Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura™ Communication Manager 5.2.1 with Avaya Aura™ Session Border Controller 6.0 for Gamma Telecom "IP Direct Connect" SIP Trunks - Issue 1.0

Abstract

These Application Notes describe the procedure to configure an Enterprise network consisting of Avaya Aura™ Communication Manager and Avaya Aura™ Session Border Controller 6.0 to interoperate with the "IP Direct Connect" SIP Trunks offering from Gamma Telecom.

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

1. Introduction

These Application Notes present a sample configuration for an Enterprise network centered on Avaya Aura™ Communication Manager using Avaya Aura^{TM} Session Border Controller to access the SIP trunking solution IP Direct Connect offered by Gamma Telecom. This solution allows an Avaya Enterprise network access to PSTN, Mobile phones and other SIP Trunk customers. An Enterprise customer with an Avaya SIP-based solution can subscribe to a network-based IP communication service from a SIP Trunking Service Provider that supports SIP-to-PSTN calls to reduce their long distance and interconnection costs. To accomplish this, customers interconnect their Avaya Aura^{TM} Communication Manager with Avaya Aura^{TM} Session Border Controller. Call will be signaled from/to Gamma Telecom's IP network via the Public Internet (or other forms of IP connectivity) and use SIP transport to establish calls to the PSTN. Calls from the customer site to the PSTN transit the Gamma Telecom where a SIP proxy server and SIP-to-PSTN gateway usually resides. As shown in **Figure 1**, the Avaya Enterprise network uses SIP trunking for call signaling with Gamma'sSession Border Controller resident within the Gamma Telecom infrastructure. The Avaya Aura™ Session Border Controller provides topology hiding without the need for Network Address Translation (NAT), SIP header manipulation and SIP signaling and media channel conversion services.

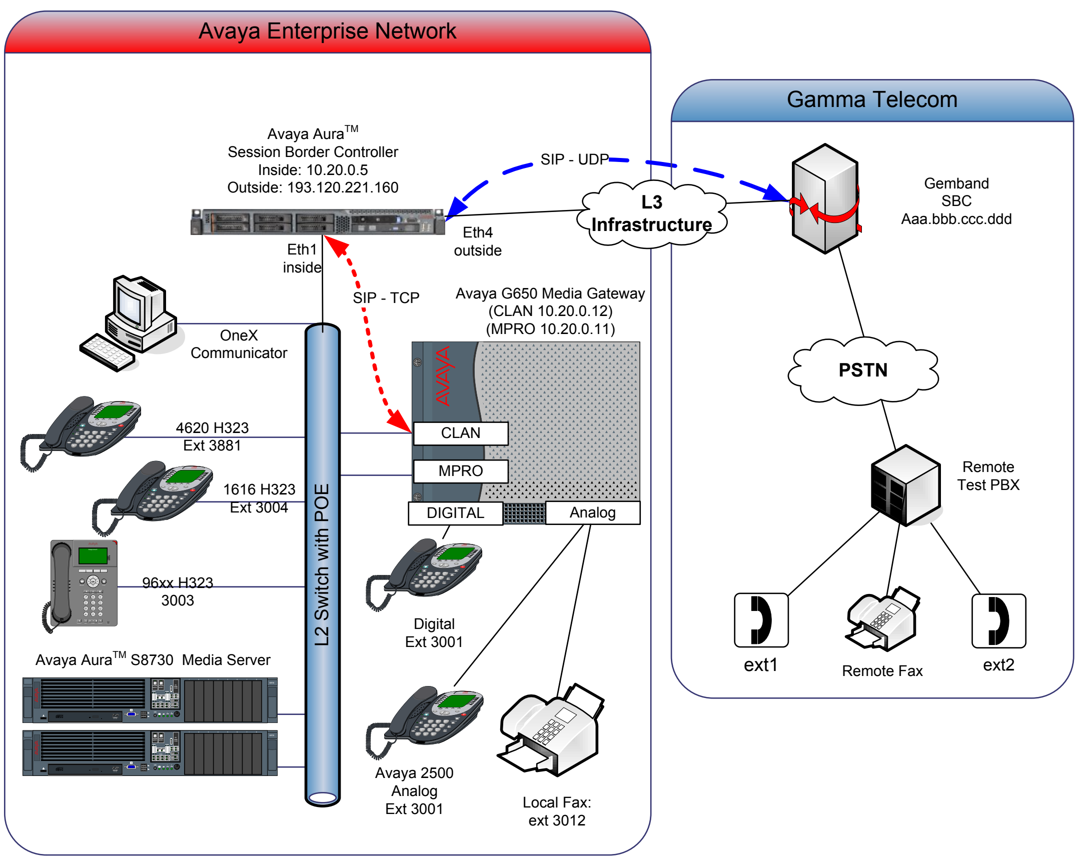


Figure 1: Sample configuration for Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} Session Border Controller with Gamma Telecom IP Direct Connect SIP Trunking

The Avaya Aura™ Session Border Controller acts as a peering host between the public Internet and the private enterprise network and provides Denial-of-Service (DoS), packet filtering and topology hiding without the need for an additional firewall or intrusion prevention system (IPS) on either the public or private side of the Avaya Aura™ Session Border Controller. Although the Avaya Aura™ Session Border Controller can be configured to provide intelligent call routing decisions, no dial-plan was provisioned on the Avaya Aura™ Session Border Controller in the sample configuration as all the call routing and number modification logic is achieved by Avaya Aura™ Communication Manager. Avaya Aura™ Session Border Controller acts as a Back-to-Back User Agent (B2BUA) for SIP calls. NAT is no longer required as the Avaya Aura™ Session Border Controller terminates and re-originates calls using its own IP addresses thereby hiding the IP address range (topology) of the private network. Network security is provided by the DoS and packet filtering module of the Avaya Aura™ Session Border Controller. The Avaya Aura™ Session Border Controller converts the SIP signaling channel from UDP to TCP for inbound and vice-versa for outbound calls. For the sample configuration shown in **Figure 1,** Avaya Aura™ Communication Manager 5.2.1 runs on an Avaya S8730 Server with an Avaya G650 Media Gateway and Avaya Aura™ Session Border Controller 6.0 runs on an Avaya Aura™ System Platform on an Avaya S8800 server. 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 Avaya Aura™ Session Border Controller. The port labeled "4" (virtual "eth2") is used for the public (outside) network interface of the Avaya Aura™ Session Border Controller. For the Avaya Aura™ Communication Manager, the results in these Application Notes are applicable to other Avaya Aura™ Communication Manager Server and Media Gateway combinations. These Application Notes will focus on the configuration of the SIP trunks and call routing. Detailed administration of the endpoint telephones will not be described. Refer to the appropriate documentation in **Section 8**.

1.1. Interoperability Compliance Testing

The primary focus of testing is to verify SIP trunking interoperability between an Avaya SIP-based network and Gamma Telecom's voice over IP network. Test cases are selected to exercise a sufficiently broad segment of functionality to have a reasonable expectation of interoperability in production configurations.

Basic Interoperability:

- PSTN calls delivered via the Service Provider's SIP trunking to an Avaya IP telephony solution
- PSTN calls sent via a Service Provider's SIP trunking from an Avaya IP telephony solution
- Calling with various Avaya telephone models including IP models as well as traditional analog and digital TDM phones
- Verify G.711a and G.729a support
- Various PTSN dialing plans including national and international calling, toll-free, operator, directory assistance and direct inward dialed calling
- SIP transport using UDP

Advanced Interoperability:

- Codec negotiation
- Telephony supplementary features, such as Hold, Call Transfer, Conference Calling and Call Forwarding
- DTMF Tone Support
- Voicemail Coverage and Retrieval
- Direct IP-to-IP Media (also known as "Shuffling") over SIP Trunk. Direct IP-to-IP media allows compatible phones to reconfigure the RTP path after call establishment directly between the Avaya phones and the Service Provider and release media processing resources on the Avaya Media Gateway
- EC500 for Avaya Aura^{TM} Communication Manager

1.2. Support

Technical Support on SIP Trunk offering from Gamma Telecom can be obtained through the following phone contacts:

