. In this case **CenturyLink SIPT** was used.
- 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 for calls between the enterprise and CenturyLink in **Section 5.4**.
- Default values can be used for all other fields.

```

change ip-network-region 3                                     Page 1 of 20
                                                           IP NETWORK REGION
Region: 3
Location:                               Authoritative Domain: 69.1.1.157
Name: CenturyLink SIPT
MEDIA PARAMETERS                                           Intra-region IP-IP Direct Audio: yes
Codec Set: 3                                               Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                         IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5

```

On **Page 4**, define the IP codec set to be used for traffic between region 3 and region 1. Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 3 will be used for calls between region 3 (the service provider region) and region 1 (the rest of the enterprise). Creating this table entry for ip network region 3 will automatically create a complementary table entry on the ip network region 1 form for destination region 3. This complementary table entry can be viewed using the **display ip-network-region 1** command and navigating to **Page 4**.

```

change ip-network-region 3                                     Page 4 of 20
Source Region: 3      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 3 y NoLimit n t
2
3 3 all

```

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Avaya Aura® SBC for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 1 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, 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 Avaya Aura® SBC.
- Set the **IMS Enabled** field to *n*.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port which can be a random unused port or 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 **Peer Detection Enabled** field to *y*. The **Peer Server** field will initially be set to *Others* and cannot be changed via administration. The **Peer Server** field would automatically change to *SM* if Communication Manager detected an Avaya Aura® Session Manager peer. No Avaya Aura® Session Manager was used in this compliance test configuration, so the **Peer Server** field value of *Others* is the proper setting.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *AA-SBC*. This node name maps to the IP address of the Avaya Aura® SBC as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to the IP address of the CenturyLink SBC.
- Set **Direct IP-IP Audio Connections** to *y*. This field will enable media shuffling on the SIP trunk associated with this signaling group allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set the **DTMF over IP** field to *rtp-payload*. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to *15*. This defines the number of seconds that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

```

add signaling-group 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: procr                Far-end Node Name: AA-SBC
Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                                Far-end Network Region: 3

Far-end Domain: 69.1.1.157

Incoming Dialog Loopbacks: eliminate    Bypass If IP Threshold Exceeded? n
                                           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? y
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 1 was configured using the parameters highlighted below.

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

```

add trunk-group 1
                                TRUNK GROUP
                                Page 1 of 21

Group Number: 1                Group Type: sip                CDR Reports: y
    Group Name: CenturyLink                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: 14

```

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** seconds was used.

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

TRUNK PARAMETERS

  Unicode Name: auto
                                     Redirect On OPTIM Failure: 15000

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

  XOIP Treatment: auto   Delay Call Setup When Accessed Via IGAR? n
```

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

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

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

                                     Numbering Format: public
                                               UI Treatment: service-provider

                                               Replace Restricted Numbers? y
                                               Replace Unavailable Numbers? y

  Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y
```

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

```

add trunk-group 1
                                Page 4 of 21
                                PROTOCOL VARIATIONS
                                Mark Users as Phone? y
                                Prepend '+' to Calling Number? n
                                Send Transferring Party Information? n
                                Network Call Redirection? n
                                Send Diversion Header? y
                                Support Request History? n
                                Telephone Event Payload Type: 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. Calling Party Information

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

In the sample configuration, five DID numbers were assigned for testing. These five DID numbers were assigned to six extensions (7001 thru 7005, and 7007). These 10-digit DID numbers were used for the outbound calling party information on the service provider trunk whenever calls were originated from these six extensions. **NOTE:** Extensions 7001 and 7002, the analog and digital phones respectively, used the same DID of 913-555-5972 for their outbound calling party information due to only having five DID numbers for this compliance test. The top entry for trunk group 5 is necessary so that Modular Messaging receives the proper extension information for any calls that roll to voicemail.

```

change public-unknown-numbering 0
                                Page 1 of 2
                                NUMBERING - PUBLIC/UNKNOWN FORMAT
                                Total
                                Ext Ext      Trk      CPN      Total
                                Len Code      Grp(s)  Prefix   CPN
                                Len
                                4  7          5          4
                                4  7001       1          9135555972  10
                                4  7002       1          9135555972  10
                                4  7003       1          9135555973  10
                                4  7004       1          9135555974  10
                                4  7005       1          9135555975  10
                                4  7007       1          9135555976  10
                                Total Administered: 9
                                Maximum Entries: 9999
                                Note: If an entry applies to
                                a SIP connection to Avaya
                                Aura(tm) Session Manager,
                                the resulting number must
                                be a complete E.164 number.

```


5.9. Outbound Routing

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

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

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

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

```
change feature-access-codes Page 1 of 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:	Act:	Deactivation:
Call Park Access Code:	125	
Call Pickup Access Code:	126	

Use the **change ars analysis x** command to configure the routing of dialed digits following the first digit 9, where **x** is the next digit in the string to be matched against the table below. The example below shows a large subset of the dialed strings tested as part of the compliance test. Towards the bottom there are example entries for 10-digit dialing. 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 String	Total		Route Pattern	Call Type	Node Num	ANI Reqd
	Min	Max				
0	1	1	1	op		n
0	8	8	1	op		n
0	11	11	1	op		n
00	2	2	1	op		n
01	9	17	1	iop		n
011	10	18	1	intl		n
..... output truncated.....						
130	11	11	1	hnpa		
1300	11	11	deny	fnpa		
131	11	11	1	fnpa		
132	11	11	1	fnpa		
133	11	11	1	fnpa		
134	11	11	1	fnpa		
135	11	11	1	fnpa		
136	11	11	1	fnpa		
137	11	11	1	fnpa		
..... output truncated.....						
172	11	11	1	hnpa		
173	11	11	1	fnpa		
174	11	11	1	fnpa		
175	11	11	1	fnpa		
176	11	11	1	fnpa		
177	11	11	1	fnpa		
178	11	11	1	fnpa		
179	11	11	1	fnpa		
180	11	11	1	fnpa		
..... output truncated.....						
2	10	10	1	fnpa		
3	10	10	1	hnpa		
4	10	10	1	fnpa		
411	3	3	1	svcl		
5	10	10	1	fnpa		
6	10	10	1	fnpa		
611	3	3	1	svcl		
7	10	10	1	hnpa		
8	10	10	1	fnpa		
811	3	3	1	svcl		
9	10	10	1	fnpa		
911	3	3	1	svcl		
913	10	10	1	fnpa		

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 used in 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 *1* 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 HNP 10 digit numbers are left unchanged.
- **LAR:** *next*

