Avaya Solution & Interoperability Test Lab

Application Notes for Configuring SIP Trunking between Cincinnati Bell Any Distance eVantage IP Service with Avaya Voice Portal – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Voice Portal with the Cincinnati Bell Any Distance (CBAD) eVantage IP service. The CBAD eVantage solution is a turn-key business trunking solution. Voice services, such as local, long distance and toll free calling, as well as high speed data and Internet services, are the primary applications of the CBAD eVantage solution. Avaya Voice Portal is a speech-enabled interactive voice response system that allows enterprises to provide multiple service resources, both self and assisted, to customers in a flexible and customizable manner.

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

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the steps for configuring a SIP trunking interface between Avaya Voice Portal and the Cincinnati Bell Any Distance (CBAD) eVantage IP service. The CBAD eVantage solution is a turn-key business trunking solution for customers. The CBAD eVantage provides customers with a single IP connection that converges voice and data services to drive optimization, reduce costs, and offer enhanced features not typically available in the traditional PSTN network. Voice services, such as local, long distance and toll free calling, as well a high speed data and Internet services, are the primary applications of the CBAD eVantage solution. Avaya Voice Portal is a speech-enabled interactive voice response system that allows enterprises to provide multiple service resources, both self and assisted, to customers in a flexible and customizable manner.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound call flows (see **Section 2.2** for descriptions) from users of the CBAD eVantage IP service to Avaya Voice Portal and subsequent call transfers to Avaya Aura™ Communication Manager skills and agents.

1.2. Support

For technical support on CBAD eVantage IP service, customers can call (866) 914-9474.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. The "Connect with Avaya" section following "Contacts / Worldwide" links provides the worldwide support directory. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support. Customers may also use specific numbers provided on http://support.avaya.com to directly access specific support and consultation services based upon their Avaya support agreements.

1.3. Known Limitations

Avaya Voice Portal currently supports only G.711 codecs, so customers with the CBAD eVantage IP service must use service profiles that include a G.711 codec.

2. Reference Configuration

The sample configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Avaya Voice Portal provides interactive voice response services to inbound callers. Avaya Voice Portal consists of one or more Media Processing Platform (MPP) servers and a Voice Portal Management System (VPMS) server.
- Avaya Aura™ Communication Manager provides the enterprise voice communications services. In this sample configuration, Communication Manager runs on an Avaya S8500C Server. This solution is extendable to other Avaya S8xxx Servers.
- Avaya Media Gateway provides the physical interfaces and resources for enterprise voice communications. In this sample configuration, an Avaya G650 Media Gateway is used. This solution is extendable to other Avaya Media Gateways.
- Avaya Aura™ SIP Enablement Services provides the SIP registrar and proxy functions to support the enterprise Avaya IP telephone network. In this sample configuration, SIP Enablement Services runs on an Avaya S8500C Server. This solution is extendable to other Avaya S8xxx Servers.
- Avaya "office" phones are represented with Avaya 9600 Series IP Telephones running H.323 firmware and Avaya 16CC IP Telephones running SIP firmware.
- Cisco Unified Border Element (CUBE) provides SIP Session Border Controller (SBC) functionality between the CBAD eVantage IP service and the enterprise internal network. For brevity, the Cisco Unified Border Element will be referred to as CUBE through the remainder of these Application Notes.
- The HTTP Application Server hosts the Voice XML (VXML) and Call Control XML (CCXML) applications that provide the directives for handling the inbound calls to Avaya Voice Portal. Avaya Voice Portal references these applications.
- The Speech Server consists of Nuance OpenSpeech Recognizer and Nuance RealSpeak. Avaya Voice Portal uses the Speech Server for Automatic Speech Recognition (ASR) and Text-To-Speech (TTS) capabilities.

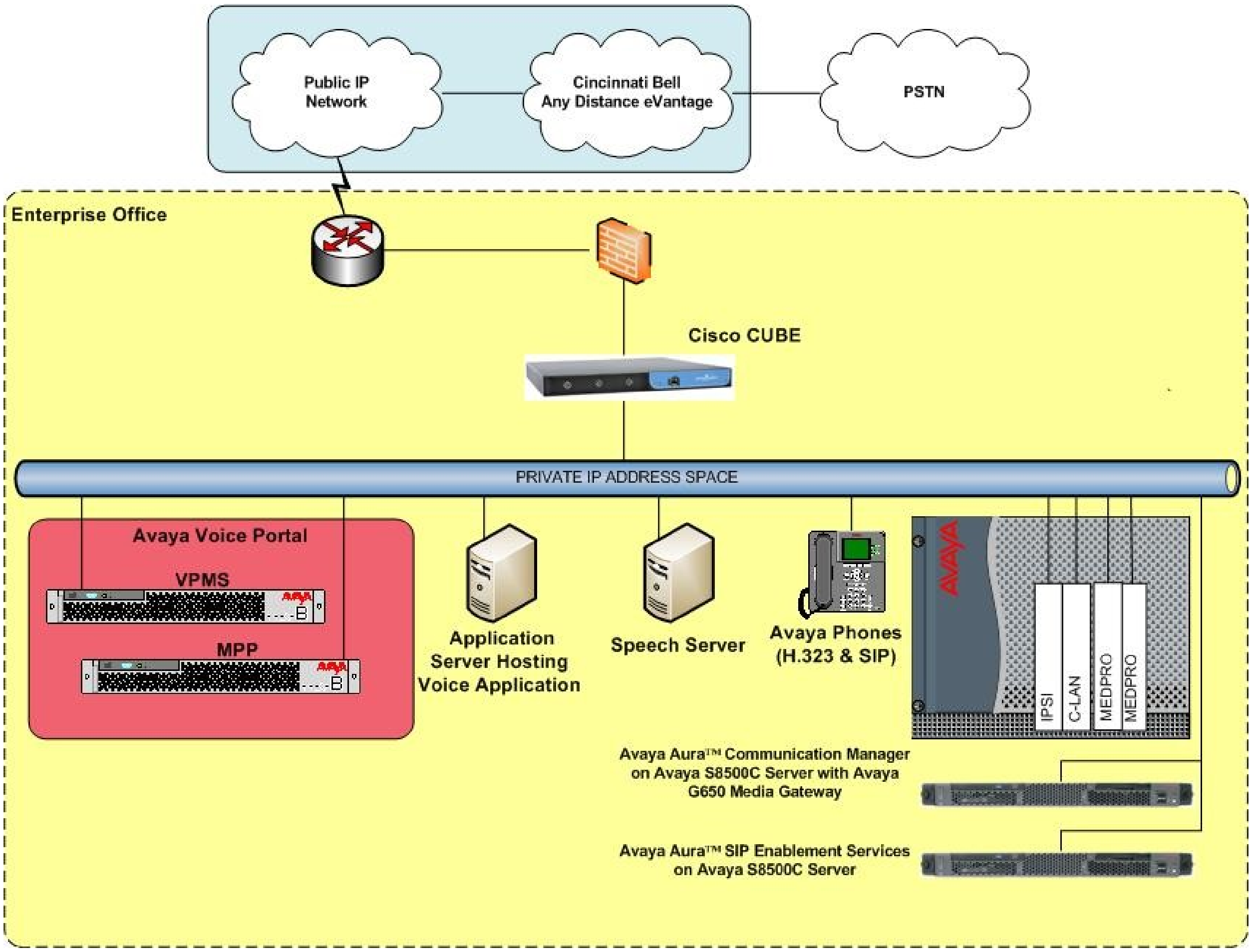


Figure 1: Sample Configuration

2.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the sample configuration described in these Application Notes, and are **for illustrative purposes only**. Customers must obtain and use the specific values for their own specific configurations.

Component	Illustrative Value in these Application Notes
Avaya Voice Portal	
VPMS IP Address MPP IP Address	10.45.122.130 10.45.122.131
Avaya Aura™ Communication Manager	
C-LAN IP Address	10.45.108.55
Vector Directory Number (VDN) Extensions	201xx
Skill (Hunt Group) Extensions	202xx
Agent Extensions	61xxx
Phone Extensions	203xx
Announcement Extensions	222xx
Avaya Aura™ SIP Enablement Services	
IP Address	10.45.108.50
Cisco CUBE	
IP Address of "Outside" Interface (connected to CBAD eVantage via public IP network)	22.160.183.211
IP Address of "Inside" Interface (connected to Avaya elements)	10.45.108.81
CBAD eVantage IP service	
Direct Inward Dialing (DID) number for service access	(513) 639-2085
Digits Passed in SIP To Header to Avaya Voice Portal	5136392085

Table 1: Illustrative Values Used in these Application Notes

2.2. Call Flows

To understand how inbound calls from the CBAD eVantage service are handled by Avaya Voice Portal, several call flows are described in this section.

The first call scenario illustrated in **Figure 2** is an inbound call arriving and remaining on Avaya Voice Portal.

1. A PSTN phone originates a call to a CBAD eVantage service number.
2. The PSTN routes the call to the CBAD eVantage IP service network.
3. The CBAD eVantage IP service routes the call to the CUBE placed at the edge of the enterprise IP network.
4. The CUBE performs SIP network address translation (NAT) and any necessary SIP header modifications, and routes the call to Avaya Voice Portal. Avaya Voice Portal matches the called party number to a VXML and/or CCXML application, answers the call, and handles the call according to the directives specified in the application.
5. In this scenario, the application sufficiently meets the caller's needs or requests, and thus the call does not need to be transferred to the Communication Manager.