- +44(0) 808 178 8000

2. Equipment and Software Validated

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

Avaya Product / Hardware Platform	Software Version
Avaya S8800 Server	Avaya Aura™ Session Border Controller – R6.0.0.1.4
Avaya S8730 Server	Avaya Aura ™ Communication Manager Access Element 5.2.1 SP 4 R015x.02.1.016.4 – patch 18250
Avaya G650 Media Gateway • IPSI (TN2312BP) • C-LAN (TN799DP) • IP Media Resource 320 (TN2602AP) • Analog (TN2793B) • Digital line (TN2214CP)	 • TN2312BP HW28 FW051 • TN799DP HW01 FW038 • TN2602AP HW08 FW055 • TN2793B 000005 • TN2214CP HW10
Avaya Telephones: • 9620/9630 (H323) • 1616 (H323) • 4621 (H323) • Avaya Digital Telephones (2420) • Avaya Analog (2500)	• Release 3.1 • Release 1.3 • Release R2.9 SP1 • N/A • N/A
Avaya One-X® Communicator (H.323)	Release 5.2.0.14
Canon Fax JX500	-
Gamma Telecom	
GENBAND S3 Session Border Controller	Firmware 4.3

3. Configure Avaya Aura™ Communication Manager

This section provides the procedures for configuring Communication Manager with SIP trunking with the Session Border Controller. The procedures include the following areas:

- Verify Avaya Aura™ Communication Manager License
- Configure IP Node Names
- Verify/List IP Interfaces
- Configure IP Codec Set
- Configure IP Network Region and IP Network Map
- Administer SIP Trunk with Avaya Aura™ Session Border Controller
- Configure Route Pattern
- Configure Public Unknown Numbering
- Configure Incoming Call Handling treatment
- Administer ARS Analysis
- Save Translations

Throughout this section the administration of Communication Manager is performed using a System Access Terminal (SAT). The following commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity. These instructions assume that the Communication Manager has been installed, configured, licensed and provided with a functional dial plan. Refer to the appropriate documentation as described in **Reference [1]** and **[2]** for more details**.** In these Application Notes Communication Manager was configured with 4 digit extention **30xx** for stations. Diaplan analysis can be verified with the **display dialplan analysis** command.

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

       Dialed   Total  Call    Dialed   Total  Call     Dialed   Total  Call
       String   Length Type    String   Length Type     String   Length Type
     30           4    ext
     8            3    dac
     9            1    fac
```

Other numbers on PSTN (accessible from the SIP trunk offering) are reachable via **ars** table with the use of **feature access code 9**.

3.1. Verify Avaya Aura™ Communication Manager License

Use the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections. Verify highlighted value, as shown below.

```
display system-parameters customer-options                     Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 100    0
           Maximum Concurrently Registered IP Stations: 18000  2
             Maximum Administered Remote Office Trunks: 0      0
Maximum Concurrently Registered Remote Office Stations: 0      0
              Maximum Concurrently Registered IP eCons: 0      0
  Max Concur Registered Unauthenticated H.323 Stations: 100    0
                        Maximum Video Capable Stations: 100    0
                   Maximum Video Capable IP Softphones: 100    9
                       Maximum Administered SIP Trunks: 1000   300
```

If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an authorized Avaya Sales representative to make the appropriate changes.

3.2. Configure IP Node Names

As SIP interaction with Service Provider is mediated by Session Border Controller, the node-name table in Communication Manager is populated with the IP address of the inside inteface of the Session Border Controller. Use the **change node-names ip** command to add the **Name** and **IP Address** for the Session Border Controller, in the example **AuraSBC-Inside** and **10.20.0.5** was used.

```
change node-names ip                                           Page   1 of   2
                                IP NODE NAMES
    Name              IP Address
AuraSBC-Inside      10.20.0.5
Gateway-private     10.20.0.1
clan-1              10.20.0.12
mpro-1              10.20.0.11
procr               0.0.0.0
```

Note: In the example some other values (CLAN, MedPro) have been already created as per installation and configuration of Communication Manager.

3.3. Verify/List IP Interfaces

Use the **list ip-interface all** command and note the **C-LAN** to be used for SIP trunks between the Communication Manager and the Session Border Cotroller.

```
list ip-interface all
                                IP INTERFACES
                                                                       Net
ON Type   Slot  Code/Sfx    Node Name/       Mask  Gateway Node      Rgn VLAN
                            IP-Address
-- ------ ----- --------    ---------------  ----  ---------------   ---  ----
 y C-LAN  01A10 TN799  D      clan-1           /24   Gateway-private  2    n
                              10.20.0.12
 y MEDPRO 01A11 TN2602        mpro-1           /24   Gateway-private  2    n
                              10.20.0.11
```

3.4. Configure IP Codec Set

Configure the list of codecs with the ones supported by the Service Provider. Use the **change ip-codec-set n** command where **n** is codec set used in the configuration. In the following example two codecs are made available for the media negotiation: G.711A and G.729. Configure the IP Codec Set as follows:

- **Audio Codec** Set **G.729**
- **Audio Codec** Set **G.711A**

Retain the default values for the remaining fields.

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

    Codec Set: 2

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

If T.38 Fax is supported by Service Provider, to configure fax support, navigate to **Page 2** and change **FAX** to **t.38-standard.** Use default values for all other fields. Submit these changes.

```
change ip-codec-set 2                                              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
```

3.5. Configure IP Network Region and IP Network Map

Use the **change ip-network-region n** command where **n** is the number of the network region used by the Enterprise. Set the **Intra-region IP-IP Direct Audio** field to **yes**. For the **Codec Set,** enter the corresponding audio codec set configured in **Section 3.4** i.e. **2**. Set the **Authoritative Domain** to the SIP domain, **avaya.com**. Retain the default values for the remaining fields and submit these changes.

Note: In the test configuration, **network region 2** was used. If a new network region is needed or an existing one is modified, ensure to configure it with the correct parameters.

```
change ip-network-region 2                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name: inside
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
```

Use the **command change ip-network-map** to specify the ip networks to be mapped with the **ip-network-region** in use for the Enterprise.

- **IP Address FROM:** the beginning of the address range i.e. **10.20.0.0**
- **IP Address TO:** the end of the address range i.e. **10.20.0.255**
- **Subnet Bits:** Number of bits to identify the subnet i.e. **24**
- **Network Region:** The network region in use in the enterprise i.e. **2**

```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING

                                             Subnet Network     Emergency
IP Address                                   Bits   Region VLAN Location Ext
--------------------------------------------- ------ ------ ---- ------------
FROM: 10.20.0.0                               /24    2      n
  TO: 10.20.0.255
FROM:                                         /             n
  TO:
```

3.6. Administer SIP Trunks with Avaya Aura™ Session Border Controller

To administer a SIP Trunk on Communication Manger, two steps are required, creation of a signaling group and trunk group.

3.6.1. Add SIP Signaling Group for Service Provider

Use the **add signaling-group n** command, where **n** is an available signaling group number, for one of the SIP trunks to the Session Border Controller, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** **sip**
- **Transport Method:** **tcp**
- **Near-end Node Name:** C-LAN node name from **Section 3.2** (i.e., **clan-1**)
- **Far-end Node Name:** Session Border Controller node name from **Section 3.2** (i.e., **AuraSBC-Inside**)
- **Near-end Listen Port:** **5060**
- **Far-end Listen Port:** **5060**
- **Far-end Domain:** Leave it blank
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connections:** **y**

```
add signaling-group 6                                           Page   1 of   1
                                SIGNALING GROUP
Group Number: 6              Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n
     IP Video? n

 Near-end Node Name: clan-1              Far-end Node Name: AuraSBC-Inside
 Near-end Listen Port: 5060              Far-end Listen Port: 5060
                                      Far-end Network Region: 2
Far-end Domain:

                                           Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload          Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                   IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

3.6.2. Configure a SIP Trunk Group for Service Provider

Add the corresponding trunk group controlled by this signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** **sip**
- **Group Name:** A descriptive name (i.e**. OUTSIDE CALL**)
- **TAC:** An available trunk access code (i.e. **806**)
- **Service Type:** Select the proper type of service between **public-ntwrk** or **tie**.
- **Signaling Group:** Number of the signaling group added in **Section 3.6.1** (i.e. **6**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to Session Border Controller (must be within the limits of the total trunks available from licensed verified in **Section 3.1**)

Note: The number of members determines how many simulataneous calls can be processed by the trunk through Session Border Controller.

```
add trunk-group 6                                               Page   1 of  21
                                TRUNK GROUP

Group Number: 6                    Group Type: sip           CDR Reports: y
  Group Name: OUTSIDE CALL                COR: 1        TN: 1        TAC: 806
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n

                                                    Signaling Group: 6
                                                  Number of Members: 100
```

Navigate to **Page 3** and change **Numbering Format** to **public.** Use default values for all other fields. Submit these changes.

```
add trunk-group 6                                               Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                     Maintenance Tests? y

                     Numbering Format: public
                                              UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n
```