```

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

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

```

6. Configure Avaya Aura® Session Border Controller (SBC)

This section illustrates an example configuration of the Avaya Aura® SBC. Similar to Avaya Aura® Communication Manager Release 6, the Avaya Aura® SBC runs on its own S8800 Server as an application template using Avaya Aura® System Platform. The installation of the System Platform is assumed to have been previously completed.

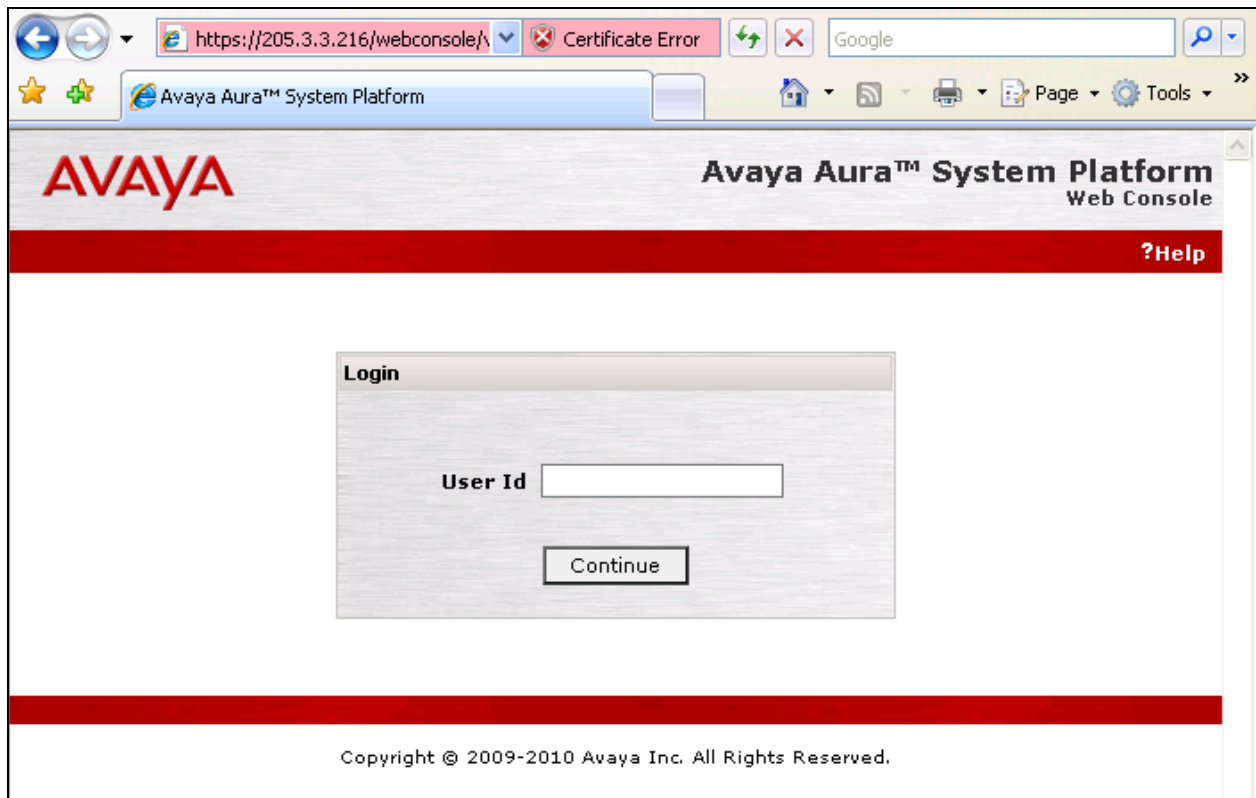
The Avaya Aura® SBC includes a configuration wizard that can be used as part of the installation of the SBC template on System Platform. As such, screens from the installation of the SBC template are presented in Section 6.1. The wizard pre-configures the underlying SBC for much of the required provisioning. After the Avaya Aura® SBC has been installed as shown in Section 6.1, any subsequent changes to the network configuration (e.g., IP address, network mask, hostname) for the Avaya Aura® SBC eth0 or eth2 interfaces must be done via the System Platform webconsole Network Configuration page. Any backup and restore actions should also use System Platform. Configuration of SBC behaviors (e.g., header manipulations) can be performed through the element manager GUI as shown in Section 6.3.

Although licensing tasks are not typically covered in Application Notes and this document does not aim to be an authoritative guide to licensing, example screens and procedures for the licensing of the Avaya Aura® SBC used for the verification testing are provided in Section 6.2.

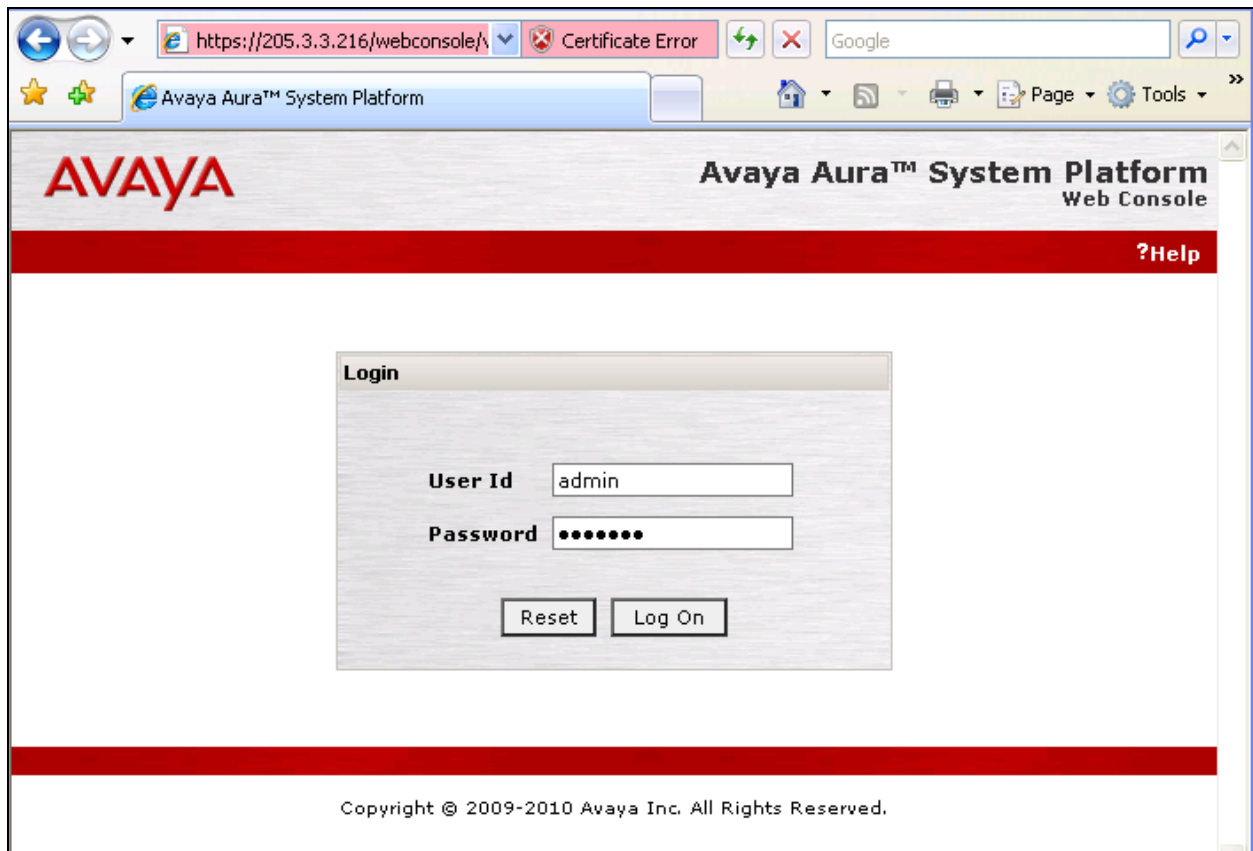
In the sample configuration, the Avaya S8800 Server has four physical network interfaces, labeled 1 through 4. The port labeled “1” (virtual “eth0”) is used for the management and private (inside) network interface of the SBC. The port labeled “3” (virtual “eth2”) is used for the public (outside) network interface of the SBC.

6.1. Avaya Aura® SBC Installation

To begin the SBC Template installation, log in to the System Platform console domain by entering `https://<ip-addr>/webconsole` as shown in the example screen below. In the sample configuration, the console domain uses the IP Address 205.3.3.216, and the system domain uses the IP Address 205.3.3.215. Enter an appropriate **User Id** and press the **Continue** button.



On the subsequent screen, enter the appropriate **Password** and click the **Log On** button.



The following screen shows the left-hand side of the System Platform webconsole menu.



The following screen shows the right-hand side, showing the System Domain "Domain-0" and the Console Domain "cdom" in the sample configuration.

The screenshot shows the 'Virtual Machine Management' section of a web interface. It includes a sidebar menu with 'Virtual Machine Management', 'Server Management', and 'User Administration'. The main content area displays 'Virtual Machine List' with a system uptime of 10 days, 21 hours, 37 minutes, and 23 seconds. Below this, it states 'Current template installed: SBCT 6.0.0.1.5 (sbc E362)' with a 'Refresh' button. A table lists three VMs:

Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
Domain-0	6.0.1.0.5	205.3.3.215	512.0 MB	16	13h 45m 35s	Running	N/A
cdom	6.0.1.0.5	205.3.3.216	1024.0 MB	1	5h 22m 52s	Running	N/A
sbc	E362	205.3.3.217	4.0 GB	4	1d 3h 21m 6s	Running	Running

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

From the left menu, select **Virtual Machine Management** → **Solution Template**. In the **Install Template From** area, choose where the template files are located. In the sample configuration, the template files were copied to the System Platform server /vsp-template/ directory prior to installation, but USB or other means may be used. Click **Search**.

The screenshot shows the 'Virtual Machine Management' interface with the 'Search Local and Remote Template' section. It displays 'Current template installed: No Template Installed'. The 'Install Template From' dropdown menu is open, showing options: 'Avaya Downloads (PLDS)', 'HTTP', 'SP Server' (highlighted), 'SP CD/DVD', and 'SP USB Disk'. The 'Template Location' text box contains '/vsp-template/'. A 'Search' button is visible at the bottom.

Select the appropriate file, such as “SBCT.ovf”. Click the **Select** button.

Virtual Machine Management