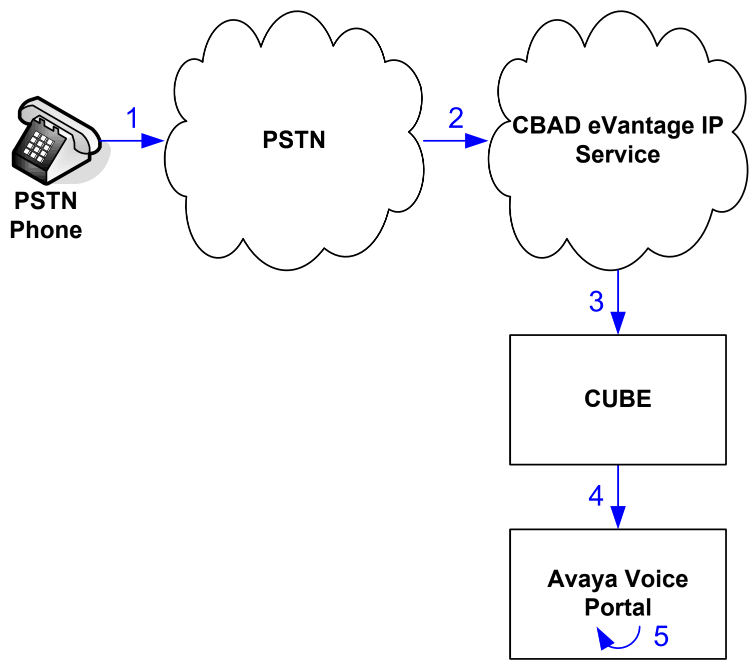


Figure 2: Inbound Call Handled Entirely by Avaya Voice Portal

The second call scenario illustrated in **Figure 3** is an inbound call arriving on Avaya Voice Portal and transferred to Communication Manager only after a Communication Manager skill has been canvassed for agent availability and an agent becomes available.

1. Same as the first four steps from the first call scenario.
2. In this scenario, the application is not sufficient to meet the caller's needs or requests, and thus the call needs to be transferred to a Communication Manager agent. Avaya Voice Portal canvasses a skill on Communication Manager by placing a call to a vector on Communication Manager through the CUBE. While the inbound call is waiting for an agent to connect to, it can receive various wait treatments like music and/or announcements.
3. Communication Manager informs Avaya Voice Portal when an agent in that skill becomes available.
4. Avaya Voice Portal instructs the CUBE to transfer the inbound call to that skill.
5. CUBE transfers the inbound call to the aforementioned skill on Communication Manager.
6. Communication Manager routes the call to the agent[1].

[1] This is the case if the agent phone is an H.323 IP phone directly configured on Communication Manager. If the agent phone is a SIP IP phone, Communication Manager will route the call to SIP Enablement Services for call termination.

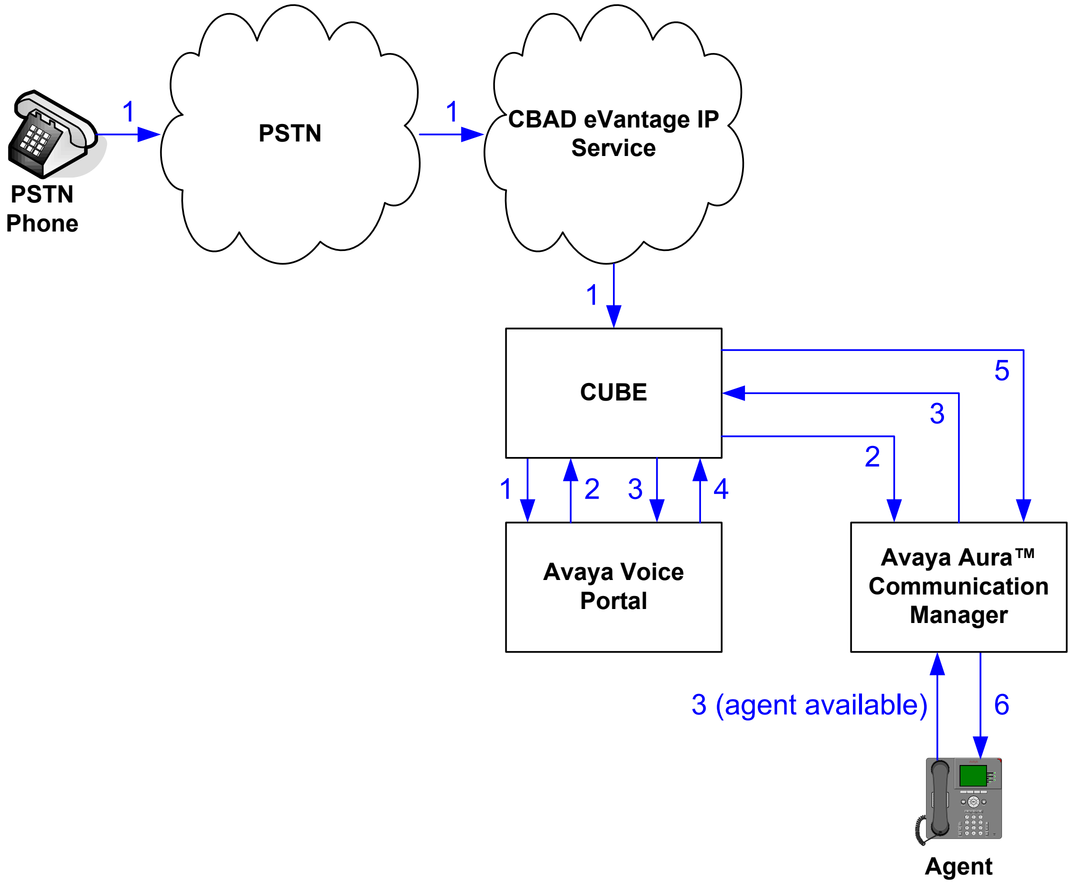


Figure 3: Inbound Call Transferred by Avaya Voice Portal to Avaya Aura™ Communication Manager Upon Available Agent

The third call scenario illustrated in **Figure 4** is an inbound call arriving on Avaya Voice Portal and transferred to a Communication Manager skill without canvassing that skill for agent availability, i.e., transferred to that skill regardless of whether an agent in that skill was available:

1. Same as the first four steps from the first call scenario.
2. In this scenario, the application is not sufficient to meet the caller's needs or requests, and thus the call needs to be transferred to a Communication Manager agent. Avaya Voice Portal instructs the CUBE to transfer the inbound call to a Communication Manager skill.
3. The CUBE transfers the inbound call to the aforementioned skill on Communication Manager.
4. An agent becomes available.
5. Communication Manager routes the call to the agent[2].

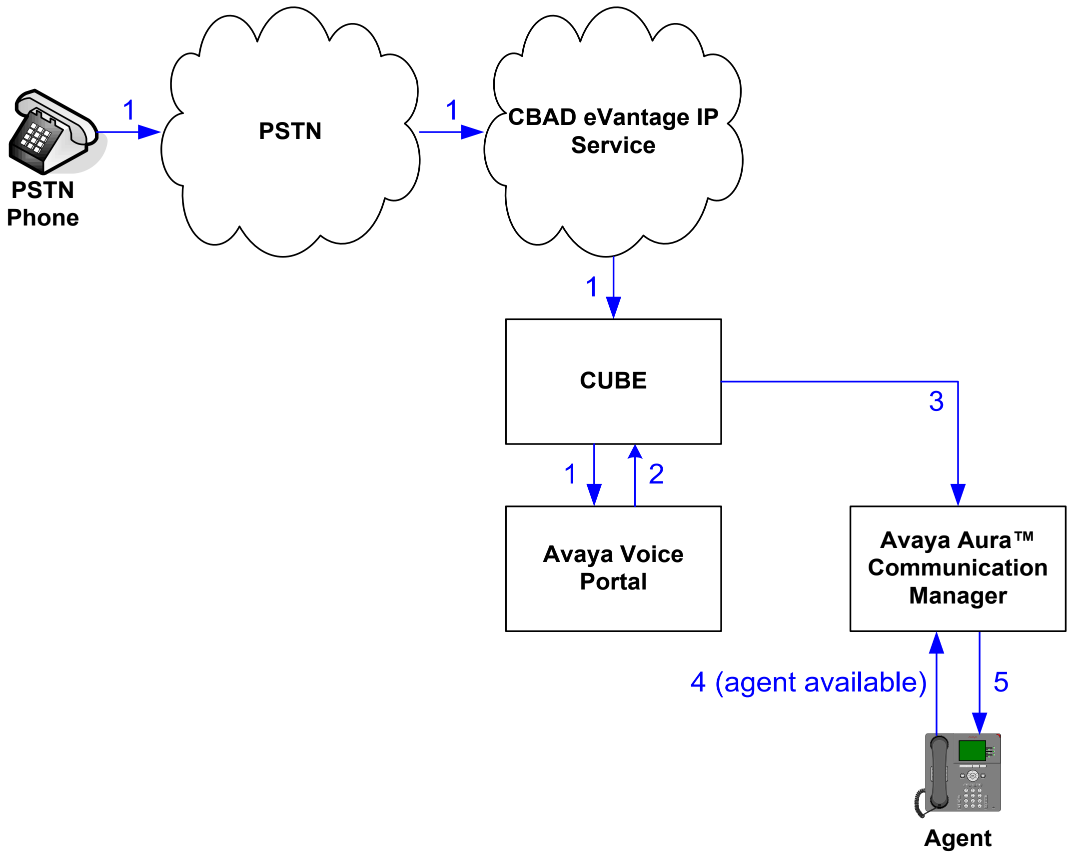


Figure 4: Inbound Call Transferred by Avaya Voice Portal to Avaya Aura™ Communication Manager Regardless of Agent Availability

[2] This is the case if the agent phone is an H.323 IP phone directly configured on Communication Manager. If the agent phone is a SIP IP phone, Communication Manager will route the call to SIP Enablement Services for call termination.

3. Equipment and Software Validated

The following equipment and software was used for the sample configuration described in these Application Notes.