3.7. Configure Route Patterns

Configure a route pattern for the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. When changing the route pattern, enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name:** A descriptive name (i.e., **toAuraSBC**)
- **Grp No:** The trunk group number from **Section 3.6.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

```
change route-pattern 6                                          Page   1 of   3
                    Pattern Number: 6   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: 6    0                                                            n   user
 2:                                                                   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            unre                                      none
 2: y y y y y n  n            rest                                      none
```

3.8. Configure Public Unknown Numbering

Use the **change public-unknown-numbering 0** command to assign number presented by Communication Manager when a call is signaled to the Session Border Controller. Add an entry for the Extensions configured in the dialplan. Enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Ext Len:** Number of digits of the Extension i.e. **4**
- **Ext. Code:** Digits beginning the Extension number, i.e. **30**
- **Trk Group:** Trunk number configured in **Section 3.6.2** i.e. **6**
- **CPN Prefix:** Number to be prepend to extension number, as assigned by the Service Provider i.e. **0130677076**
- **Total CPN Len** Number of digits i.e. **11**

```
change public-unknown-numbering 0                                 Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                  Total Administered: 1
 4  30              6         0130677076      11        Maximum Entries: 9999
```

3.9. Configure Incoming Call Handling treatment

Use the **change inc-call-handling-trmt trunk-group n** (where n is the trunk group defined in **Section 3.6.2**) command to map the number requested in an incoming call from the Service Provider to a Communication Manager extension. Enter the following values for the specified fields, and retain default values for the remaining fields. Submit these changes.

- **Number Len:** Number of digits i.e. **11**
- **Number Digits:** Digits at beginning of the number to be matched i.e. **0130677076**
- **Del:** Number of digits to be removed i.e. **10**
- **Insert** Digits to insert at the beginning of the dialed number to make the extention

```
change inc-call-handling-trmt trunk-group 6                      Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len     Digits
public-ntwrk    11 0130677076       10  300
```

3.10. Administer ARS Analysis

This section provides sample Automatic Route Selection (ARS) used for routing calls with dialed digits beginning with **0** corresponding to national numbers accessible via the Service Provider. Use the **change ars analysis 0** command and add an entry to specify how to route the calls. Enter the following values for the specified fields and retain the default values for the remaining fields. Submit these changes.

- **Dialed String:** Dialed prefix digits to match on, in this case **0**
- **Total Min:** Minimum number of digits, in this case **3**
- **Total Max:** Maximum number of digits, in this case **25**
- **Route Pattern:** The route pattern number from **Section 3.7** i.e. **6**
- **Call Type:** **pubu**

Note: Additional entries may be added for different number destinations.

```
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             3    25     6        pubu          n
```

3.11. Save Translations

Configuration of Communication Manager is complete. Use the **save translations** command to save these changes.

4. Install and Configure Avaya Aura™ Session Border Controller

This section provides the procedures for installing and configuring the Session Border Controller, assuming that System Platform has been installed as described in **Reference [5]** on the Avaya S8800 Server.

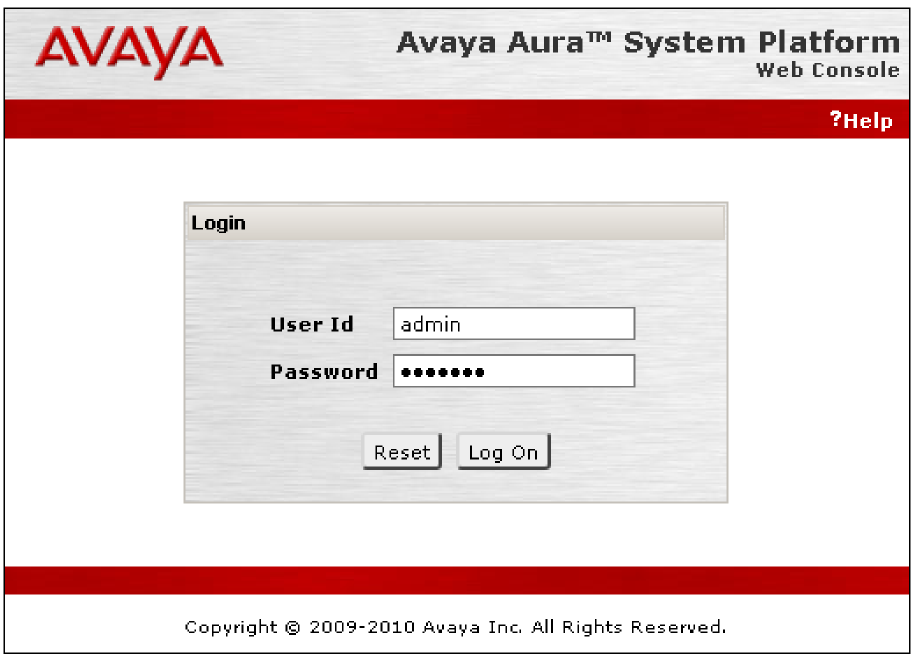
4.1. Installation of Avaya Aura™ Session Boarder Controller

The installation consists of the following steps:

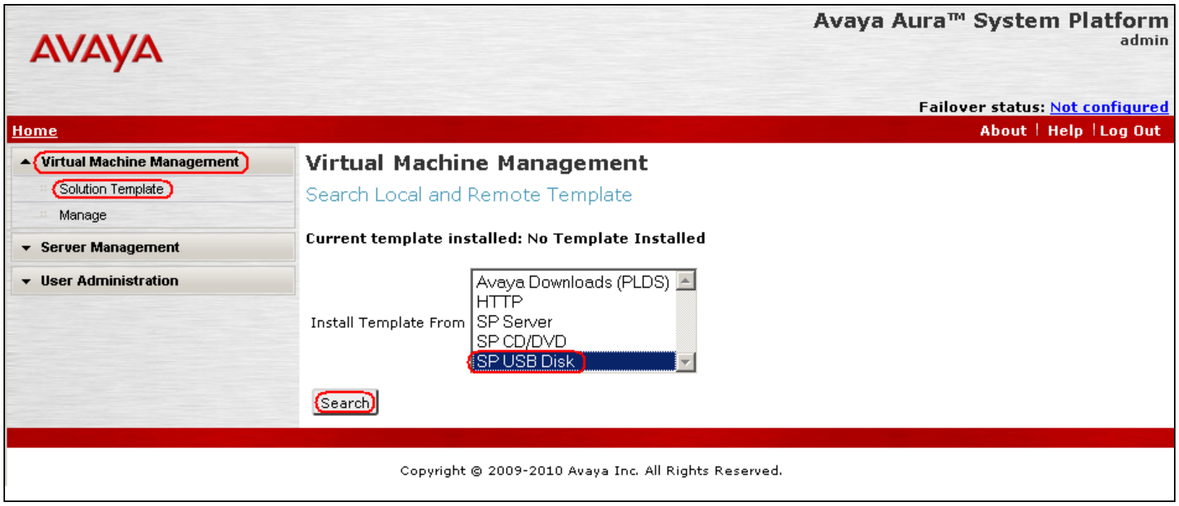
- Virtual Machine Template Installation
- Initial Configuration of the Virtual Machine Template
- Template Deployment

4.1.1. Virtual Machine Template Installation

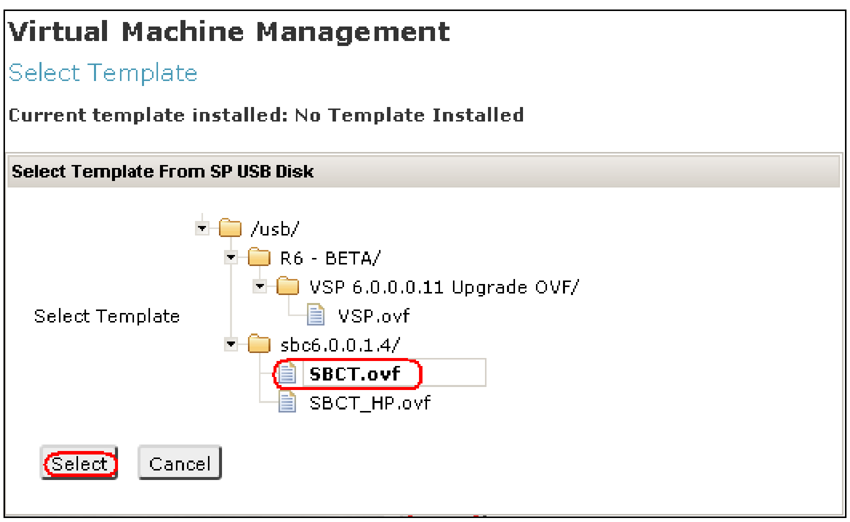
Installation is accomplished by accessing the browser-based GUI of System Platform using the URL "**https://<ip-address>**", where "<ip-address>" is the IP address of Console Domain. Log in with the appropriate credentials, as shown in the picture below.