Select Template

Current template installed: No Template Installed

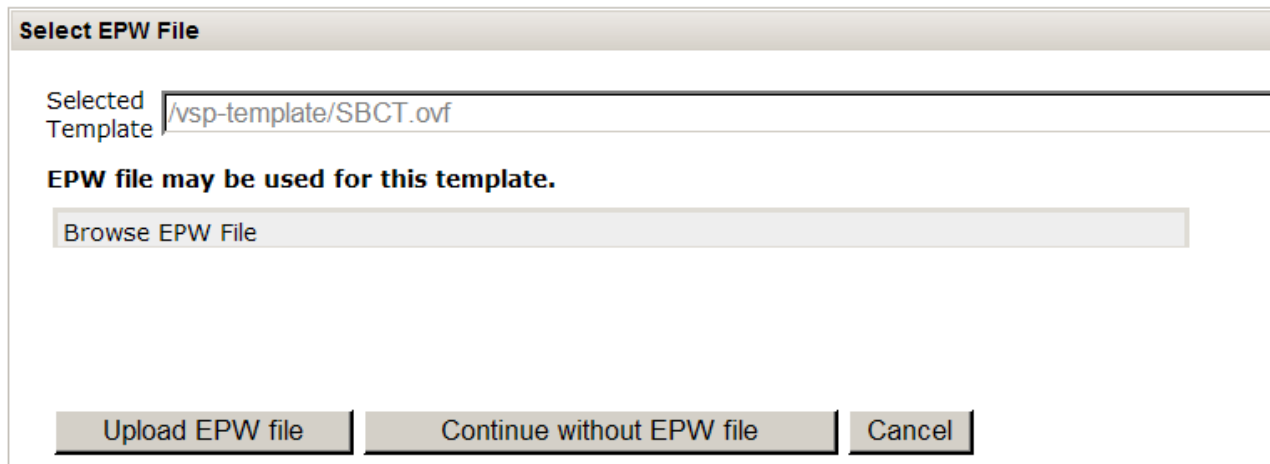


In the resultant screen shown below, the **Selected Template** can be observed. If an EPW file is available, it may be uploaded and used. In the sample configuration, the **Continue without EPF file** button was used.

Virtual Machine Management

Select Template

Current template installed: No Template Installed



The **Template Details** screen is presented. If satisfied that the information is correct, click the **Install** button.

Virtual Machine Management

Template Details

Current template installed: No Template Installed

Product ID: SBCT
Product Vendor: Avaya
Product Version: 6.0.0.1.5

Virtual Machines:

sbc
Product ID: sbc
Product Vendor: Avaya
Product Version: E362

After clicking the Install button, the screen will update similar to the following, showing “Processing your request, please wait”

Virtual Machine Management

Template Details

Current template installed: No Template Installed

Processing your request, please wait..... ▼

Product ID: SBCT
Product Vendor: Avaya
Product Version: 6.0.0.1.5

Virtual Machines:

sbc
Product ID: sbc
Product Vendor: Avaya
Product Version: E362

The installation will proceed until user input is expected, as shown below.

Virtual Machine Management

Template Installation

Cancel Installation

Template Installation In Progress

Workflow Status					
Start Time	Task Description	State	% Complete	Estimate	Actual
09:39:42	Download disk image for sbc	Complete	100	37s	✓
09:39:42	Download plugins for VMs	Complete	100	2s	✓
09:39:45	Check Template for Web Application	Complete	100	14s	✓
09:40:00	Download pre-install web application	Complete	100	0s	✓
09:40:00	Pre-Install Web Application Deployment	Complete	100	7s	✓
09:40:07	Wait For User To Complete Data Entry	In Progress	0		<div style="width: 0%; height: 10px; background-color: #ccc;"></div>

The following shows the first screen in a series of Installation screens, beginning with **Network Settings**. In the top portion of the screen, the System Domain **Domain-0 IP Address**, Console Domain **CDom IP Address**, **Gateway IP Address**, and **Network Mask** are pre-populated with information from System Platform. In the sample configuration, no DNS was entered during the System Platform installation. The Avaya Aura® SBC Installation requires that the Primary DNS be populated, even if DNS is not really used. In the screen below, the Primary DNS is configured to be the same address as the Console Domain.

In the bottom portion of the screen, the **IP Address** and **Hostname** of the Avaya Aura® SBC are configured. The IP Address 205.3.3.217 becomes the private, inside IP Address as well as the management address for the Avaya Aura® SBC.

Network Settings

Enter network settings

Domain-0 IP Address	<input type="text" value="205.3.3.215"/>
CDom IP Address	<input type="text" value="205.3.3.216"/>
Gateway IP Address	<input type="text" value="205.3.3.1"/>
Network Mask	<input type="text" value="255.255.255.0"/>
Primary DNS	<input type="text" value="205.3.3.9"/>
Secondary DNS	<input type="text"/>
HTTPS Proxy (if required) [IP Address:Port Number]	<input type="text" value="205.3.3.9:443"/>

Scroll down if necessary, and click **Next Step**.

Virtual Machine	IP Address	Hostname	Domain
SBC	<input type="text" value="205.3.3.217"/>	<input type="text" value="AuraSBC"/>	

[Next Step](#) 

The resulting screen allows VPN Access parameters to be configured. Configure as appropriate, or skip, and click **Next Step**.

VPN Access

Configure VPN Access

Would you like to configure the VPN remote access parameters for System Platform?

Yes No

VPN Access Configuration

VPN Router IP Address


Remote Access Network

Remote Access Network Subnet Mask

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

 [Previous Step](#)

[Next Step](#) 

The following screen shows the **Session Border Controller Data** configuration screen.

In the upper portion of the screen with heading **SIP Service Provider Data**, leave the **Service Provider** drop-down menu blank. The **IP Address** and **Port** fields are configured with the CenturyLink supplied IP Address (69.1.1.157) and port (5060) for the service as shown in **Figure 1**. If it is desired to use DNS to the CenturyLink network DNS server, the IP Address and port can still be specified here. The **Media Network** and **Media Netmask** fields are configured with the appropriate network routing information for the subnet. In the sample configuration, CenturyLink media IP addresses (signaled in SDP) are on the 69.1.1.0/24 network with network mask 255.255.255.0.