Component	Version
Avaya Voice Portal	5.0
Voice Portal Management System (VPMS)	5.0.0.0.4602
Media Processing Platform (MPP)	5.0.0.0.4603
Avaya S8500C Server	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3 with update 17294)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface (IPSI)	HW28 FW040
TN799DP Control-LAN (C-LAN)	HW01 FW026
TN2302AP IP Media Processor (MedPro)	HW20 FW118
TN2602AP IP Media Resource 320 (MedPro)	HW02 FW047
TN2501AP VAL-ANNOUNCEMENT	HW02 FW020
Avaya S8500C Server	Avaya Aura™ SIP Enablement Services 5.2 (SES-5.2.0.0-947.3b with update SES-2.0.947.3-SP1)
Avaya 9600 Series IP Telephones	Avaya one-X™ Deskphone Edition H.323 Release 3.0
Avaya 16CC SIP Telephone	Release 1.0.92
Nuance Speech Servers	5.0
Nuance OpenSpeech Recognizer	3.0
Nuance RealSpeak	4.0
Cisco Unified Border Element (CUBE)	12.4(24)T1
Cincinnati Bell Any Distance eVantage Service	

Table 2: Equipment and Software Versions

4. Configure Avaya Voice Portal

Avaya Voice Portal handles inbound calls according to the directives specified by VXML and/or CCXML applications. The applications do not reside on Avaya Voice Portal, but rather on one or more separate application servers. References to those applications are administered on Avaya Voice Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Avaya Voice Portal, the called party number is matched against those administered called numbers. If a match is found, then the corresponding application is accessed to handle the call. If no match[3] is found, Avaya Voice Portal informs the caller that the call cannot be handled, and disconnects the call.

For the sample configuration described in these Application Notes, a simple VXML application was used to exercise Voice Portal self-service as well as call flow scenarios expected to occur with the CBAD eVantage IP service. In production, enterprises can develop their own VXML and/or CCXML applications to meet their specific customer self-service needs, or consult Avaya Professional Services and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes. Consult [1], [2], and [3] for further details if necessary.

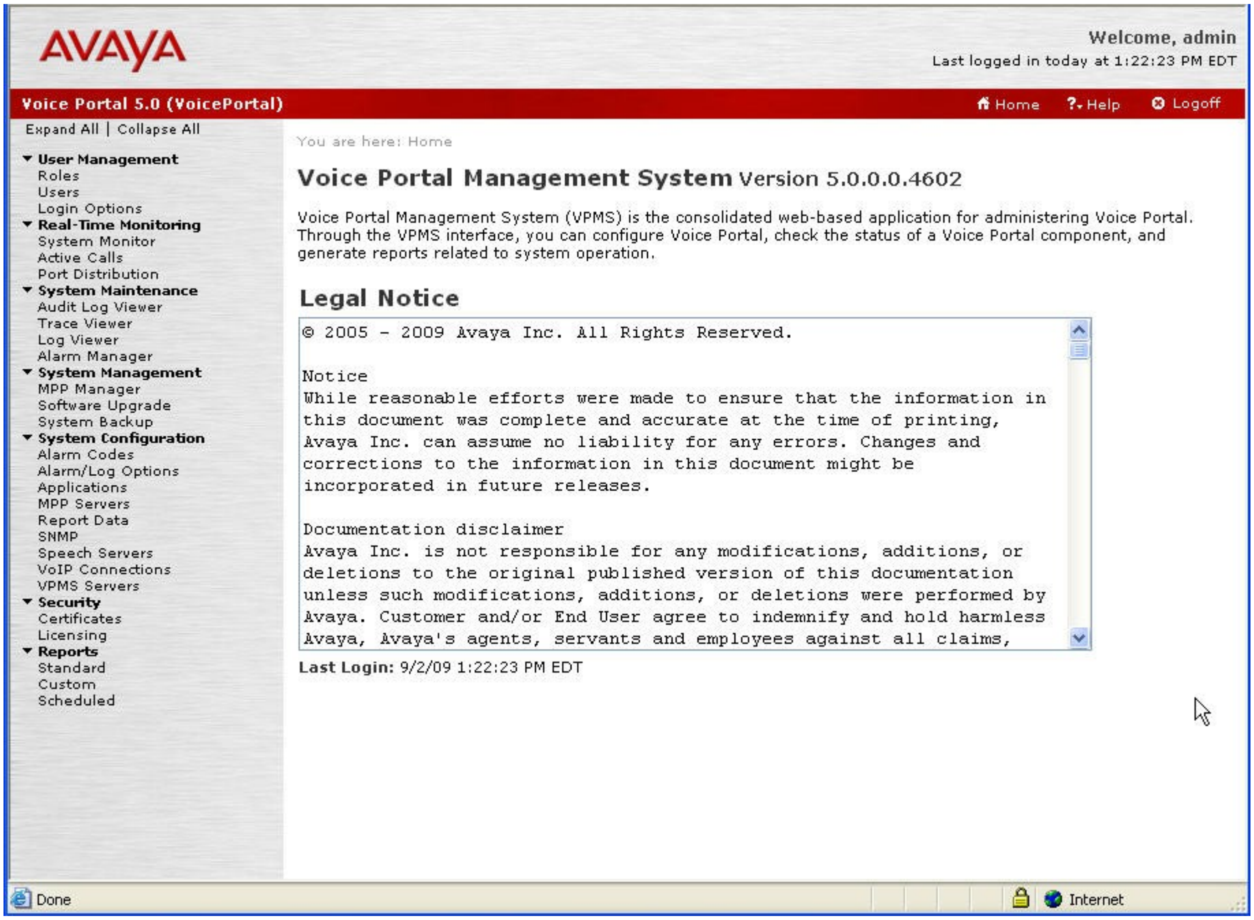
These Application Notes also assume that the necessary Avaya Voice Portal licenses have been installed and basic Avaya Voice Portal administration has already been performed. Consult [1], [2], and [3] for further details if necessary.

Avaya Voice Portal configuration required for interoperating with the CBAD eVantage IP service includes following areas:

- Install certificate for TLS authentication
- Configure SIP connection
- Add MPP server
- Configure VoIP audio format
- Add speech server
- Add application references
- Start MPP server

[3] One application reference may be configured with "inbound default" as the called number to handle all inbound calls that do not match any other application references.

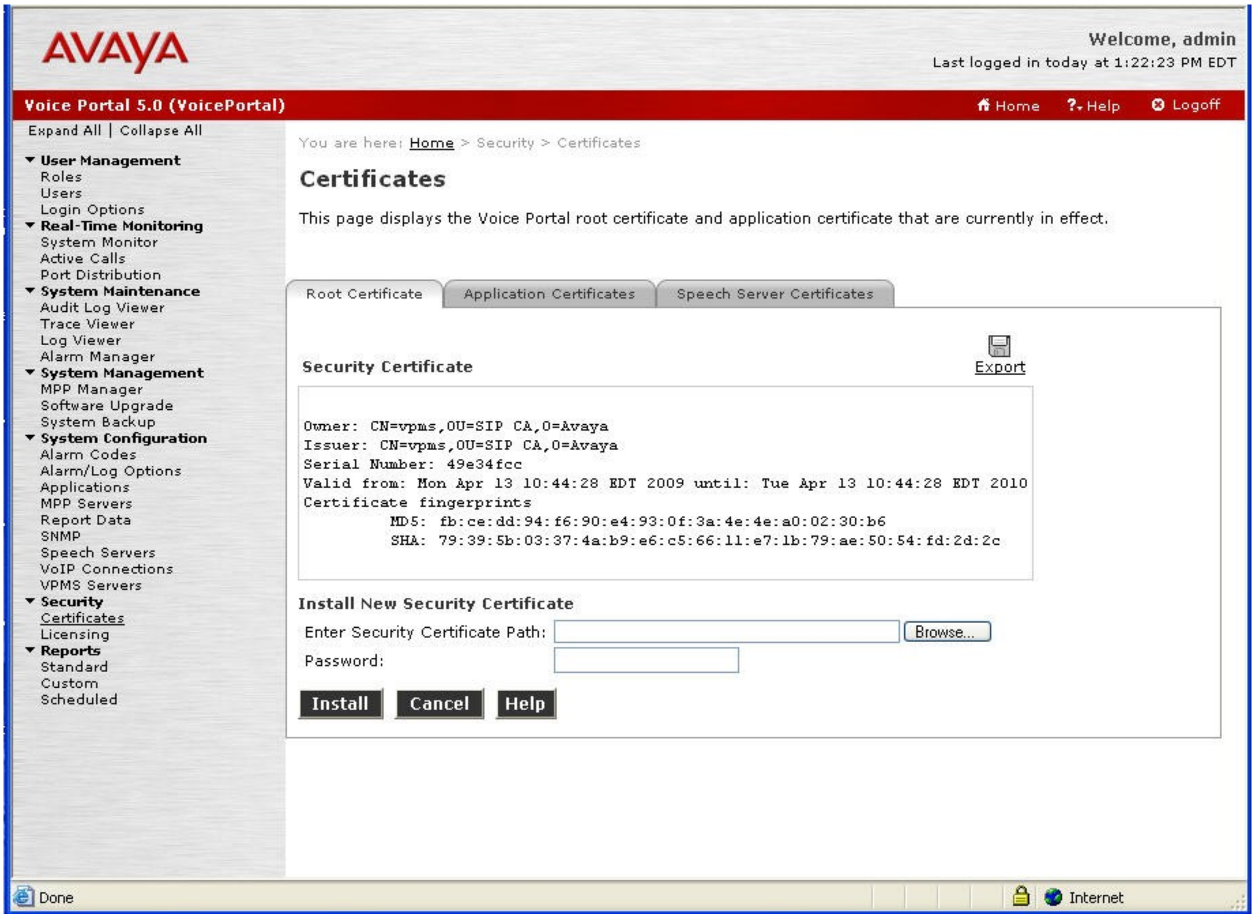
Avaya Voice Portal is configured via the Voice Portal Management System (VPMS) web interface. To access the web interface, enter `http://<ip-addr>/VoicePortal` as the URL in an Internet browser, where `<ip-addr>` is the IP address assigned to the VPMS server. Log in using the Administrator user role. The initial Voice Portal screen after login is shown below.



Note: All of the screens shown in this section were taken after Avaya Voice Portal had been configured. The navigation sequence to each screen is displayed at the top of each screen.