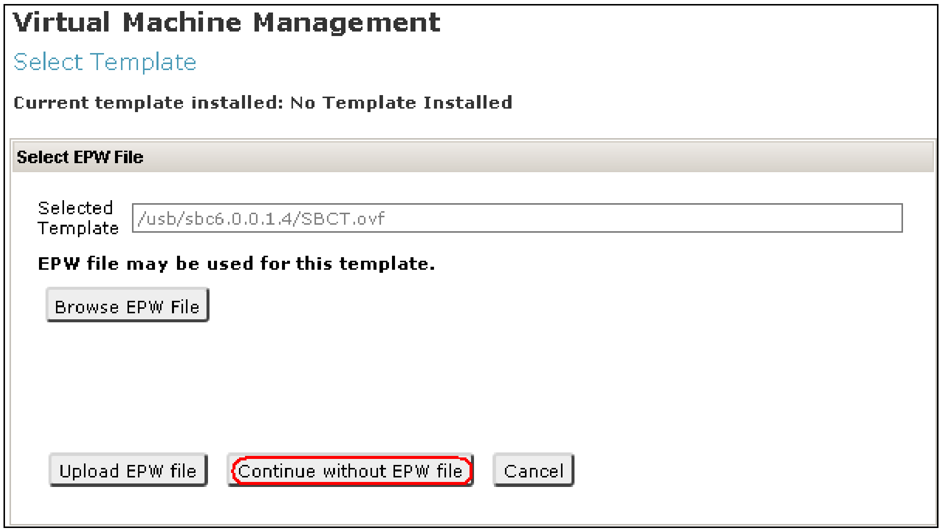
After logging in, expand the menu on the left hand side of the page, **Virtual Machine Management** and select **Solution Template** A list of possible sources for the new template to be deployed is presented, select the appropriate one (in these Application Notes installation from **USB Disk** was used, other installation methods may be used). Click on the **Search** button. The diagram below illustrates the process.



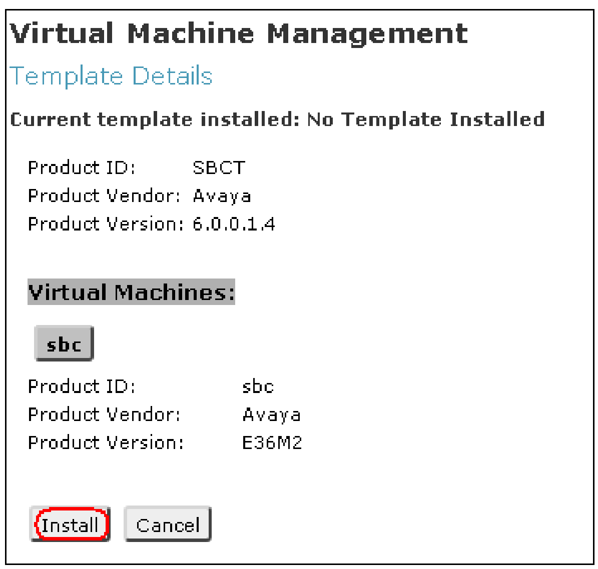
A directory listing will be presented. Expand the directory hierarchy to locate the Solution Template to be installed: select by clicking on the file name (i.e. **SBCT.ovf**) and then clicking on the **Select** button, as shown in the diagram below.



The installer will prompt for EPW file, if it is not available click on **Continue without EPW file** button as shown in the diagram below.

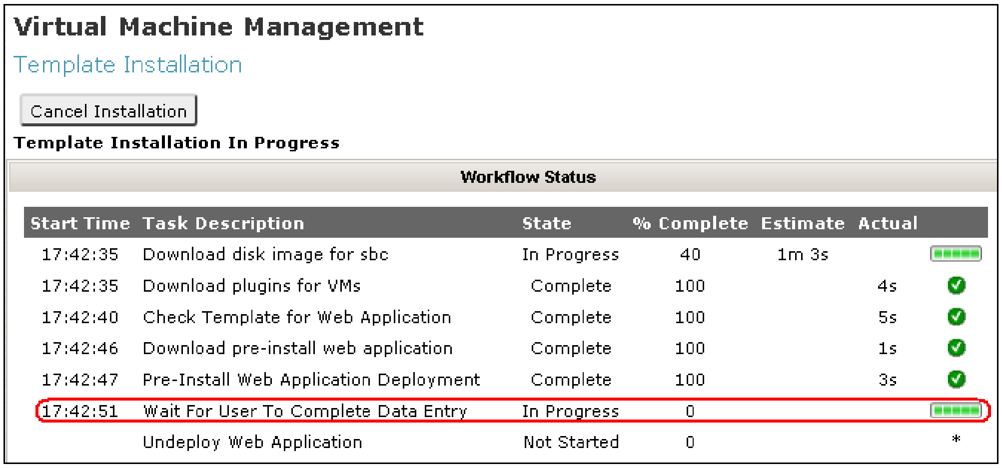


The installer will summarize the new virtual machine properties, to progress with the installation click on **Install** button.

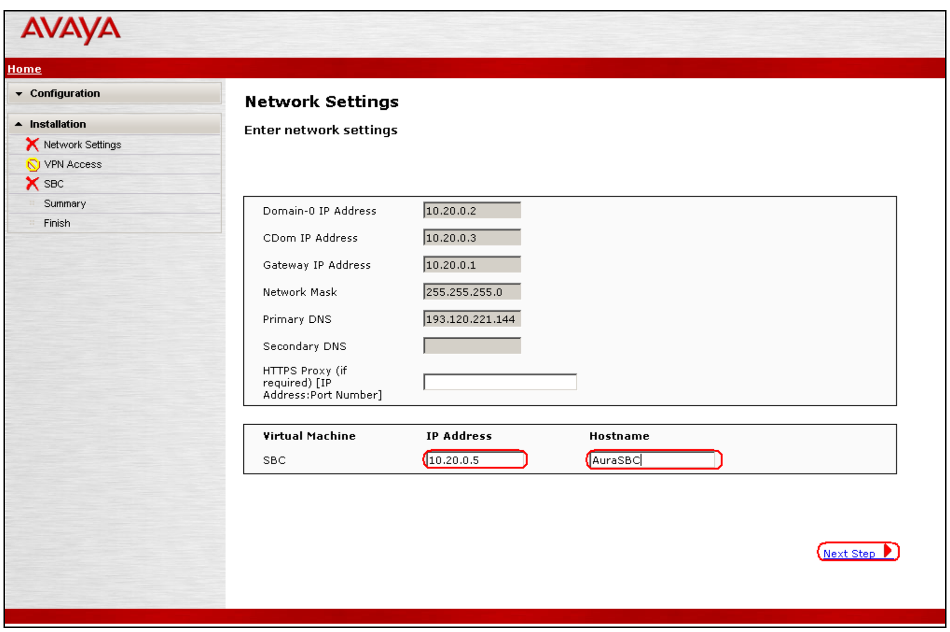


4.1.2. Initial Configuration of the Virtual Machine Template

Once the installation process has started, the installer will progress presenting a workflow report, and when reaching the step "**Wait For User To Complete Data Entry**", the installer will attempt launching a pop-up window to gather the configuration information. If pop-up blocker is enabled in the browser is enabled, disable it in order to access the configuration window. The figure below illustrates the workflow report.



On the new window, specify **IP Address** for the Inside interface (i.e. **10.20.0.5**) and **Hostname** (i.e. **AuraSBC**). Click on **Next Step** to progress with the configuration.



The installer (not shown) will prompt for enabling VPN Access from underlying System Platform. Select **No** if not required. Click on **Next Step** to advance in the configuration.

In the next screen the configuration wizard will prompt for Session Border Controller Data. Fill all the sections of the form.