In the middle portion of the screen with heading **SBC Network Data**, the **Public IP Address** of the Avaya Aura® SBC known to the CenturyLink network is configured. As shown in **Figure 1**, CenturyLink will signal to IP Address 205.1.1.21. In the sample configuration, the **Gateway** for the public interface is 205.1.1.1. Note that the Private (Management) Interface information has already been completed with the IP Address (205.3.3.217) provided as the **Virtual Machine IP Address** on the first screen of the series.

In the lower portion of this screen with heading **Enterprise SIP Server**, the **IP Address** of the Avaya Aura® Communication Manager is configured. As shown in **Figure 1**, the Avaya Aura® SBC will signal to the Avaya Aura® Communication Manager at **IP Address** 205.3.3.48. TCP Transport was selected in the sample configuration to facilitate tracing visibility. The **SIP Domain** is configured to “avayalab.com” to match the CenturyLink configuration of the enterprise SIP domain.

SBC

Session Border Controller Data

SIP Service Provider Data				
Service Provider	IP Address	Port	Media Network	Media Netmask
<input type="text"/>	<input type="text" value="69.1.1.157"/>	<input type="text" value="5060"/>	<input type="text" value="69.1.1.0"/>	<input type="text" value="255.255.255.0"/>

SBC Network Data			
Interface	IP Address	Net Mask	Gateway
Private (Management)	<input type="text" value="205.3.3.217"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="205.3.3.1"/>
Public	<input type="text" value="205.1.1.21"/>	<input type="text" value="255.255.255.128"/>	<input type="text" value="205.1.1.21"/>

Enterprise SIP Server		
IP Address	Transport	SIP Domain
<input type="text" value="205.3.3.48"/>	<input type="text" value="TCP"/>	<input type="text" value="avayalab.com"/>

[◀ Previous Step](#)

[Next Step ▶](#)

Once complete, click **Next Step**. A summary screen will be presented. The summary screen for the sample configuration is shown below.

Summary

Network Settings	
Domain-0 Address	205.3.3.215
CDom Address	205.3.3.216
Gateway Address	205.3.3.1
Network Mask	255.255.255.0
Primary DNS	205.3.3.9
Secondary DNS	Not set
HTTPS Proxy	205.3.3.9:443

Virtual Machine	IP Address	Hostname
SBC	205.3.3.217	AuraSBC

VPN Access	
VPN Access	Not Configured

SBC	
Service Provider	Not set
Service Provider IP Address	69.1.1.157
Service Provider Port	5060
Service Provider Media Network	69.1.1.0
Service Provider Media Netmask	255.255.255.0
Public IP Address	205.1.1.21
Public Netmask	255.255.255.128
Public Gateway	205.1.1.1
Enterprise SIP Server IP	205.3.3.48
Enterprise SIP Server Domain	avayalab.com
Enterprise SIP Server Transport	TCP

[◀ Previous Step](#)

[Next Step ▶](#)

A **Confirm Installation** screen is presented. After reading and heeding the Warning, click the **Accept** button if satisfied.

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook, 555-025-600*.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

Accept

Install

After clicking **Accept**, the screen is updated, and the **Install** button may be clicked to proceed.

Confirm Installation

The following optional fields have not been set

Secondary DNS

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook*, 555-025-600.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

[◀ Previous Step](#)

The Virtual Machine Management window, which had previously been at the “Wait for User to Complete Data Entry” step, has now continued, as shown in the abridged screen below.

Virtual Machine Management

Template Installation

Cancel Installation

Template Installation In Progress

Workflow Status						
Start Time	Task Description	State	% Complete	Estimate	Actual	
09:39:42	Download disk image for sbc	Complete	100	37s		✓
09:39:42	Download plugins for VMs	Complete	100	2s		✓
09:39:45	Check Template for Web Application	Complete	100	14s		✓
09:40:00	Download pre-install web application	Complete	100	0s		✓
09:40:00	Pre-Install Web Application Deployment	Complete	100	7s		✓
09:40:07	Wait For User To Complete Data Entry	Complete	100		26m 25s	✓
10:06:33	Undeploy Web Application	Complete	100	0s		✓