4.1. Install Certificate for TLS Authentication

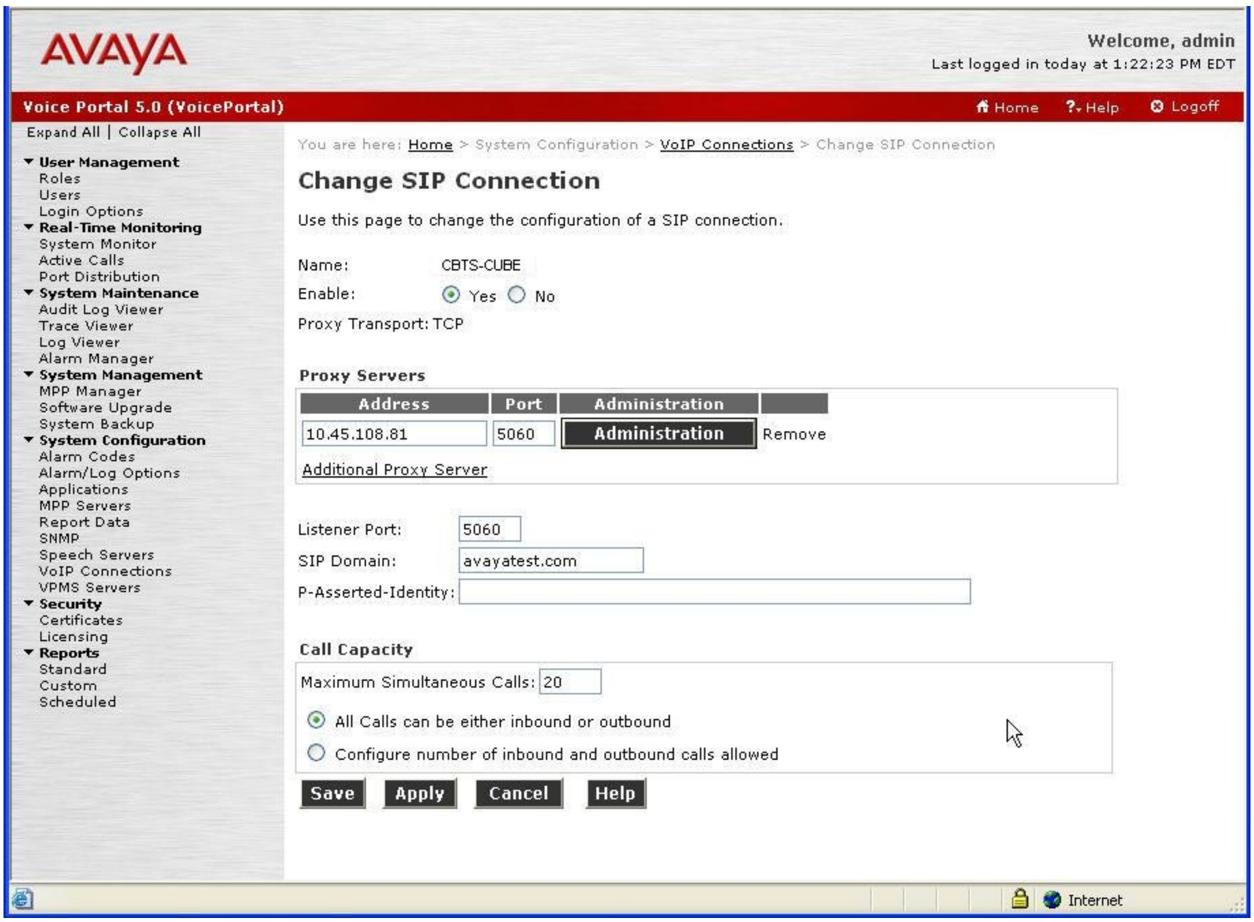
In the compliance test, Avaya Voice Portal was configured to use TCP on SIP interface to the CUBE (to facilitate debugging). A production environment is more likely to use TLS authentication over the SIP interface between Avaya Voice Portal and the CUBE. To install the certificate for TLS authentication, navigate to **Security → Certificates** and select the **Root Certificate** tab. Specify the directory path where the certificate is located and the password, and then click **Install**. The screen below shows a certificate that has already been installed.



4.2. Configure SIP Connection

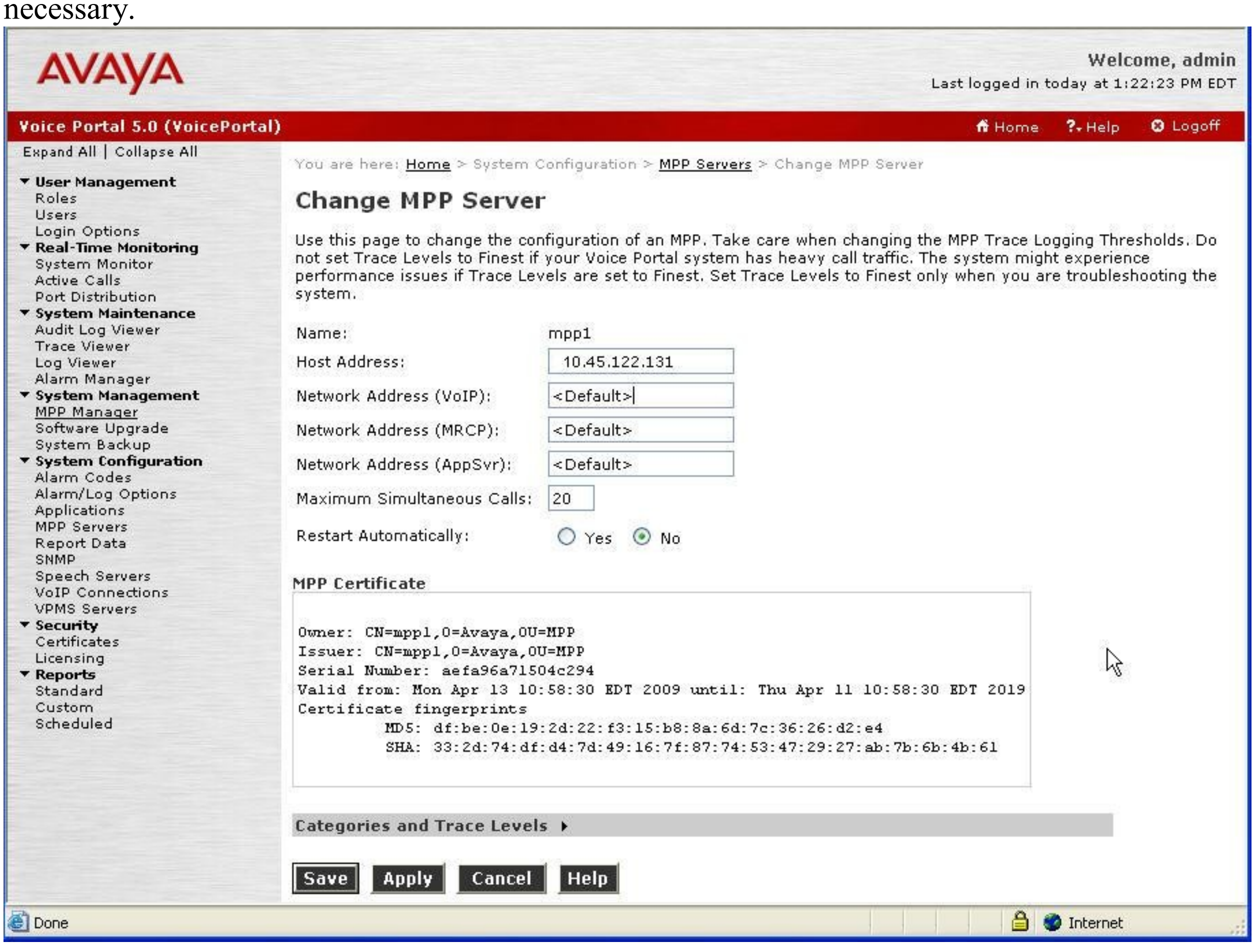
To configure a SIP connection to the CUBE, navigate to **System Configuration → VoIP Connections**, click on the **SIP** tab. The SIP tab is displayed as shown below. Configure the parameters as follows:

- Enter a descriptive text for **Name**.
- Select the ***Yes*** radio button for **Enable**.
- Select ***TCP*** as the **Proxy Transport**.
- Specify the private side IP address assigned to the CUBE for **Proxy Server Address** and specify ***5060*** for **Proxy Server Port**.
- Set **Listener Port** fields to ***5060*** for TCP.
- For **SIP Domain**, specify the SIP domain used in the enterprise (see **Section 5.3 Step 4**).
- Set the **Maximum Simultaneous Calls**. In this example, a maximum of 20 calls is specified.
- Accept the default values for the other fields.