Under: SIP Service Provider Data

- **Service Provider:** Select from the drop down list a Service Provider template configuration, (i.e. **AT&T**)
- **IP Address:** The IP address of the Signalling interface offered by Gamma Telecom (i.e. **83.245.6.117**)
- **Port:** Enter the Port number for the signaling interface with the Service Provider (i.e. **5060**)
- **Media Network:** The network used by Service Provider for rtp-media (i.e. **83.245.6.117**)
- **Media Netmask:** The net mask used by Service Provider (i.e. **255.255.255.0**)

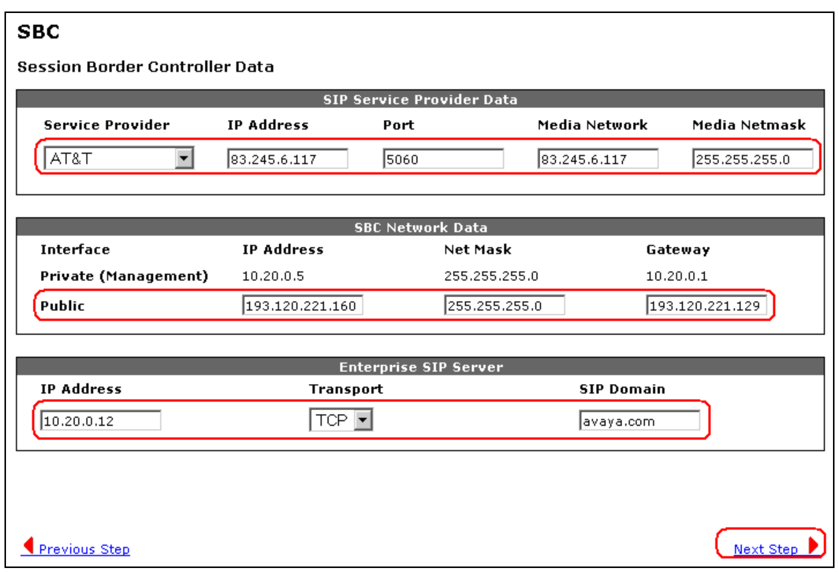
Under: SBC Network Data / Public

- **IP Address:** The IP Address of the outside interface used by SBC for signalling and media with the sip Provider (i.e.**193.120.221.160**)
- **Net Mask:** The net mask for the outside interface (i.e. **255.255.255.0**)
- **Gateway:** The default gateway on the outside interface (i.e. **193.120.221.129**)

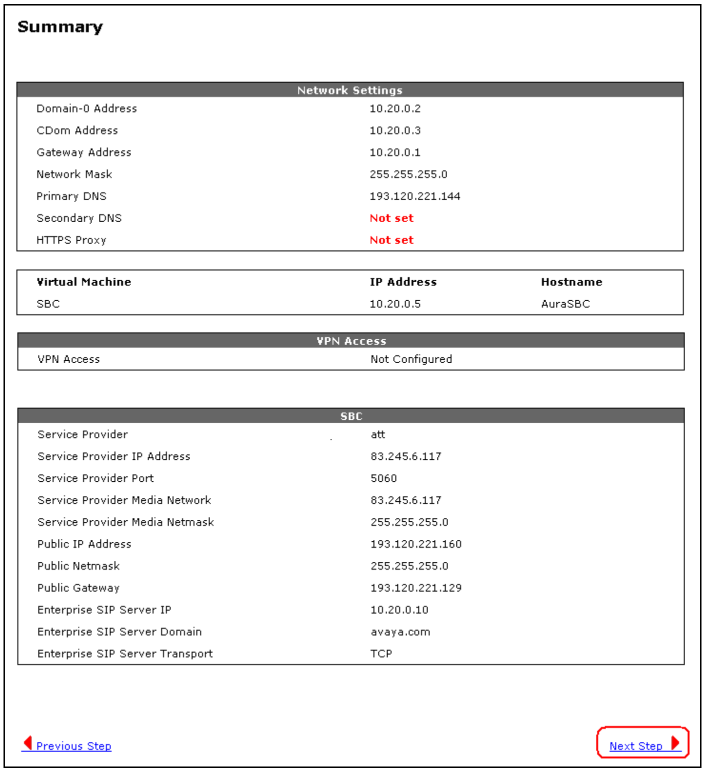
Under: Enterprise SIP Server

- **IP Address:** The IP Address of the signalling interface on Communication Manager, in these Application Notes the CLAN interface is used
- **Transport:** Select from the drop down list, the transport to be used for signalling calls with Communication Manager, as configured in **Section 3.6.1**, i.e. **TCP**
- **SIP Domain:** The SIP domain configured **Section 3.5** (i.e. **avaya.com**)

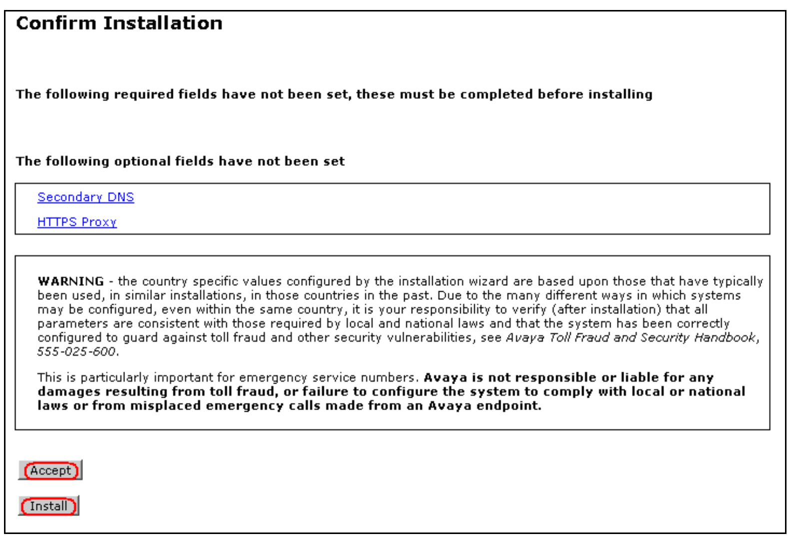
Click on **Next Step**. The diagram below illustrates the configuration used in these Application Notes.



The configuration wizard offers the opportunity to review the configuration entered in a **Summary** page as illustrated below. Click on **Next Step** to advance with the installation or navigate back with the **Previous Step** link.



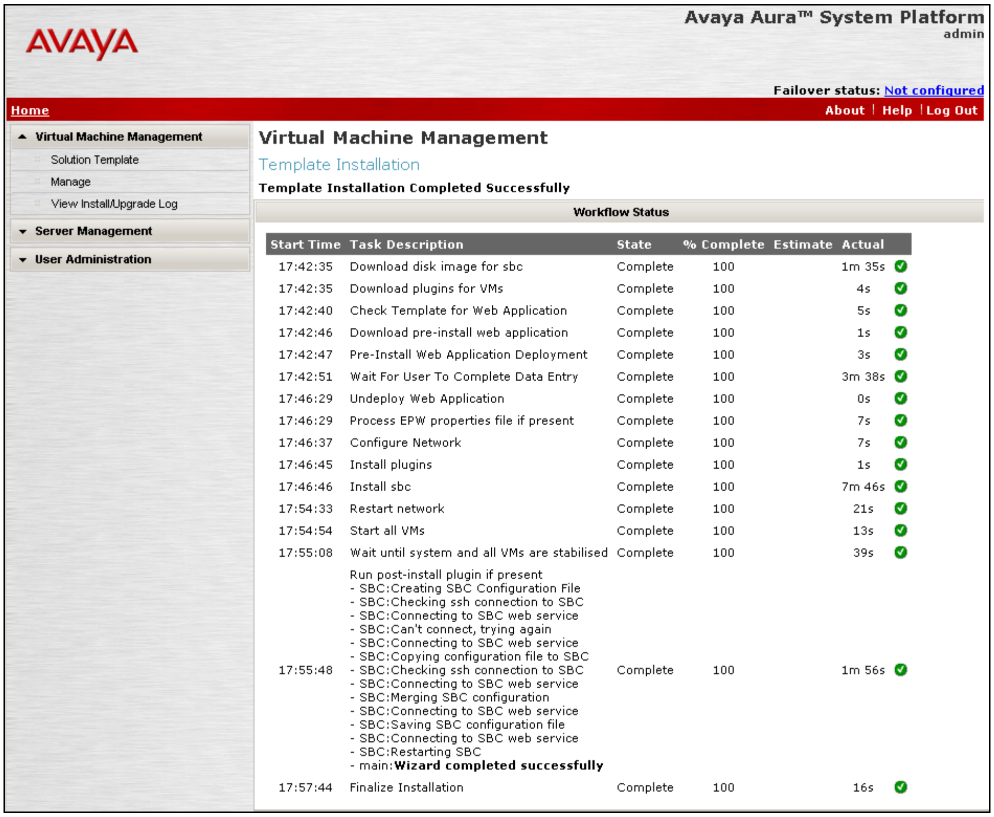
A **Confirm Installation** screen is presented by the wizard, click on **Accept** and then **Install** to proceed with the installation.