Wait for the “Finalize Installation” task to reach the “Complete” State, as shown below. This same information is available via the **View Install/Upgrade Log** link on the left (not shown).

09:40:07	Wait For User To Complete Data Entry	Complete	100	26m 25s	✓
10:06:33	Undeploy Web Application	Complete	100	0s	✓
10:06:34	Process EPW properties file if present	Complete	100	19s	✓
10:06:54	Configure Network	Complete	100	4s	✓
10:06:58	Install plugins	Complete	100	1s	✓
10:07:00	Install sbc	Complete	100	8m 11s	✓
10:15:11	Restart network	Complete	100	23s	✓
10:15:35	Start all VMs	Complete	100	13s	✓
10:15:49	Wait until system and all VMs are stabilised	Complete	100	40s	✓
10:16:30	Run post-install plugin if present - SBC:Creating SBC Configuration File - SBC:Checking ssh connection to SBC - SBC:Connecting to SBC web service - SBC:Can't connect, trying again - SBC:Connecting to SBC web service - SBC:Copying configuration file to SBC - SBC:Checking ssh connection to SBC - SBC:Connecting to SBC web service - SBC:Merging SBC configuration - SBC:Connecting to SBC web service - SBC:Saving SBC configuration file - SBC:Connecting to SBC web service - SBC:Restarting SBC - main: Wizard completed successfully	Complete	100	2m 20s	✓
10:18:50	Finalize Installation	Complete	100	15s	✓

Once the SBC template install has completed, select **Virtual Machine Management** on the left. Now, the **Virtual Machine List** shows that the SBC Template is installed.



The screenshot shows the 'Virtual Machine Management' section of a web interface. It includes a navigation menu on the left with 'Virtual Machine Management', 'Server Management', and 'User Administration'. The main content area displays the 'Virtual Machine List' with a system uptime of 10 days, 21 hours, 37 minutes, and 23 seconds. A 'Refresh' button is present next to the current template installed: SBCT 6.0.0.1.5 (sbc E362). Below this is a table listing the VMs:

Name	Version	IP Address	Maximum Memory	Maximum Virtual CPUs	CPU Time	State	Application State
✓ Domain-0	6.0.1.0.5	205.3.3.215	512.0 MB	16	13h 45m 35s	Running	N/A
✓ cdom	6.0.1.0.5	205.3.3.216	1024.0 MB	1	5h 22m 52s	Running	N/A
✓ sbc	E362	205.3.3.217	4.0 GB	4	1d 3h 21m 6s	Running	Running

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

6.2. Avaya Aura® SBC Licensing

After the Avaya Aura® SBC has been installed, the system can be licensed. The license, which is a function of the “box-identifier” shown in the output of the “show system-info” CLI command, can be obtained from an Avaya authorized representative. The procedures in this section assume the license file is available.

To log in, either select the wrench  [sbc](#) icon shown in the prior screen, or enter `https://<ip-addr>` where <ip-addr> is the management IP Address of the SBC. In the example configuration, the IP Address 205.3.3.217 can be used  <https://205.3.3.217>, to access a log in screen. Enter appropriate **Username** and **Password** and click **Login**.

Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name

Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Login"/>

The following shows an abridged screen after logging in. From the tabs available at the top, select the **Tools** tab.



Choose a tool to view from the left panel

From the menu on the left panel, select **Upload license file** as shown in the abridged menu below.

Tools

Update software

Retrieve license

Upload license file

The following screen shows the right panel after **Upload license file** has been selected on the left.

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Upload License File

You can upload a license file from your computer to Net-Net OS-E. You can optionally apply the license file immediately. Otherwise, the license file will not take effect until Net-Net OS-E is restarted.

BOX: 1

File: Browse...

Apply License

Upload

Use the **Browse...** button to select the location of the license file obtained from the Avaya authorized representative. Check the **Apply License** box. Click the **Upload** button.

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Upload License File

You can upload a license file from your computer to Net-Net OS-E. You can optionally apply the license file immediately. Otherwise, the license file will not take effect until Net-Net OS-E is restarted.

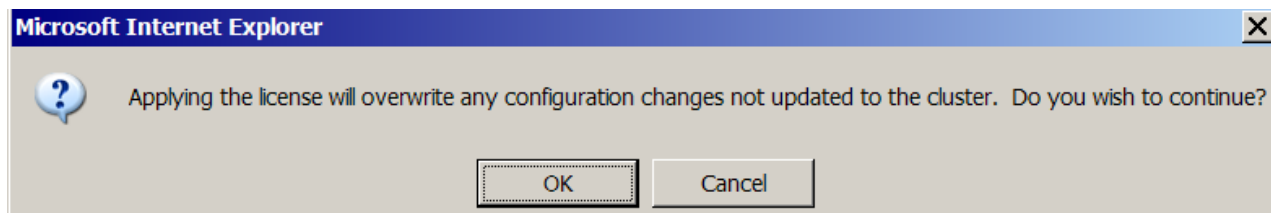
BOX: 1