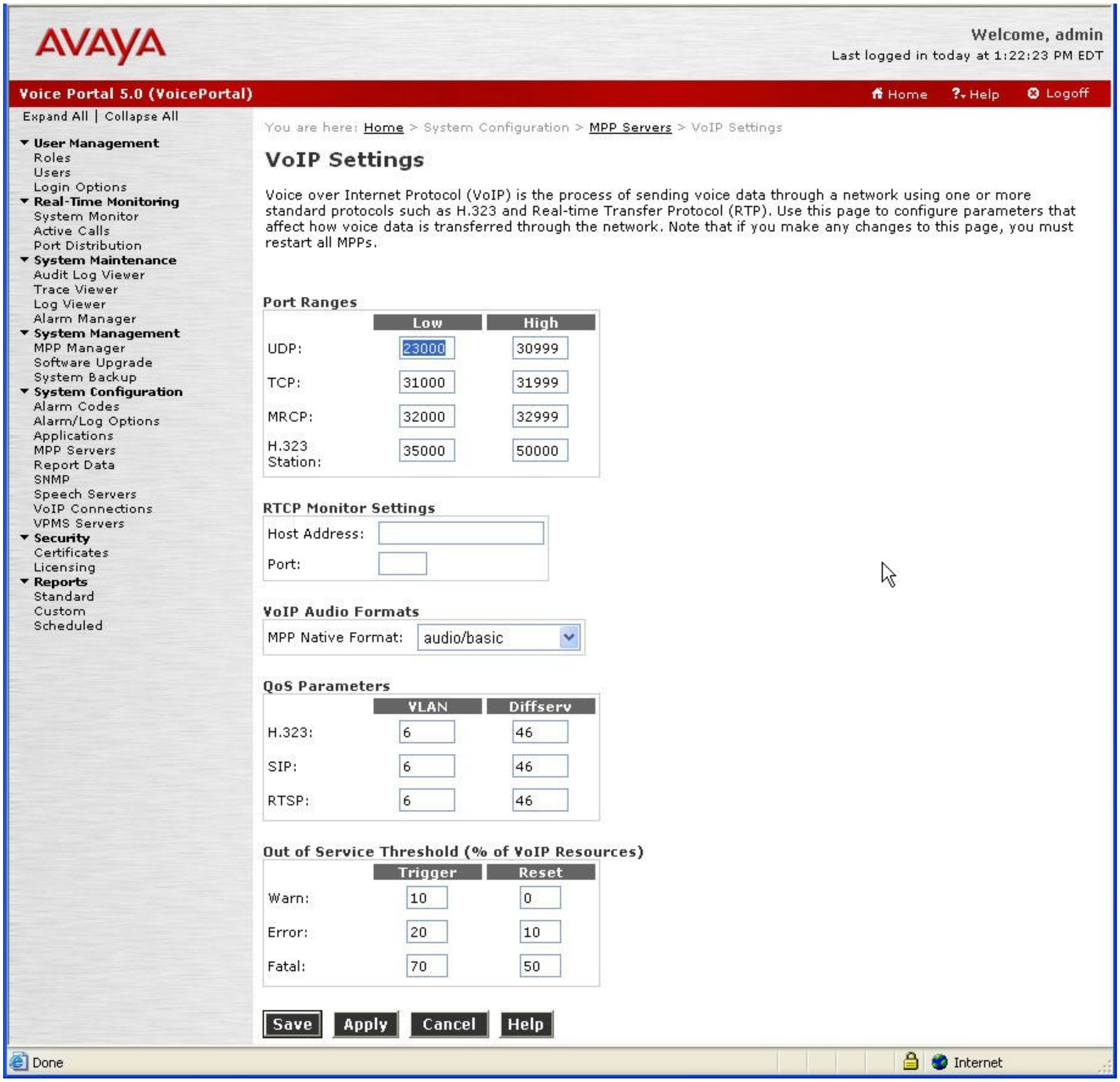
4.3. Add MPP server

Add an MPP server by navigating to **System Configuration → MPP Servers**. In the MPP Server configuration page, specify a descriptive **Name** and the **Host Address** of the MPP server. Also, specify the **Maximum Simultaneous Calls** supported on this MPP server. The screen below shows the configuration for the MPP server used in the compliance test. Only one MPP server was used in the compliance test. Repeat these steps to configure additional MPP servers if necessary.



4.4. Configure VoIP Audio Format

The **VoIP Audio Format** for MPP servers is configured in the **VoIP Settings** screen accessible from **System Configuration → MPP Servers** (via the **VoIP Settings** button). The Avaya Voice Portal supports both G.711 mu-law and G.711 a-law. The **MPP Native Format** field in the screen below is set to ***audio/basic*** for mu-law.

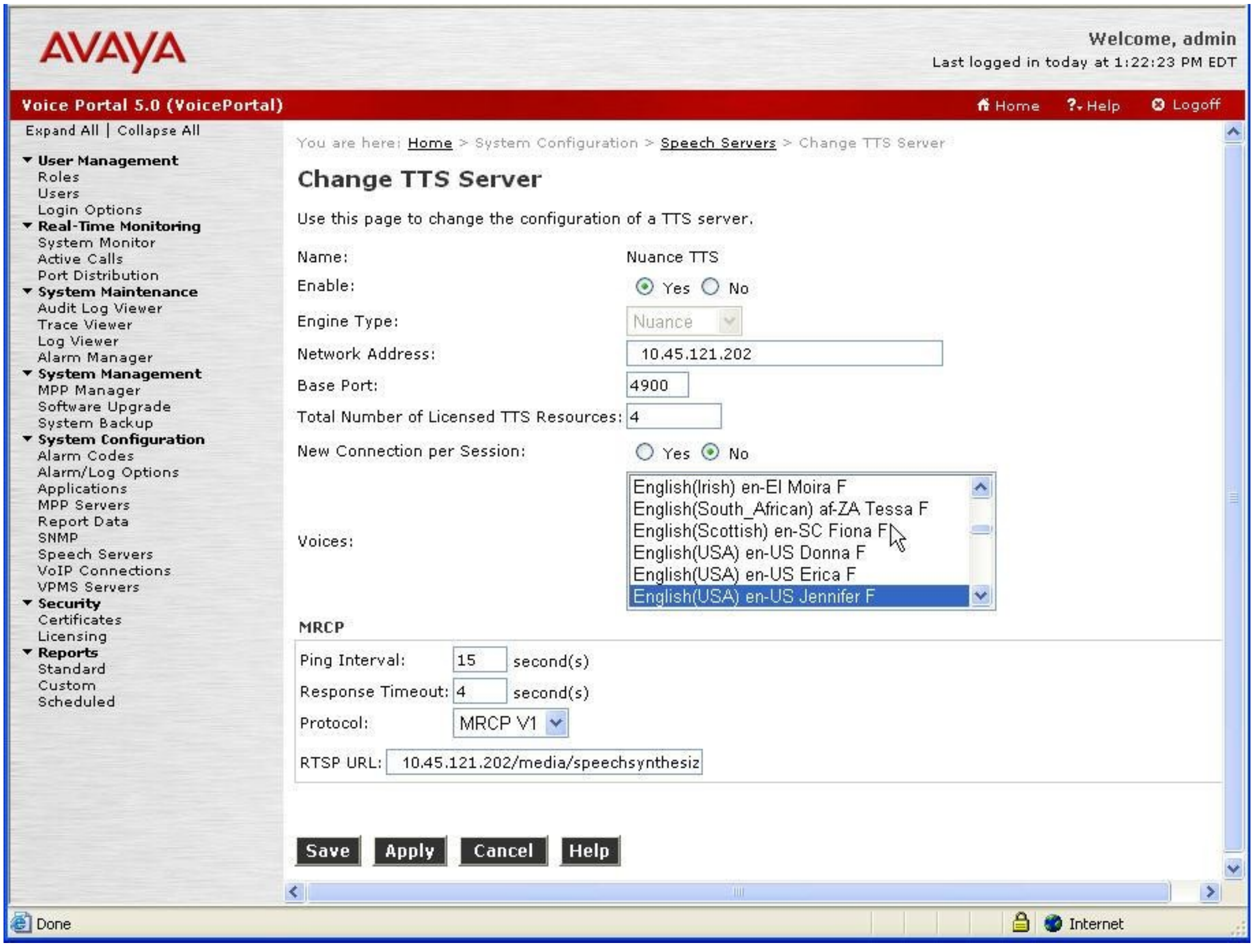


4.5. Add Speech Server

Adding a speech server for providing ASR and/or TTS services is part of the standard configuration for Avaya Voice Portal; this configuration is not directly related to achieving interoperability between the CBAD eVantage IP service and Avaya Voice Portal. It is included here for completeness.

To configure the ASR server, navigate to **System Configuration → Speech Servers**, select the **ASR** tab, and then click **Add**. The screen below shows the configuration for the ASR server used in the compliance test. Set the **Engine Type** to the appropriate value. In the test configuration, a Nuance ASR server was used so the engine type was set to ***Nuance***. Set the **Network Address** field to the IP address assigned to the speech server and select the desired **Languages** to be supported. The other fields were set to their default values.

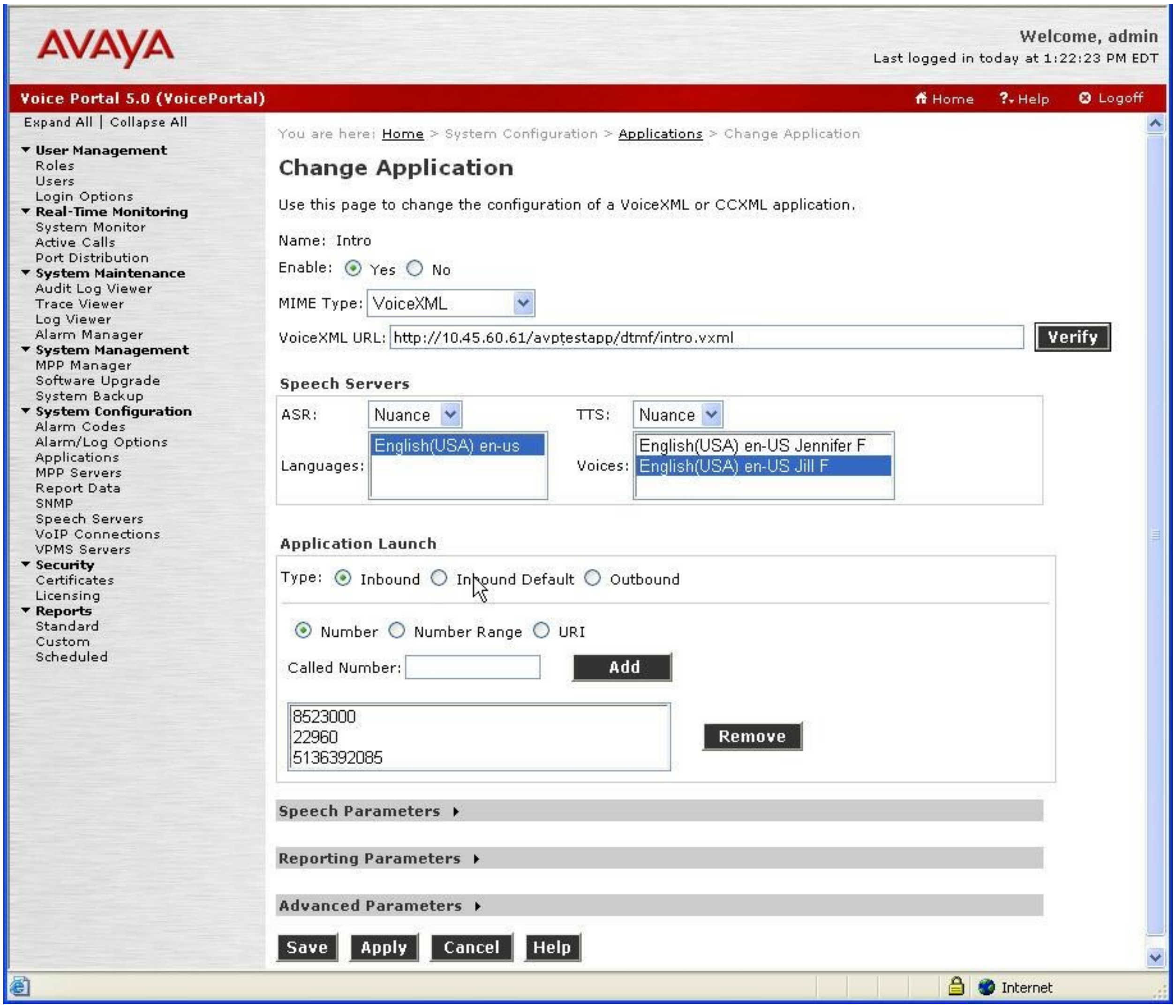
To configure the TTS server, navigate to **System Configuration → Speech Servers**, select the **TTS** tab, and then click **Add**. The screen below shows the configuration for the TTS server used in the compliance test. In this configuration, a Nuance TTS server was used so the engine type was set to ***Nuance***. Set the **Network Address** field to the IP address assigned to the speech server and select the desired **Languages** to be supported. The other fields were set to their default values.