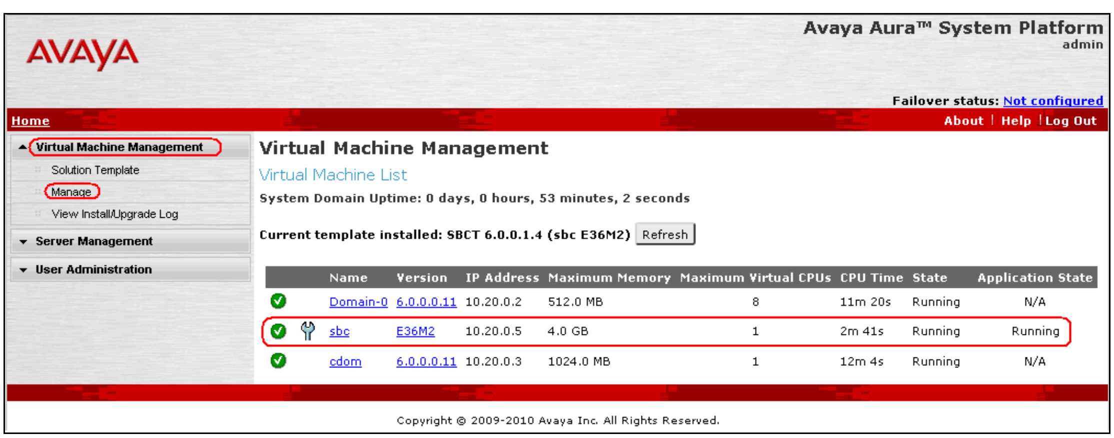
The pop-up window will close.

4.1.3. Template Deployment

Once the user data is entered, the installer will deploy the Virtual Machine Template with all the configuration provided. The installation workflow gets updated until completion, as shown in the figure below.



Click on the left hand side of the menu **Virtual Machine Management → Manage** to verify that the **sbc** is in **Running** state.



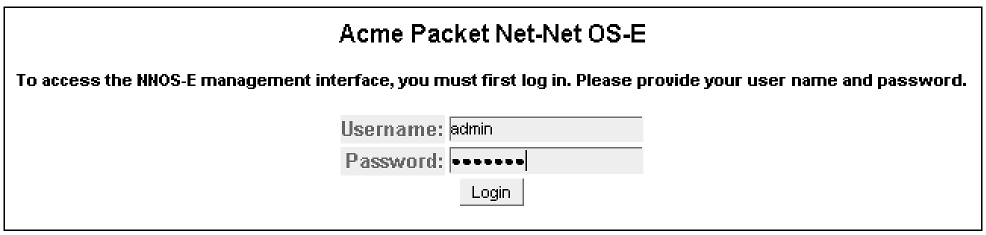
4.2. Configuration of Avaya Aura™ Session Border Controller

This section provides the procedures for configuring Session Border Controller and includes the following items:

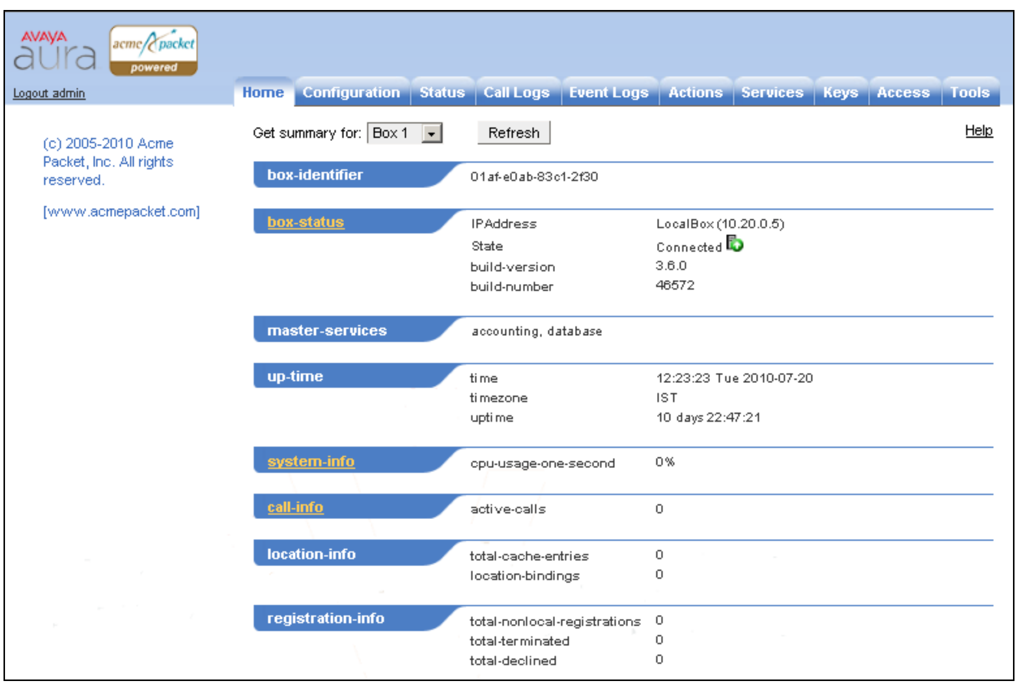
- Log in to Avaya Aura™ Session Border Controller using the GUI
- Licensing Avaya Aura™ Session Border Controller
- Administer SIP Domains
- Save the Configuration

4.2.1. Log in to Avaya Aura™ Session Border Controller using the GUI

Configuration is accomplished by accessing the browser-based GUI of Session Border Controller, using the URL "**https://<ip-address>**", where "<ip-address>" is the IP address of the inside interface of the Session Border Controller. Log in with the appropriate credentials.

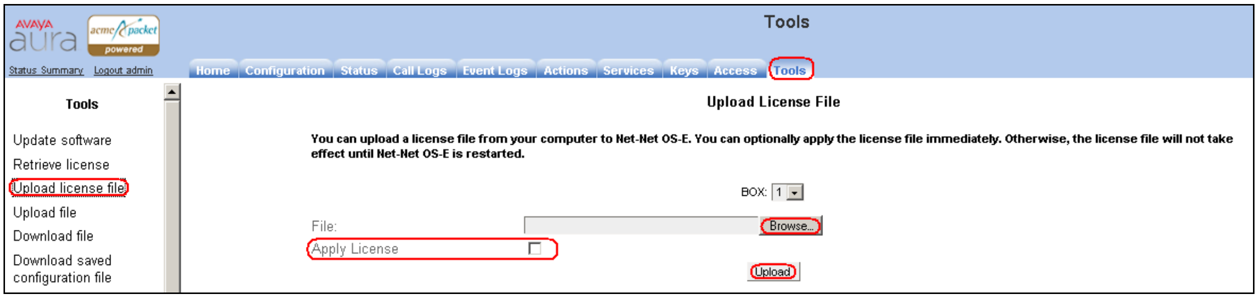


The **Home** page is displayed.



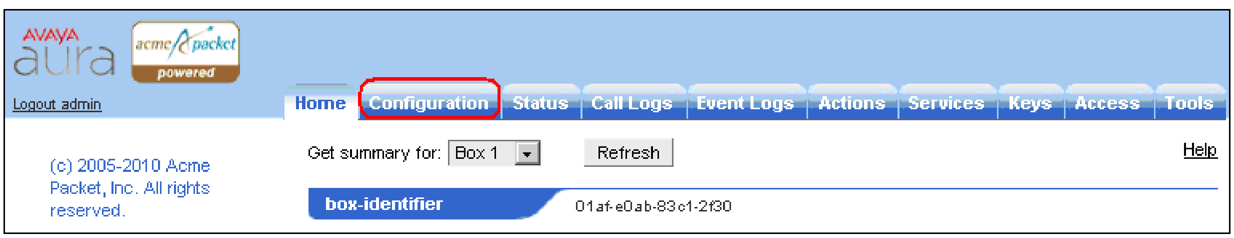
4.2.2. Licensing Avaya Aura™ Session Border Controller

To upload a license file, select the **Tools** tab on the toolbar. Click on **Upload license file** on the left hand menu. In the main web frame, click on **Browse** to select the previously obtained license file from the web client PC, tick the **Apply License** checkbox and click on **Upload**.