File: Documents\License Files\wlm36227\license.xml Browse...

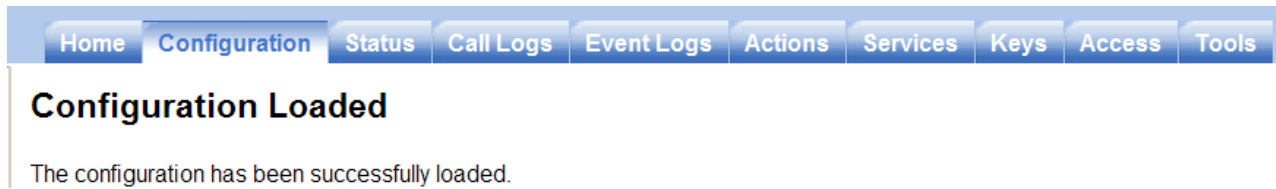
Apply License

Upload

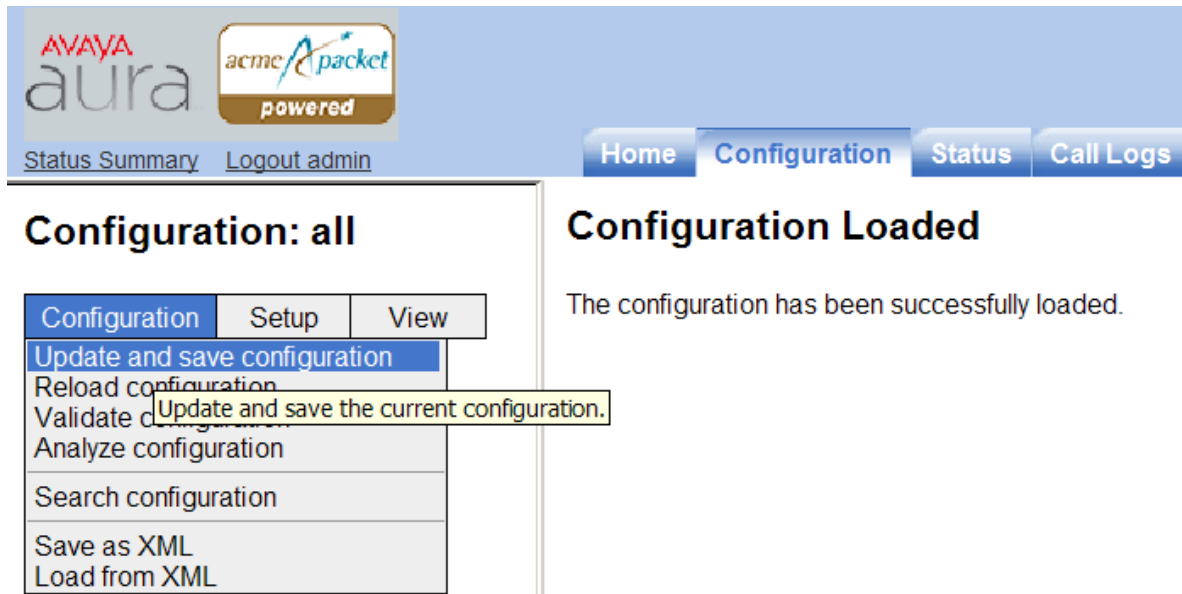
Heed the warning, and select **OK** if appropriate to proceed.



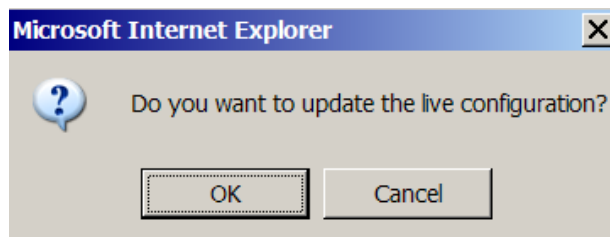
After the license has been successfully uploaded, select the **Configuration** tab as shown below.



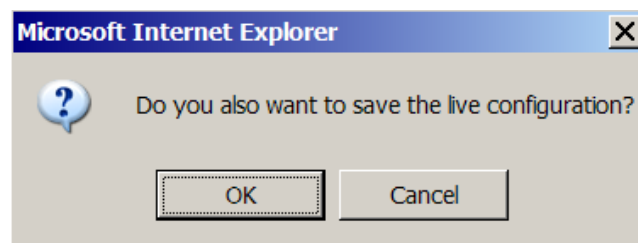
From the left, select **Configuration** → **Update and save configuration** as shown below.



Click **OK** to update the live configuration.



Click **OK** to save the live configuration.



Select the **Actions** tab as shown below.



Choose an action to invoke from the left panel

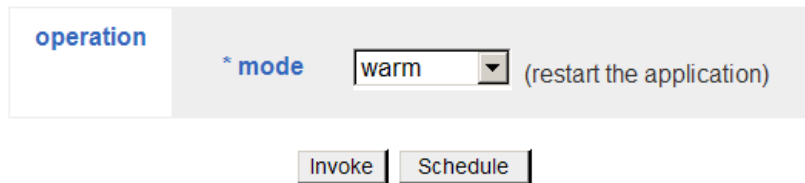
Scroll down the actions menu on the left and select **restart** as shown in the abridged screen below.

- ping
- playback
- presence
- presence-end-subscription
- presence-subscribe
- prune-assoc
- pt-script
- radius
- radius-authorize
- raid-check-consistency
- raid-set-adapter
- reg-lookup
- reg-lookup-detail
- registration
- remove-device
- restart

From the right panel, select “warm” from the **mode** drop-down menu, and click the **Invoke** button, as shown below.

restart

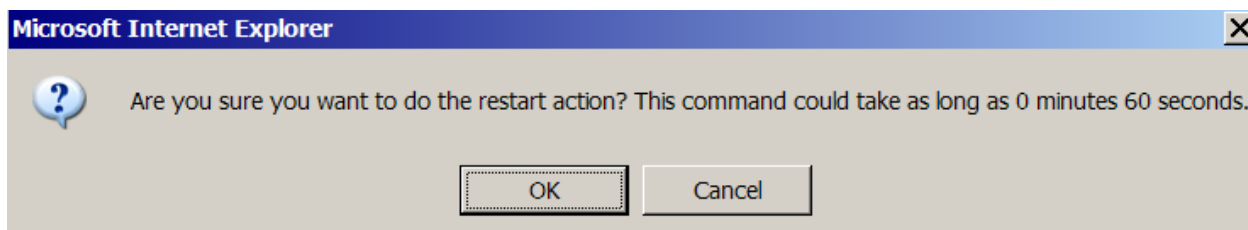
restart the Net-Net OS-E



operation * mode warm (restart the application)

Invoke Schedule

Select **OK** to proceed with the warm restart.



A screen such as the following will be displayed to show that the SBC is restarting. After the restart, the licensing procedure is complete. If further configuration is required, log back in, as described in the next section.



restart

restart the Net-Net OS-E

Net-Net OS-E is restarting...

6.3. Avaya Aura® SBC Element Manager Configuration

After the installation wizard is completed, subsequent configuration can be performed through the element manager of the SBC. The configuration screens will be familiar to the reader experienced with the Acme Packet Net-Net OS-E.

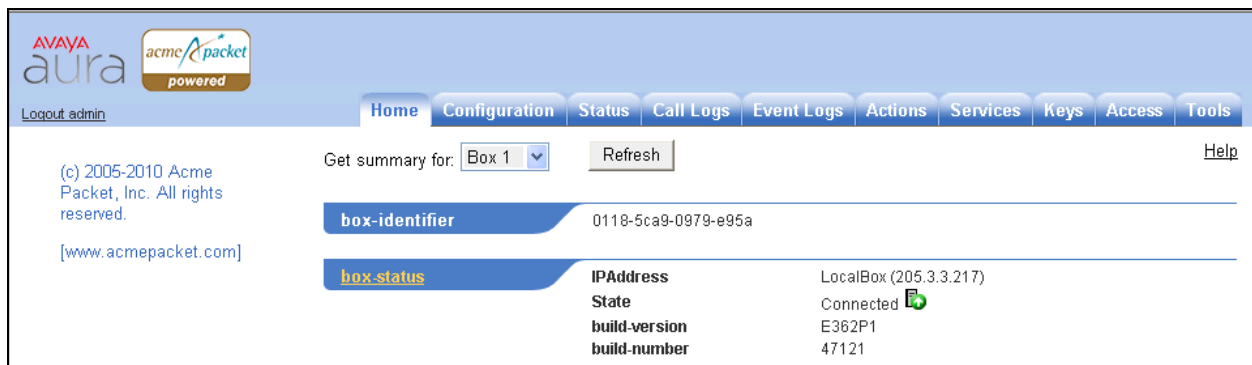
To log in, either select the wrench  [sbc](#) icon shown in the final screen in Section 6.1, or enter the `https://<ip-addr>` where `<ip-addr>` is the management IP Address of the SBC. In the example configuration, the IP Address 205.3.3.217 can be used  `https://205.3.3.217` to access a log in screen. Enter appropriate **Username** and **Password** and click **Login**.


Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name

Username:
Password:

The following shows an abridged **Home** screen after logging in. Note the tabs at the top.



box-identifier		0118-5ca9-0979-e95a
box-status		
IPAddress	LocalBox (205.3.3.217)	
State	Connected 	
build-version	E362P1	
build-number	47121	

6.3.1. Configuration of the CenturyLink SIP Signaling Port

Pre-GA versions of the configuration wizard did not allow the SIP signaling port to be configured to a port other than the default 5060. Although the version shown in these Application Notes allowed configuration of the SIP signaling port via the wizard, the information in this section is included in case the signaling port may need to be changed at any time. The following configuration should not be required using the GA version of the Avaya Aura® SBC.

Select the **Configuration** tab. Using the menu on the left hand side, expand **vsp** → **enterprise** → **servers** and click on **sip-gateway Telco**, as shown below.

- [-] vsp
 - [-] default-session-config
 - media
 - in-codec-preferences
 - out-codec-preferences
 - sip-directive
 - log-alert
 - [+] header-settings
 - third-party-call-control
 - [+] policies
 - [-] session-config-pool
 - [+] entry ToTelco
 - [-] entry ToPBX
 - to-uri-specification
 - request-uri-specification
 - [+] entry Discard
 - [+] dial-plan
 - [-] enterprise
 - [-] servers
 - [+] sip-gateway PBX
 - [+] sip-gateway Telco

Expand the **servers:** heading and select **Edit** for the “server_Telco1” entry corresponding to the CenturyLink network (i.e., host 64.1.1.157 in the screen below).

Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configure vspenterprise\servers\sip-gateway Telco [Help](#) [Index](#)

[Manage connections](#), [Log instant messages](#), [Record media](#), [Record files](#),
[Set up accounting](#), [Change "from:" URI](#), [Change "to:" URI](#)

general:

* name	<input type="text" value="Telco"/>