4.6. Add Application References

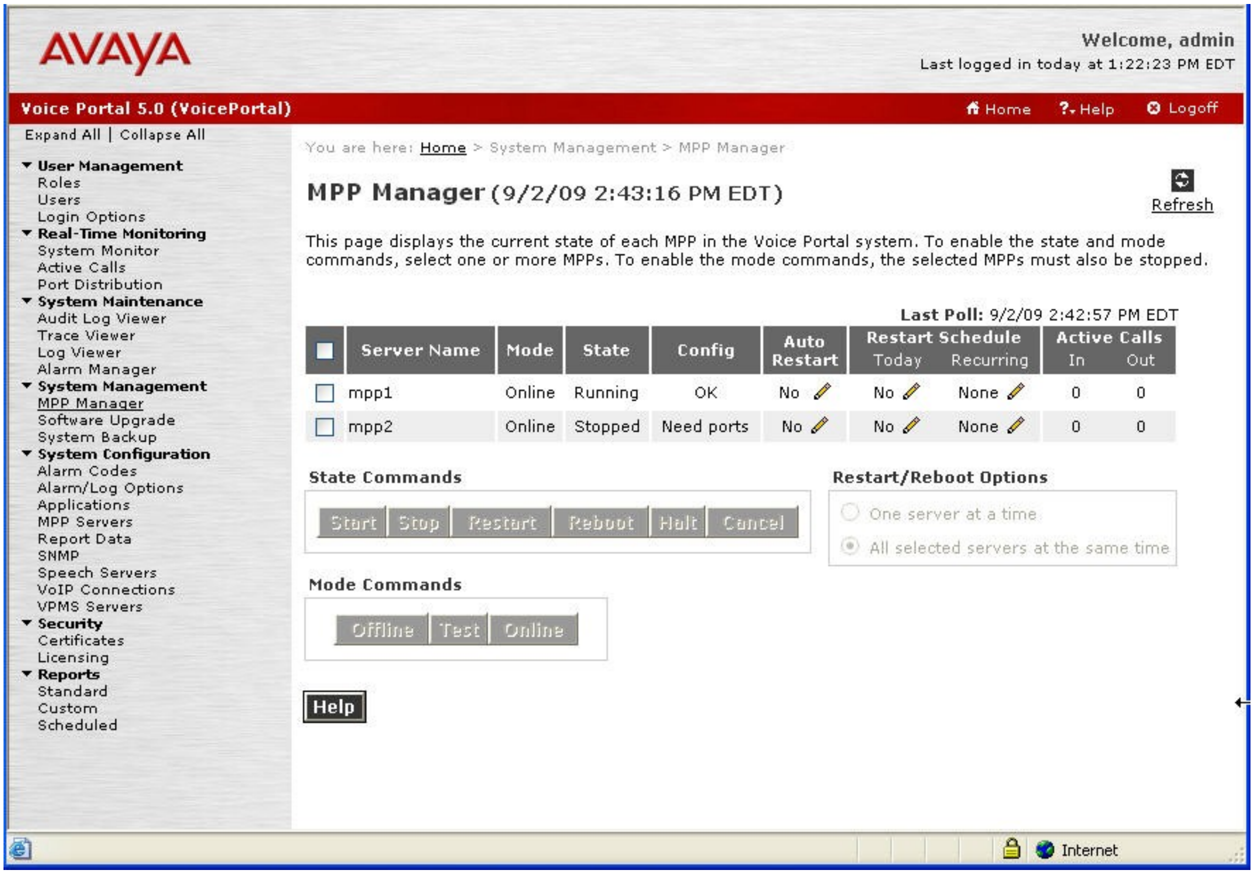
Adding a voice application for Avaya Voice Portal is part of Voice Portal's standard administration; this configuration is not directly related to achieving interoperability between the CBAD eVantage service and Avaya Voice Portal. It is included here for completeness.

Navigate to **System Configuration → Applications** to add a Voice Portal application. Specify a **Name** for the application, select the ***Yes*** radio button for **Enable,** set the **MIME Type** field to the appropriate value (e.g., ***VoiceXML***), and set the **VoiceXML URL** field to point to a VoiceXML application on the application server. Next, specify the type of **ASR** and **TTS** servers to be used by the application and the called number that invokes the application (***5136392085***, see **Section 2.1**). The configuration for the voice application used in the compliance test is shown in the screen below.



4.7. Start MPP Server

Start the MPP server from **System Management → MPP Manager** as shown below. Select the MPP for use and then click the **Start** button (the compliance test used only one MPP server; the other one shown in the screen was used for other purposes). The **Mode** of the started MPP should be ***Online*** and the **State** should be ***Running*** (when the other end of the SIP connection, i.e., the CUBE, has been properly configured).



5. Configure Avaya Aura™ Communication Manager

This section describes the administration steps for Avaya Aura™ Communication Manager in support of the sample configuration described in these Application Notes. The steps are performed from the System Access Terminal (SAT) interface of the Communication Manager.

These Application Notes assume that basic administration on Communication Manager, including stations (both H.323 and SIP), C-LAN, Media Processor, and announcement boards, etc., has already been performed. Similarly, these Application Notes assume that the proper configuration of the Avaya Aura™ SIP Enablement Services has already been performed to provide SIP support for the enterprise Avaya IP telephony network. These standard administration tasks are not directly related to achieving interoperability between the CBAD eVantage IP service and Avaya Voice Portal. Please consult [4], [5] and [6] for further details if necessary.

The administration procedures in this section include the following areas:

- System parameters
- Dial plan
- IP network parameters
- Inbound calls
- Call center

5.1. System Parameters

This section reviews the Communication Manager licenses and features that are required for the sample configuration described in these Application Notes. For required licenses that are not enabled in the steps that follow, contact an authorized Avaya account representative to obtain the licenses.

Enter the **display system-parameters customer-options** command. On Page 2 of the **system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of SIP trunks expected to be used.

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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 800   100
           Maximum Concurrently Registered IP Stations: 18000 1
             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: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 800   252
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

On Page 4 of the **system-parameters customer-options** form, verify that the bolded field in the following screenshot is set to "**y**".

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

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

            IP Attendant Consoles? y
```

5.2. Dial Plan

Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings administered in the sample configuration:

- 3-digit dial access codes (indicated with a **Call Type** of ***fac***) beginning with the digit **0** – the Call Center Automatic Call Distribution (ACD) feature access codes in this sample configuration conform to this format.
- 5-digit extensions with a **Call Type** of ***ext*** beginning with the digit ***2*** – local extensions for stations, Skill (Hunt Group) Extensions, Vector Directory Numbers (VDNs), and announcements in this sample configuration conform to this format.
- 5-digit extensions with a **Call Type** of **ext** beginning with the digit ***6*** – login ID's for ACD agents in this sample configuration conform to this format.
- 4-digit dial access codes (indicated with a **Call Type** of ***dac***) beginning with ***** – Trunk Access Codes (TACs) defined for trunk groups in this sample configuration conform to this format.

```
change 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
  0             3    fac
  2             5    ext
  6             5    ext
  *             4    dac
```

5.3. IP Network Parameters

These Application Notes assume that the appropriate IP network regions and IP codec sets have already been administered to support internal calls, i.e., calls within the Avaya site. For simplicity in this sample configuration, all Communication Manager elements, e.g., stations, C-LAN and MedPro boards, etc., within the Avaya site are assigned to a single IP network region and all internal calls use a single IP codec set. This section describes the steps for administering an additional IP network region to represent the CBAD eVantage IP service, and another IP codec set for transferred inbound calls, i.e., inbound calls from the CBAD eVantage IP service to Avaya Voice Portal that are subsequently transferred to Communication Manager.

1. Enter the **change ip-codec-set ci** command, where **ci** is the number of an IP codec set used only for internal calls. On Page 1 of the **ip-codec-set** form, ensure that ***G.711MU*** is included in the codec list as shown below.

```
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:
 3:
```

2. Enter the **change ip-codec-set ct** command, where **ct** is the number of an unused IP codec set. This IP codec set will be used for transferred inbound calls. On Page 1 of the **ip-codec-set** form, provision ***G.711MU*** as the only codec as shown below.