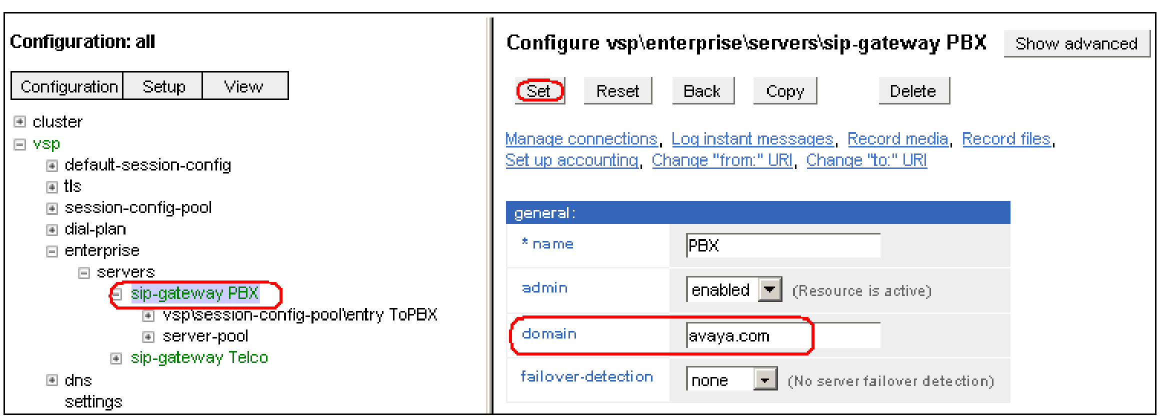


4.2.3. Administer SIP Domains

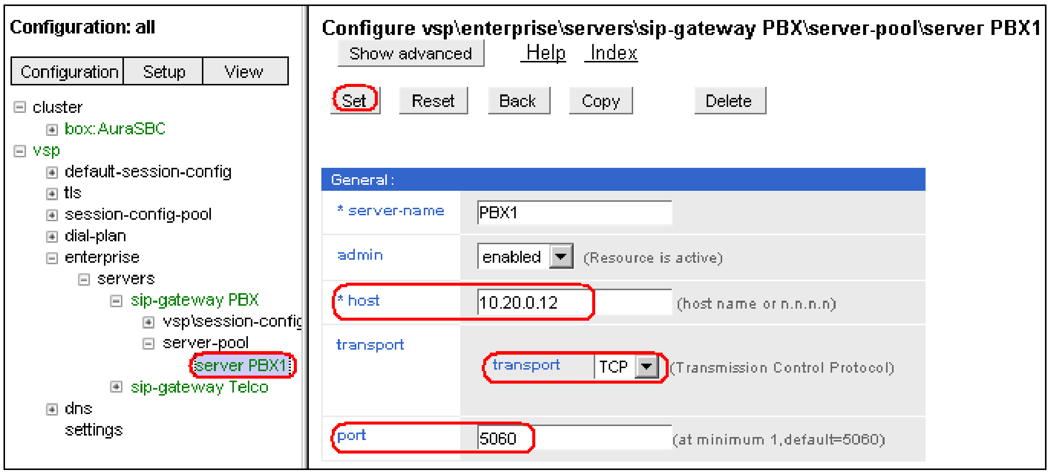
The Session Border Controller performs topology hiding by translating the private domain avaya.com to the public domain assigned by the Service Provider for outbound calls and vice-versa for inbound calls. The following steps assign the domain names to the corresponding SIP Entities. Select the **Configuration** tab on the toolbar.



Expand the menu on the left: **vsp → enterprise → servers** and click on **sip-gateway PBX.** The **Configure vsp\enterprise\servers\sip-gateway PBX** page is displayed. Ensure that the proper domain i.e. **avaya.com** is set in the domain field, if modifying the value then click **Set**.

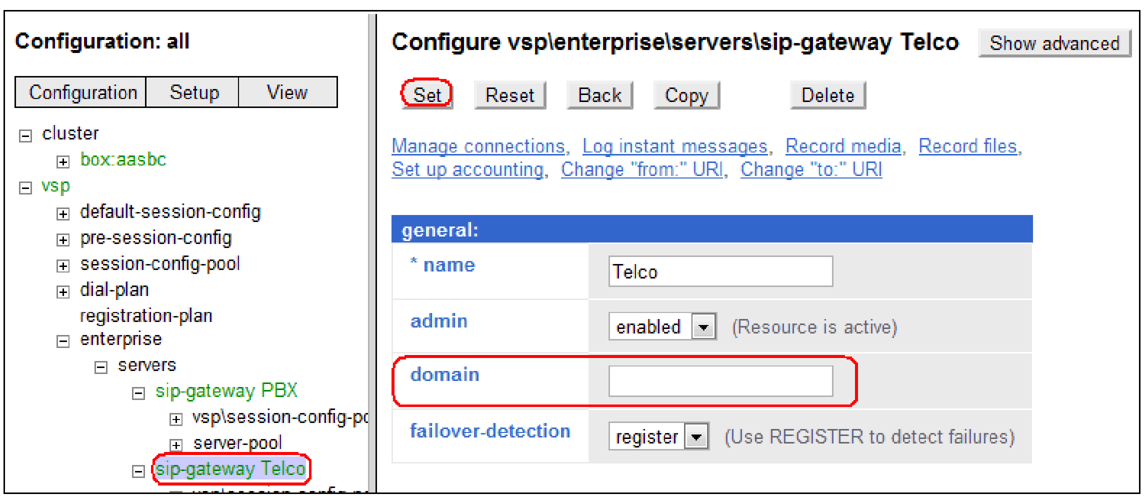


Expand the menu on the left: **vsp → enterprise → servers→ sip-gateway PBX→server-pool** and click on **server PBX1.** The **Configure vsp\enterprise\servers\sip-gateway PBX\server-pool\server PBX1** page is displayed. Ensure that **host** (i.e. **10.20.0.12**), **transport** (i.e. **TCP**) and **port** (i.e. **5060**) are set according to the definition of the sip signalling group defined on Communication Manager in **Section 3.6.1**. Click **Set** to retain the changes made.

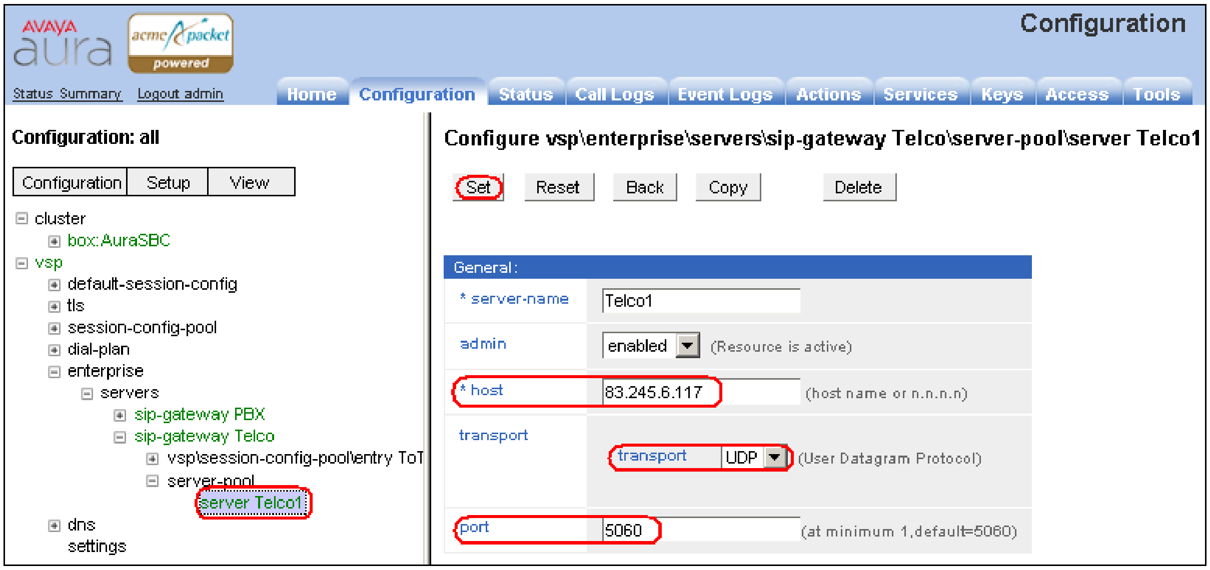


Select **sip-gateway Telco** on the left pane. The **Configure vsp\enterprise\servers\sip-gateway Telco** page is displayed. Fill in the **domain** field with the appropriate domain if in use by Service Provider, then click **Set**.

Note: Field is left blank in these Application Notes.