admin	<input type="button" value="enabled"/> (Resource is active)
domain	<input type="text"/>
failover-detection	<input type="button" value="ping"/> (Use OPTIONS to detect failures)

servers:

server	server	admin	host	transport	port	outbound-normalization	inbound-normalization
Edit Delete	server_Telco1	enabled	69.1.1.157	UDP	5060	Configure	Configure

[Add server](#)

After clicking **Edit**, in the **port** field enter the proper SIP signaling port used by the CenturyLink network. In the sample configuration, CenturyLink is expecting SIP signaling to UDP port 5060, as shown below. Click the **Set** button.

The screenshot shows the configuration page for a SIP gateway named 'Telco1'. The page has a navigation bar at the top with tabs for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. Below the navigation bar, the title is 'Configure vsp|enterprise|servers|sip-gateway Telco|server-pool|server Telco1'. There are buttons for 'Show advanced', 'Help', and 'Index'. Below these are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The main configuration area is titled 'General:' and contains the following fields:

* server-name	<input type="text" value="Telco1"/>
admin	<input type="button" value="enabled"/> (Resource is active)
* host	<input type="text" value="69.1.1.157"/> (host name or n.n.n.n)
transport	<input type="button" value="transport"/> <input type="button" value="UDP"/> (User Datagram Protocol)
port	<input type="text" value="5060"/> (at minimum 1, default=5060)

6.3.2. Quality Of Service (QoS) Markings for SIP Signaling

The procedure in this section is optional. The procedure can be used to achieve SIP signaling re-marking using the Avaya Aura® SBC.

The default QoS behavior after using the installation wizard will be to preserve the TOS values. That is, the TOS value received from the private side of the Avaya Aura® SBC will be transmitted to CenturyLink on the public side of the SBC. For example, for an outbound call to CenturyLink, if Avaya Aura® Session Manager sends a SIP INVITE to the Avaya Aura® SBC with a Differentiated Services Code Point (DSCP) value of 46, then the Avaya Aura® SBC will send a SIP INVITE to CenturyLink with a DSCP of 46. The following screen, accessible via **vsp → session-config-pool → entry ToTelco → sip-settings**, shows the settings as configured by the installation wizard. Note that the **outleg-tos** is set to “preserve”.

Configure vsp\session-config-poolentry ToTelco\sip-settings

Show advanced

[Help](#)

[Index](#)

Set

Reset

Back

Delete

general:

mode	auto-determine <input type="text"/>	(The Net-Net OS-E determines the mode, either back-to-back user agent or proxy.)
transport	transport any <input type="text"/>	(All protocol types)
port	directive auto-determine <input type="text"/>	(The Net-Net OS-E sets the SIP port.)

message-options:

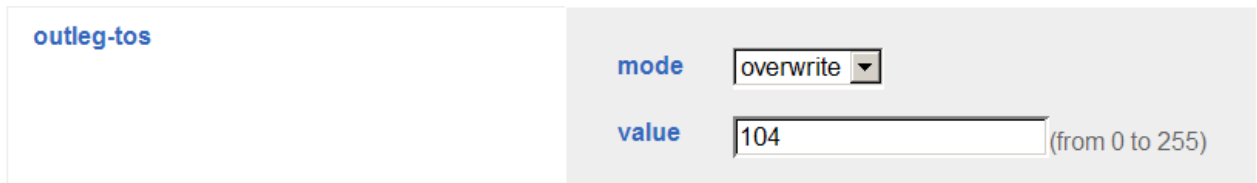
preserve-call-id	disabled <input type="text"/>	(Resource is inactive)
handle-3xx-locally	disabled <input type="text"/>	(Resource is inactive)
handle-3xx-locally-server-arbitration	disabled <input type="text"/>	(Resource is inactive)
handle-3xx-locally-lookup-original-invite	disabled <input type="text"/>	(Resource is inactive)
inleg-tos	mode preserve <input type="text"/>	
outleg-tos	mode preserve <input type="text"/>	

If it is desired to have the Avaya Aura® SBC re-mark SIP signaling to a different DSCP towards CenturyLink, the outleg-tos parameter can be changed. Select “overwrite” from the **outleg-tos mode** drop-down menu.



outleg-tos	mode <input type="text" value="preserve"/>
auto-accept-reinvite-with-no-sdp-on-in-leg	<input type="text" value="disabled"/> (Resource is inactive)

In the **value** field that appears after selecting “overwrite”, enter the decimal value corresponding to the byte containing the ToS field. For example, if the value is set to 104 (0x68) as shown below, the DSCP value 26 (0x1A) will be sent to CenturyLink (decoded by Wireshark as “Assured Forwarding 31”). Click the **Set** button. Proceed to save and activate the configuration as described in Section 6.4. If DSCP value 28 (0x1C) is desired (decoded by Wireshark as “Assured Forwarding 32”), then the **value** field can be set to 112.



outleg-tos	mode <input type="text" value="overwrite"/>
	value <input type="text" value="104"/> (from 0 to 255)

Proceed to save and activate the configuration as described in Section 6.4.