```
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.711MU           n         2        20
 2:
 3:
```

3. Enter the **change node-names ip** command, and add a node name and the private side IP address for the CUBE. Also note the node name and IP address of a C-LAN board that is assigned to one of the IP network regions administered for local Communication Manager elements within the Avaya site. This C-LAN board will be used in **Section 5.4, Step 1** for administering a SIP trunk to the CUBE.

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                 IP Address
CBTS-CUBE              10.45.108.81
CLAN1A                 10.45.108.55
```

4. Enter the **display ip-network-region nrc**, where **nrc** is the number of the IP network region to which the C-LAN board in **Step 3** is assigned. Note the value for **Authoritative Domain**.

```
change ip-network-region 1                                  Page   1 of  19
                                IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avayatest.com
    Name: PN1
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                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

5. Enter the **change ip-network-region nrv**, where **nrv** is the number of an unused IP network region. This IP network region will be used to represent the CBAD eVantage IP service.

```
Change ip-network-region 20                                  Page   1 of  19
                               IP NETWORK REGION
  Region: 20
Location:         Authoritative Domain:
    Name:
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
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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 3 of the **ip-network-region** form, for the IP network region pair consisting of this IP network region as the source region and the IP network region from Step 4 as the destination region (**dst rgn**), provision the following:

- **codec set** – Set to the codec set administered in **Step 2**.
- **direct WAN** – Set to ***y***.
- **WAN-BW-limits** – Set to the maximum number of calls or bandwidth allowed between the two IP network regions. The setting shown below was used for testing purposes only.

```
change ip-network-region 20                                  Page   3 of  19

 Source Region: 20  Inter Network Region Connection Management     I       M
                                                                   G  A    e
 dst codec direct  WAN-BW-limits   Video      Intervening    Dyn  A  G    a
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions       CAC  R  L    s
 1    2     y    NoLimit                                          n all
 2
 3
 4
```

5.4. Inbound Calls

This section describes the steps for administering the SIP trunks between Communication Manager and the CUBE for receiving the transferred calls from Avaya Voice Portal (through the CUBE).

1. Enter the **add signaling-group s** command, where **s** is the number of an unused signaling group, and provision the following:

   - **Group Type** – Set to ***sip***.
   - **Transport Method** – Set to ***tcp***. Note that this is the transport protocol used between the Communication Manager and the CUBE.
   - **Near-end Node Name** – Set to the node name of the C-LAN board noted in **Section 5.3, Step 3**.
   - **Far-end Node Name** – Set to the node name of the CUBE as administered in **Section 5.3, Step 3**.
   - **Near-end Listen Port** and **Far-end Listen Port** – set to ***5060***.
   - **Far-end Network Region** – Set to the IP network region administered in **Section 5.3, Step 5**.
   - **Far-end Domain** – Leave blank.
   - **DTMF over IP** – Set to ***rtp-payload*** to enable Communication Manager to use DTMF according to RFC 2833.
   - **Direct IP-IP Audio Connections** – Set to ***y***, indicating that the RTP paths should be optimized to reduce the use of the MedPro resources on Avaya G650 Media Gateway when possible.

```
add signaling-group 20                                          Page   1 of   1

 Group Number: 20             Group Type: sip
                        Transport Method: tcp
  IMS Enabled? n

   Near-end Node Name: CLAN1A                Far-end Node Name: CBTS-CUBE
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 20
      Far-end Domain:

                                           Bypass If IP Threshold Exceeded? 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? n                   Direct IP-IP Early Media? n
 H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 6
```

2. Enter the **add trunk-group t** command, where **t** is the number of an unused trunk group. On Page 1 of the **trunk-group** form, provision the following:
   - **Group Type** – Set to ***sip***.
   - **Group Name** – Enter a descriptive name.
   - **TAC** – Enter a trunk access code that is consistent with the dial plan as defined in **Section 5.2**.
   - **Direction** – Set to ***incoming***.
   - **Service Type** – Set to ***public-ntwrk***.
   - **Signaling Group** – Set to the number of the signaling group administered in **Step 1**.
   - **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group.

```
add trunk-group 20                                          Page   1 of  21
                              TRUNK GROUP

Group Number: 20                 Group Type: sip           CDR Reports: y
  Group Name: CBTS-CUBE                 COR: 1        TN: 1        TAC: *020
   Direction: incoming     Outgoing Display? n
 Dial Access? n                                  Night Service:

Service Type: public-ntwrk        Auth Code? n

                                                     Signaling Group: 20
                                                   Number of Members: 40
```

3. Enter the **change public-unknown-numbering 0** command to specify the connected party numbers sent on transferred inbound calls. Provision an entry for each local extension range assigned to phones, agents, skills (hunt groups), and VDNs on Communication Manager as follows:

    - **Ext Len** – Enter the total number of digits in the local extension range.
    - **Ext Code –** Enter enough leading digits to identify the local extension range.
    - **Trk Grp(s)** – Enter the number of the trunk group administered in **Step 2**.
    - **CPN Prefix** – If necessary, enter enough prefix digits to form the desired connected party number.
    - **Total CPN Len** – Enter the total length of the connected party number to be sent.

    As shown below, for transferred calls to Communication Manager 5-digit connected party numbers 2xxxx and 6xxxx are sent (i.e., the connected party's extension is sent without modification).

```
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: 3
 5  2            20                        5            Maximum Entries: 9999
 5  6            20                        5
```

5.5. Call Center

The configuration of Communication Manager Call Center elements – ACD (Automatic Call Distribution) enablement, agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are standard administration procedures not directly related to achieving interoperability between the CBAD eVantage IP service and Avaya Voice Portal, and therefore beyond the scope of these Application Notes. Consult [4], [5], [7] and [8] for further details if necessary. The samples that follow are provided for reference purposes only. The bolded entries in the sample forms were used for the compliance test.

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

                          Call Center Release: 5.0

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

Sample Call Center Optional Features Form – Page 6

```
display system-parameters features                            Page  11 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                   Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
               Converse Signaling Tone (msec): 100         Pause (msec): 70
                     Prompting Timeout (secs): 10
                  Interflow-qpos EWT Threshold: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                            BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
```

Sample Feature-Related System Parameters Form – Page 11

```
display system-parameters features                              Page  12 of  18
                        FEATURE-RELATED SYSTEM PARAMETERS

  AGENT AND CALL SELECTION
                         MIA Across Splits or Skills? n
                          ACW Agents Considered Idle? y
                          Call Selection Measurement: current-wait-time
    Service Level Supervisor Call Selection Override? n
                                 Auto Reserve Agents: none


  CALL MANAGEMENT SYSTEM
                            REPORTING ADJUNCT RELEASE
                                       CMS (appl mis):
                                       IQ  (appl ccr):

                               BCMS/VuStats LoginIDs? y
                 BCMS/VuStats Measurement Interval: hour
         BCMS/VuStats Abandon Call Timer (seconds):
                   Validate BCMS/VuStats Login IDs? n
                          Clear VuStats Shift Data: on-login
               Remove Inactive BCMS/VuStats Agents? n
```

Sample Feature-Related System Parameters Form – Page 12

```
display feature-access-codes                                    Page   5 of   8
                               FEATURE ACCESS CODE (FAC)

                         Automatic Call Distribution Features

                    After Call Work Access Code:
                             Assist Access Code:
                            Auto-In Access Code: 017
                           Aux Work Access Code: 019
                              Login Access Code: 015
                             Logout Access Code: 016
                          Manual-in Access Code: 018
      Service Observing Listen Only Access Code:
      Service Observing Listen/Talk Access Code:
          Service Observing No Talk Access Code:
                    Add Agent Skill Access Code:
                 Remove Agent Skill Access Code:
             Remote Logout of Agent Access Code:
```

Sample Feature Access Code (FAC) Form – Page 5

```
display hunt-group 100                                          Page   1 of   3
                                  HUNT GROUP

            Group Number: 100                              ACD? y
              Group Name: 100                            Queue? y
         Group Extension: 20200                         Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:

             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

Sample Hunt Group (Skill) Form – Page 1

```
display hunt-group 100                                          Page   2 of   3
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none            Service Objective (sec): 20
     Supervisor Extension:                Service Level Supervisor? n


      Controlling Adjunct: none



 Timed ACW Interval (sec):                  Dynamic Queue Position? n
   Multiple Call Handling: none


Interruptible Aux Threshold: none
                                 Redirect on No Answer (rings):
                                               Redirect to VDN:
                     Forced Entry of Stroke Counts or Call Work Codes? n
```

Sample Hunt Group (Skill) Form – Page 2

```
display agent-loginID 61001                                   Page   1 of   2
                                 AGENT LOGINID

                Login ID: 61000                                   AAS? n
                    Name: Agent-61000                           AUDIX? n
                      TN: 1                             LWC Reception: spe
                     COR: 1                    LWC Log External Calls? n
           Coverage Path:                    AUDIX Name for Messaging:
           Security Code:
                                         LoginID for ISDN/SIP Display? n
                                                             Password:
                                               Password (enter again):
                                                          Auto Answer: station
                                                    MIA Across Skills: system
                                            ACW Agent Considered Idle: system
                                            Aux Work Reason Code Type: system
                                              Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                             Forced Agent Logout Time:   :
```

Sample Agent Form – Page 1

```
display agent-loginID 61001                                   Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                                Service Objective? n
Call Handling Preference: skill-level              Local Call Preference? n

    SN   RL SL          SN   RL SL          SN   RL SL          SN   RL SL
 1: 100     1       16:                 31:                 46:
 2:                 17:                 32:                 47:
 3:                 18:                 33:                 48:
 4:                 19:                 34:                 49:
 5:                 20:                 35:                 50:
 6:                 21:                 36:                 51:
 7:                 22:                 37:                 52:
 8:                 23:                 38:                 53:
 9:                 24:                 39:                 54:
10:                 25:                 40:                 55:
11:                 26:                 41:                 56:
12:                 27:                 42:                 57:
13:                 28:                 43:                 58:
14:                 29:                 44:                 59:
15:                 30:                 45:                 60:
```

Sample Agent Form – Page 2