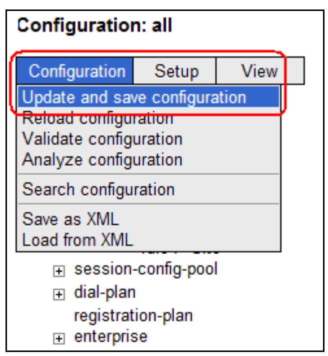


Expand the menu on the left: **vsp → enterprise → servers→ sip-gateway Telco→server-pool** and click on **server Telco1.** The **Configure vsp\enterprise\servers\sip-gateway Telco1** page is displayed. Ensure that **host** (i.e. **83.245.6.117**), **transport** (i.e. **UDP**) and **port** (i.e. **5060**) are set according to the information provided by the SIP Service Provider. Click **Set** to retain the changes made.

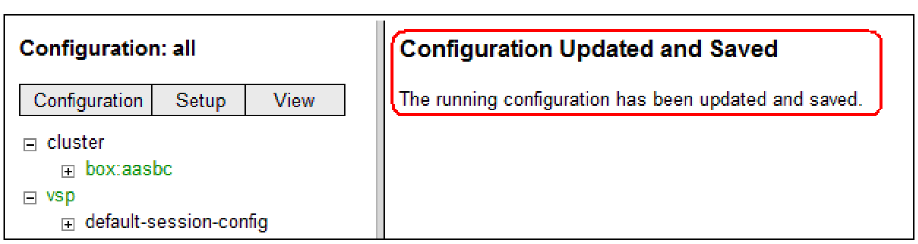


4.3. Save the Configuration

Click **Configuration** on the left pane then select **Update and save configuration**.



Click **ok** when presented to confirm the action (not shown). Once the configuration is written to disk the **Configuration Updated and Saved** message is displayed.



5. Verification Steps

This section provides the verification steps that may be performed to verify that Avaya enterprise network can establish and receive calls with the Service Provider.

5.1. Verify Avaya Aura™ Communication Manager Trunk Status

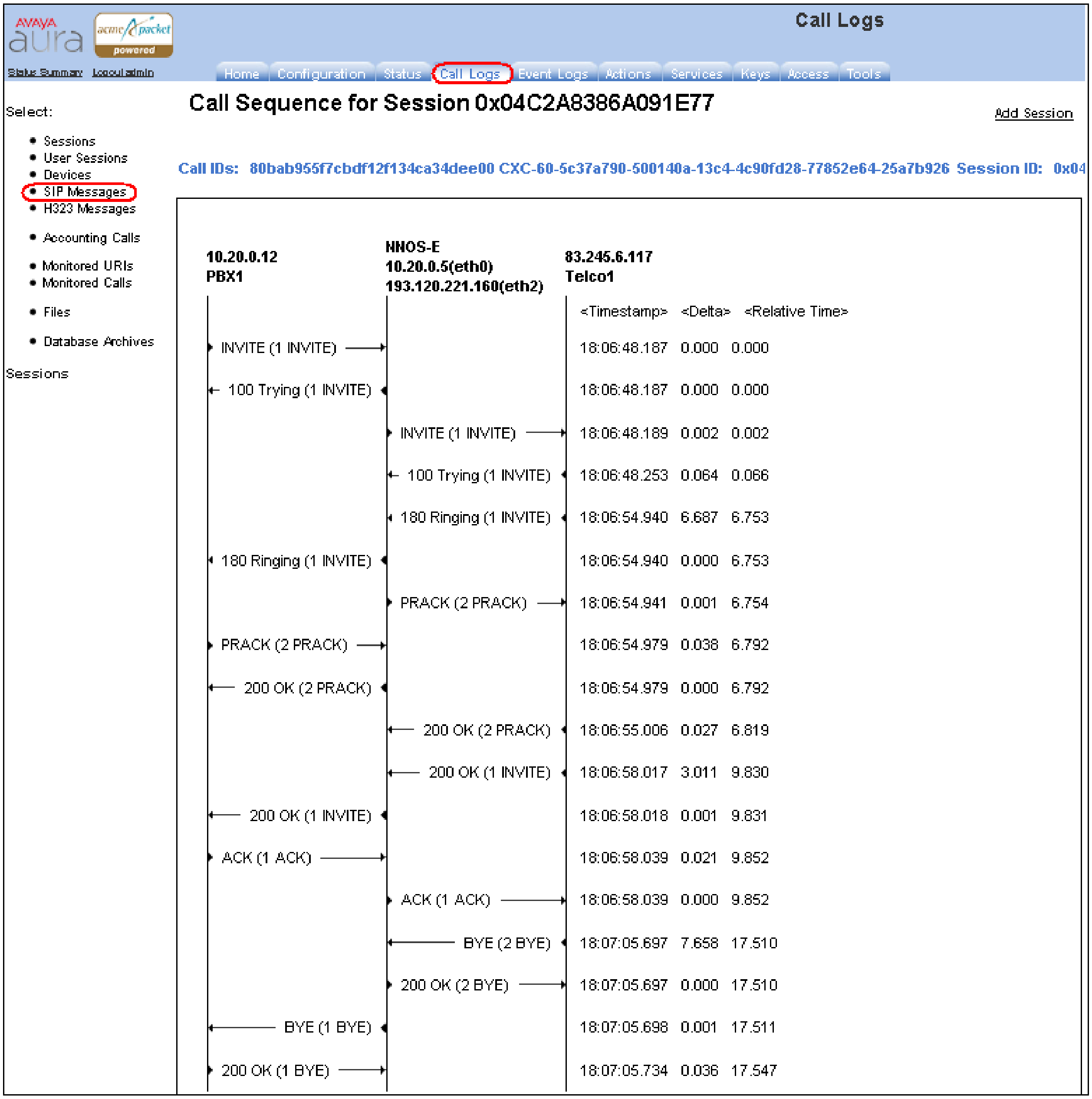
On Communication Manager Access Element, ensure that all the signalling groups are in-service status, by issuing the command **status signalling-group n** where **n** is the signalling group number.

```
status signaling-group 6
                         STATUS SIGNALING GROUP

        Group ID: 6                              Active NCA-TSC Count: 0
      Group Type: sip                             Active CA-TSC Count: 0
  Signaling Type: facility associated signaling
     Group State: in-service
```

5.2. SIP Monitoring on Avaya Aura™ Session Border Controller

On the SBC, select **Call Logs** tab from the tool bar and click on the SIP Messages on the let hand pane. A list of sip message is presented (not shown) select the existing call to expand into a ladder diagram (in diagram below).



6. General Test Approach

6.1. Interoperability Compliance Testing

The primary focus of testing is to verify SIP trunking interoperability between a Communication Manager and Session Border Controller using a generic SIP trunking service. Test cases are selected to exercise a sufficiently broad segment of functionality to have a reasonable expectation of interoperability in production configurations.

Basic Interoperability:

- PSTN calls delivered via the Service Provider's SIP trunking to an Avaya IP telephony solution
- PSTN calls sent via a Service Provider's SIP trunking from an Avaya IP telephony solution
- Calling with various Avaya telephone models including IP models as well as traditional analog and digital TDM phones
- Verify Codec Support for G.711a and G.729a
- Various PTSN dialing plans including national and international calling, toll-free, operator, directory assistance and direct inward dialed calling
- SIP transport using UDP
- Fax Testing using T.38 standard transport.

Advanced Interoperability:

- Codec negotiation
- Telephony supplementary features, such as Hold, Call Transfer, Conference Calling and Call Forwarding
- DTMF Tone Support
- Voicemail Coverage and Retrieval
- Direct IP-to-IP Media (also known as "Shuffling") over SIP Trunk. Direct IP-to-IP media allows compatible phones to reconfigure the RTP path after call establishment directly between the Avaya phones and the Session Boarder Controller and release media processing resources on the Avaya Media Gateway
- EC500 for Communication Manager

6.2. Test Results and Remarks

All test cases successfully completed.

7. Conclusion

As illustrated in these Application Notes, an Avaya Enterprise Network running Avaya Aura™ Communication Manager 5.2.1 and Avaya Aura™ Session Border Controller 6.0 can be configured to interoperate successfully with the SIP trunking service IP Direct Connect offer from Gamma Telecom. The reference configuration shown in these Application Notes is representative of a basic Enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation.

8. References

The Avaya product documentation is available at http://support.avaya.com unless otherwise noted.

[1] "Installing and Configuring Avaya Aura™ System Platform", Release 1.1, November 2009

[2] "Avaya Aura™ Communication Manager Overview", Document Number 03-300468, Issue 6, Release 5.2, May 2009

[3] "Administering Network Connectivity on Avaya Aura™ Communication Manager", Document Number 555-233-504, Issue 14, May 2009

[4] "SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers", Document Number 555-245-206, Issue 9, May 2009

[5] "Installing and Configuring Avaya Aura™ System Platform", Release 1.1.1 April 2010

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.