6.3.3. Disabling Third Party Call Control

The installation wizard for CenturyLink in the release documented in these Application Notes will enable the **admin** field for third party call control.

Navigate to **vsp** → **default-session-config** → **third-party-call-control**. As shown below, the installation wizard in the release covered by these Application Notes sets the **admin** field to enabled.

Configuration: all

Configuration Setup View

- cluster
 - box:AuraSBC
- vsp
 - default-session-config
 - media
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control
 - tls
 - session-config-pool
 - dial-plan
 - enterprise
 - dns

Configure vsp\default-session-config\third-party-call-control

Show advanced

Set Reset Back Delete

admin	enabled	(Resource is active)
status-events	both	(both call-legs)
handle-refer-locally	disabled	(Resource is inactive)
refer-maintain-identity	false	
ringback-file	<input type="text"/>	Browse System Files
busy-file	<input type="text"/>	Browse System Files

To disable third-party-call-control, select disabled from the **admin** drop-down and click **Set** as shown below.

Configure vsp\default-session-config\third-party-call-control

Show advanced

[Help](#) [Index](#)

Set Reset Back Delete

admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	disabled	(Resource is inactive)

After disabling, the third-party-call-control link becomes red as shown below.

Configuration: all

Configuration Setup View

- cluster
 - box:AuraSBC
- vsp
 - default-session-config
 - media
 - sip-directive
 - log-alert
 - header-settings
 - third-party-call-control

Configure vsp\default-session-config\third-party-call-control

Show advanced

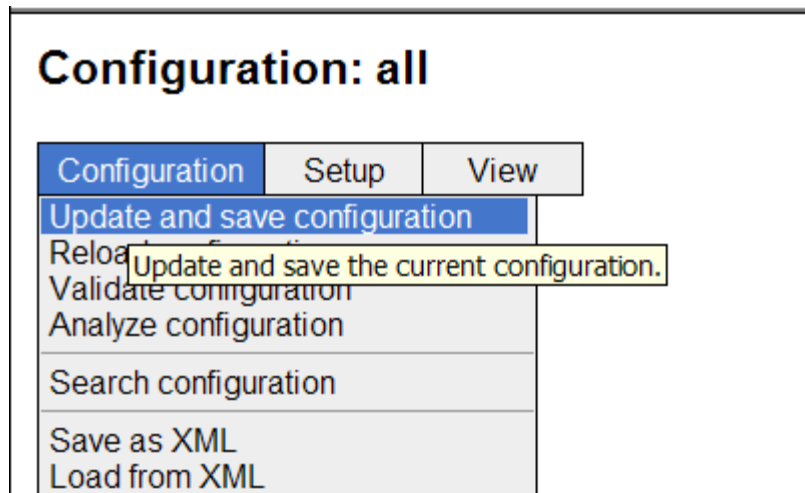
Set Reset Back Delete

admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	disabled	(Resource is inactive)
refer-maintain-identity	false	

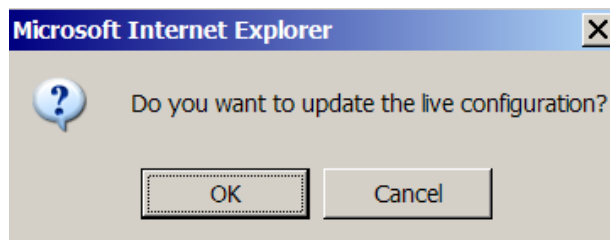
Proceed to save and activate the configuration as described in **Section 6.4**.

6.4. Saving and Activating Configuration Changes

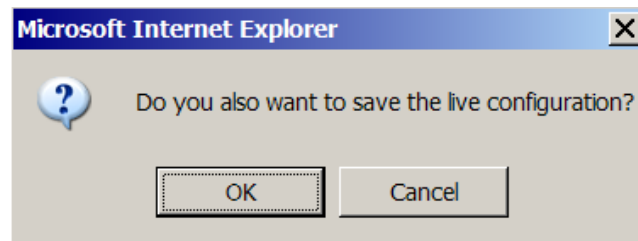
To save and activate configuration changes, select **Configuration** → **Update and save configuration** from the upper left hand side of the user interface, as shown below.



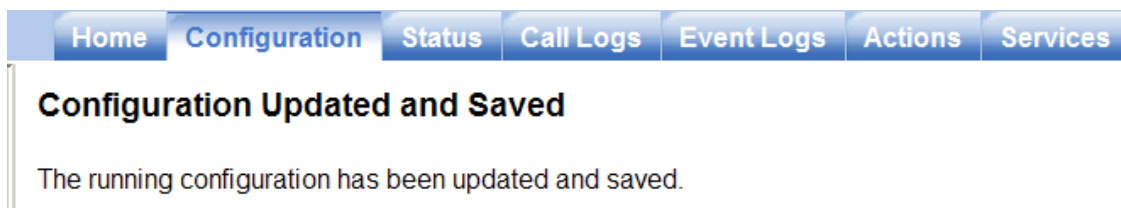
Click **OK** to update the live configuration.



Click **OK** to save the live configuration.



A screen that includes the following should appear.



7. CenturyLink SIP Trunking Configuration

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

During the signup process, CenturyLink will require that the customer provide the public IP address used to reach the SBC at the edge of the enterprise. CenturyLink will provide the IP address of the CenturyLink SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the Communication Manager and the SBC configuration discussed in the previous sections. The configuration between CenturyLink and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the CenturyLink network.

8. Verification Steps

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

Verification Steps:

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

Troubleshooting commands on Communication Manager:

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

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager and the Avaya Aura® Session Border Controller to CenturyLink SIP Trunking. CenturyLink SIP Trunking is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. CenturyLink SIP Trunking provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. CenturyLink SIP Trunking passed compliance testing. Please refer to **Section 2.2** 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*, Release 6.0, June 2010, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.0, August 2010, Document Number 555-245-205.
- [3] *4600 Series IP Telephone LAN Administrator Guide*, October 2007, Document Number 555-233-507.
- [4] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [5] *Avaya one-X® Communicator Getting Started*, August 2010.
- [6] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [7] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [8] RFC 4244, *An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>
- [9] *Modular Messaging Admin Guide Release 5.2 with Avaya MSS*, August 2011.

©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.