```
display vector 110                                          Page   1 of   6
                                  CALL VECTOR

    Number: 110              Name: VP Test Vector 1
          Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y  ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y  Holidays? y
 Variables? y   3.0 Enhanced? y
01 announcement 22221
02 queue-to     skill 1st  pri m
03 stop
04
05
06
07
08
09
10
11
12
```

Sample Vector Form – Page 1

```
display vector 120                                          Page   1 of   6
                                  CALL VECTOR

    Number: 100              Name: VP Test Vector 2
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n          Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y  ASAI Routing? y
 Prompting? y   LAI? y  G3V4 Adv Route? y   CINFO? y   BSR? y  Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    6   secs hearing ringback
02 announcement 22221
03 queue-to     skill 1st  pri m
04 wait-time    10  secs hearing music
05 announcement 22222
06 goto step    4             if unconditionally
07 stop
08
09
10
11
12
```

Sample Vector Form – Page 1

```
display vdn 20110                                              Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 20110
                                 Name*: VP-VDN1
                           Destination: Vector Number        110
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

               Service Objective (sec): 20

                           1st Skill*: 100
                           2nd Skill*:
                           3rd Skill*:



* Follows VDN Override Rules
```

Sample Vector Directory Number Form – Page 1

```
display vdn 20120                                              Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 20120
                                 Name*: VP-VDN2
                           Destination: Vector Number        120
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none

               Service Objective (sec): 20

                           1st Skill*: 100
                           2nd Skill*:
                           3rd Skill*:



* Follows VDN Override Rules
```

Sample Vector Directory Number Form – Page 1

6. Configure Cisco Unified Border Element (CUBE)

The CUBE configuration used in the sample configuration is provided below as reference. Refer to **Table 1** in **Section 2.1** for the various IP addresses used in the CUBE configuration. Also note that the usernames and passwords contained in the configuration were masked as **xxxxxxxx** for security reasons.

In real deployment at customer sites, Cincinnati Bell will take the responsibility for provisioning the CUBE (including installation and configuration) even though this device will be placed as Customer Premise Equipment (CPE) at the edge of the enterprise IP network.

```
Current configuration : 3566 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname DevConnectCUBE
!
boot-start-marker
boot system flash:c2801-adventerprisek9_ivs-mz.124-24.T1.bin
boot-end-marker
!
logging message-counter syslog
logging buffered 4096
enable password xxxxxxxx
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
dot11 syslog
ip source-route
!
!
!
!
ip cef
ip name-server 12.127.16.67
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
no voice call carrier capacity active
!
voice service voip
```

```
 address-hiding
 allow-connections sip to sip
 fax protocol cisco
 sip
  localhost dns:as.voip.fuse.net
   outbound-proxy dns:edge.voip.fuse.net
!
!
!
voice class codec 99
 codec preference 1 g729r8
 codec preference 2 g711ulaw
 codec preference 3 g711alaw
!
!
!
!
!
!
!
!
!
!
!
!
!
!
voice-card 0
 dsp services dspfarm
!
!
!
!
!
username xxxxxxxx password xxxxxxxx
archive
 log config
  hidekeys
!
!
!
!
!
ip tcp synwait-time 5
ip ftp username xxxxxxxx
ip ftp password xxxxxxxx
!
class-map match-all class11
 description --- match VoIP RTP ---
 match access-group 111
class-map match-all class10
 description --- match VoIP signaling ---
 match access-group 110
!
!
```

```
policy-map udp-policy
 class class10
    priority percent 9
 class class11
    priority percent 65
!
!
translation-rule 40
 Rule 1 null null
!
!
!
!
!
interface FastEthernet0/0
 description --- WAN ---
 ip address 22.160.183.211 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.45.108.81 255.255.255.0
 speed 100
 full-duplex
!
ip default-gateway 22.160.183.193
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 22.160.183.193
ip route 10.45.122.0 255.255.255.0 10.45.108.1
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
!
!
control-plane
!
!
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
dial-peer voice 100 voip
 description OutToAcme
 destination-pattern .T
 voice-class codec 99
 session protocol sipv2
```

```
 session target dns:as.voip.fuse.net
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 101 voip
 description OutToAvaya
 destination-pattern 513639208.
 voice-class codec 99
 voice-class sip outbound-proxy ipv4:10.45.122.131
 session protocol sipv2
 session target ipv4:10.45.122.131
 session transport tcp
 incoming called-number .
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 2 voip
 description OutToAvayaCM
 destination-pattern 2....
 voice-class codec 99
 voice-class sip outbound-proxy ipv4:10.45.108.55
 session protocol sipv2
 session target ipv4:10.45.108.55
 session transport tcp
 incoming called-number 5136392085
 dtmf-relay rtp-nte
 no vad
!
!
gateway
 timer receive-rtp 1200
!
sip-ua
 credentials username 5136392085 password 7
014355560E5F225F001D68593C5245432E5D22 realm as.voip.fuse.net
 credentials username 5136392086 password 7
1542595E537B79710962677244523554520770 realm as.voip.fuse.net
 credentials username 5136392087 password 7
101F5D4A5347465B2D557F7B717F6A627B4452 realm as.voip.fuse.net
 calling-info sip-to-pstn number set 5136392085
 no remote-party-id
 retry invite 2
 retry response 3
 retry bye 3
 retry prack 6
 timers expires 300000
 registrar dns:as.voip.fuse.net expires 1800
 sip-server dns:as.voip.fuse.net
 connection-reuse
!
!
!
gatekeeper
 shutdown
!
```

```
!
line con 0
line aux 0
line vty 0 4
 session-timeout 60
 login local
 transport input telnet ssh
line vty 5 15
 session-timeout 60
 privilege level 15
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
end
```

7. General Test Approach and Test Results

The test environment was comprised of:

- A simulated enterprise site with Avaya Voice Portal, Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya IP phones (H.323 and SIP), an Cisco Unified Border Element (CUBE), an HTTP application server, and a speech server (Nuance OpenSpeech Recognizer and Nuance RealSpeak).
- A laboratory version of the Cincinnati Bell Any Distance eVantage IP service, to which the simulated enterprise site was connected via the public IP network.

The main test objectives were to verify the following features and functionality:

- Inbound calls to access Avaya Voice Portal.
- Inbound caller interaction with Avaya Voice Portal, including prompting, caller DTMF input, speech recognition, and TTS functionality.
- Canvassing of Communication Manager skills for agent availability before transferring inbound call to the skills.
- Transferring inbound calls to Communication Manager skills regardless of agent availability.
- Call and two-way talk path establishment between callers and Communication Manager agents following transfers from Avaya Voice Portal.
- G.711 mu-law codec support.
- DTMF tones / RFC 2833 support.
- SIP trunking interface between CUBE and Avaya Voice Portal.
- Serviceability testing on recovery from network failure and power outage.

The above test objectives with the limitation as noted in **Section 1.3** were verified. The compliance test passed successfully.

8. Verification Steps

8.1. Verification Tests

The following steps may be used to verify the configuration:

1. Place an inbound call to an Avaya Voice Portal application, and verify that two-way talk path exists. Interact with the Avaya Voice Portal prompts and verify that the call remains stable for several minutes and disconnect properly.
2. Place an inbound call to an Avaya Voice Portal application that can canvass an Avaya Aura™ Communication Manager skill for agent availability, and select the appropriate prompt(s) to request a transfer to an agent. Verify that when no agent in the skill is available, the caller hears wait treatment while waiting to be transferred. Verify that when an agent in the skill becomes available, the call is successfully transferred to the agent and two-way talk path exists between the caller and the agent.
3. Place an inbound call to an Avaya Voice Portal application that can transfer an inbound call to a Communication Manager skill regardless of agent availability, and select the appropriate prompt(s) to request a transfer to an agent. Verify that the transfer completes successfully. Verify that when no agent in the skill is available, the call does not drop. Verify that when an agent in the skill becomes available, the call is successfully routed to the agent and two-way talk path exists between the caller and the agent.

8.2. Troubleshooting Tools

The Communication Manager **list trace vector**, **list trace vdn**, **list trace tac**, and/or **status trunk-group** commands are helpful diagnostic tools to verify correct operation and to troubleshoot problems. MST (Message Sequence Trace) diagnostic traces (performed by Avaya Support) can be helpful in understanding the specific interoperability issues.

The logging and reporting functions within the Avaya VPMS web interface may be used to examine the details of Avaya Voice Portal calls. In addition, if port monitoring is available, a SIP protocol analyzer such as Wireshark (a.k.a. Ethereal) can be used to capture SIP traces at the various interfaces. SIP traces can be instrumental in understanding SIP protocol issues resulting from configuration problems.

9. Conclusion

These Application Notes describe the steps for configuring Avaya Voice Portal with the CBAD eVantage IP service using a SIP trunking interface. The compliance test verified successfully that the CBAD eVantage IP service can interoperate with Avaya Voice Portal via a properly configured SIP trunking interface.

The sample 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. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

10. References

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

[1] *Planning for Voice Portal*, March 2009.
[2] *Implementing Voice Portal on multiple servers*, March 2009.
[3] *Administering Voice Portal*, March 2009.
[4] *Administering Avaya Aura^TM Communication Manager*, Doc # 03-300509, May 2009.
[5] *Avaya Aura^TM Communication Manager Feature Description and Implementation*, Doc # 555-245-205, May 2009.
[6] *Administering Avaya Aura^TM SIP Enablement Services on the Avaya S8300 Server*, Doc # 03-602508, May 2009.
[7] *Avaya Call Center Release 5.0 Call Vectoring and Expert Agent Selection (EAS) Guide*, Release 5.0, January 2008, Document Number 07-600780.
[8] *Avaya Call Center Release 5.0 Automatic Call Distribution (ACD) Guide*, Release 5.0, January 2008, Document Number 07-602568.

Cincinnati Bell eVantage service description and other information:
[9] http://www.evolvebusinesssolutions.com/eVantage/

11. Change History

Issue	Date	Reason
0.1	09/15/2009	Initial issue
0.2	09/25/2009	Reviewed by Cincinnati Bell

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.