Avaya Solution & Interoperability Test Lab

Application Notes for configuring Amcom Speech Auto Attendant Version 7.0 with Avaya Aura® Communication Manager 6.2 and Avaya Aura® Session Manager 6.2 – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Amcom Speech Auto Attendant with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The solution used Avaya Aura® Session Manager to route calls between Avaya Aura® Communication Manager and Amcom Speech Auto Attendant. The overall objective of the interoperability compliance testing was to verify the basic functions of Amcom Speech Auto Attendant with Avaya Aura® Communication Manager using a SIP trunk.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the procedures to integrate Amcom Speech Auto Attendant application with Avaya Aura® Communication Manager via a SIP trunk configured on Avaya Aura® Session Manager. Avaya Aura® Session Manager provides SIP trunking and network routing service to route calls between Avaya Aura ® Communication Manager and the Amcom Speech Auto Attendant server. Amcom Speech Auto Attendant is an Intelligent Virtual Agent that provides natural interaction with the SDC Comprehensive Database using speech recognition. IntelliSPEECH allows callers to connect their call, initiate a page, or access information by saying a command rather than using operator assistance or confusing touchtone menus.

2. General Test Approach and Test Results

The general test approach was to verify test calls made from Avaya Aura® Communication Manager to Amcom Speech Auto Attendant to exercise basic features such as DTMF, PIN, speech recognition, and call transfer.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute a full product performance or feature testing performed by third party vendors, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a third party solution.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP trunks between Session Manager and Amcom Speech server.
- Basic features on the speech server: DTMF, speech recognition and blind transfer.
- Basic telephony features on Communication Manager: hold and retrieve call, voice mail.
- Transfer calls off-net via SIP trunk.
- Codec negotiation: G.711 and G.729.

2.2. Test Results

All test cases passed.

2.3. Support

For technical support on the Amcom Speech Intelligent Auto Attendant product, contact Amcom software support via telephone or their website below.

- **Telephone:** (888) 797-7487
- **Web:** http://www.amcomsoftware.com

3. Reference Configuration

Figure 1 illustrates a sample configuration used for the compliance test. Avaya Aura® Communication Manager is considered as the main switch for the compliance test with Amcom Speech Auto Attendant. Avaya Aura® Communication Manager, Avaya Communication Server 1000 system and Amcom Speech server have SIP trunks to Avaya Aura® Session Manager. The Avaya CS1000 is used to receive the transferred call from Communication Manager for transferring calls off-net. The compliance test used Avaya Aura® Messaging as the voicemail system.

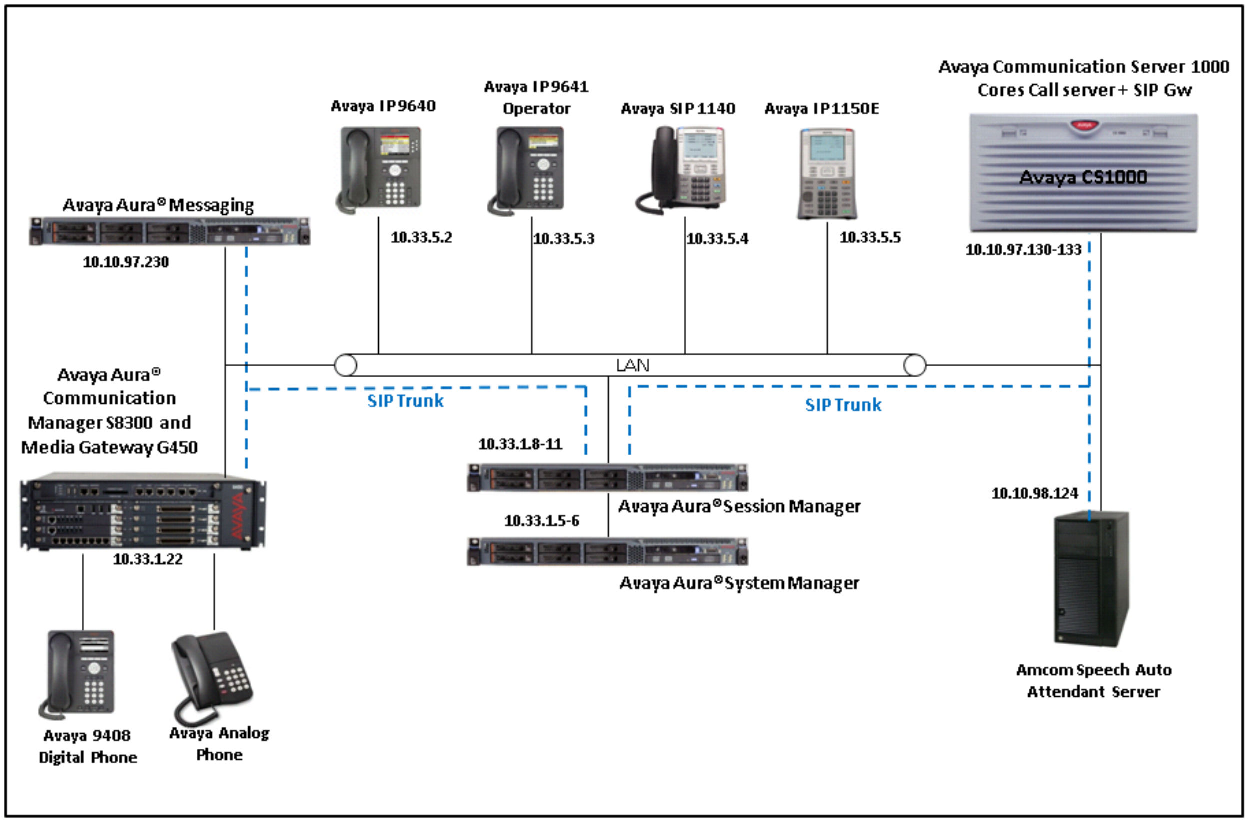


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

The following equipment and software were used for the compliance test:

Equipment/Software	Release/Version
Avaya S8800 server running Avaya Aura® Session Manager Server	Avaya Aura® Session Manager 6.2 (Build No 6.2.2.0.6225)
Avaya S8800 server running Avaya Aura® System Manager Server	Avaya Aura® System Manager 6.2.0 SP2 (Build No: 6.2.0.0.15669-6.2.12.202 Software No: 6.2.14.1.1925)
Avaya S8300D Server	Avaya Aura® Communication Manager 6.2 Build R016x.02.0.823.0
Avaya Media Gateway G450	31 .22 .0.1
Avaya S8800 Server	Avaya Aura® Messaging 6.1 SP2
Avaya Communication Server 1000E/CPPM	Avaya Communication Server 1000 Release 7.5 Q+ Deplist 1 (created: 2012-07-23) and Service Update 1 (Created: 2012-0708)
Avaya IP SIP Phone 1140E	4.3
Avaya IP H.323 9640	3.1.03
Avaya IP Unistim Phone 1150E	0x27C8J
Avaya IP SIP 9641	6.2.0
Amcom Speech Auto Attendant	7.0.001
Amcom Speech Operating System	Windows 2008 R2 64-Bit
Amcom Middleware SIP Manager=FreeSwitch	Version 1.2.0

5. Configure Avaya Aura® Communication Manager

This document assumes that the Avaya Aura® Communication Manager system was properly installed and configured per the product documentation. This section provides the steps on how to provision Communication Manager to work with the Amcom Speech Auto Attendant server. For more information about how to install and configure Avaya Aura® Communication Manager, please refer to **Section 10 [1]**.

The following summarizes the tasks which need to be done on Communication Manager:

- Verify the Communication Manager license.
- Configure IP Node Name.
- Configure IP Codec.
- Configure IP Network Region.
- Configure SIP Signaling Group.
- Configure Trunk Group.
- Configure Route Pattern.
- Configure Dialing Plan and AAR Table.

5.1. 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.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

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

      IP PORT CAPACITIES                                                USED
                          Maximum Administered H.323 Trunks: 4000   0
                Maximum Concurrently Registered IP Stations: 2400   2
                  Maximum Administered Remote Office Trunks: 4000   0
     Maximum Concurrently Registered Remote Office Stations: 2400   0
                   Maximum Concurrently Registered IP eCons: 68     0
       Max Concur Registered Unauthenticated H.323 Stations: 100    0
                             Maximum Video Capable Stations: 2400   0
                        Maximum Video Capable IP Softphones: 2400   0
                            Maximum Administered SIP Trunks: 4000  15
       Maximum Administered Ad-hoc Video Conferencing Ports: 4000   0
        Maximum Number of DS1 Boards with Echo Cancellation: 80     0
                                  Maximum TN2501 VAL Boards: 10     0
                          Maximum Media Gateway VAL Sources: 50     0
                Maximum TN2602 Boards with 80 VoIP Channels: 128    0
               Maximum TN2602 Boards with 320 VoIP Channels: 128    0
        Maximum Number of Expanded Meet-me Conference Ports: 300    0

           (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Configure IP Node Name

This section describes the steps for setting an IP node name for Session Manager in Communication Manager. Enter the "**change node-names ip"** command, and add a node name for Session Manager and its IP address. Make a note for the Communication Manager "**procr**" IP address.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
default                0.0.0.0
interopsm              10.33.1.11
procr                  10.33.1.22
procr6                 ::
```

5.3. Configure IP Codec

The IP codec set is used in the IP network region for communications between Communication Manager and Session Manager. To administer the IP Codec in Communication Manager, enter "**change ip-codec-set <n>**" command, where **n** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** when configuring an IP network region to specify which audio codecs may be used within and between network regions. In the sample configuration, only one network region is used.

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

                          IP Codec Set

    Codec Set: 1

    Audio         Silence       Frames   Packet
    Codec         Suppression   Per Pkt  Size(ms)
 1: G.711MU            n          2         20
 2: G.729              n          2         20
 3: G.722-64K                     2         20
 4: G.722.1-32K                   1         20
 5: G.722.1-24K                   1         20
 6: G.722.2            n          1         20
 7:
```

5.4. Configure IP Network Region

To administer the IP Network Region, enter "**change ip-network-region <n>**" command, where **n** is a number between **1** and **250** inclusive, configure the following and leave other fields at default.

- **Authoritative Domain**: Enter the appropriate value. This will be used in **Section 5.5** and **Section 6.1**. In the test configuration, SIP domain name "**bvwdev.com**" was used.
- **Codec Set**: Enter the IP codec set number **1** as provisioned in **Section 5.3**.

```
change ip-network-region 1                                          Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1        Authoritative Domain: bvwdev.com
    Name: Main Network Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
```

5.5. Configure SIP Signaling Group

To configure SIP signaling group, enter "**add signaling-group <s>**" command, where **s** is an available signaling group, configure the following fields and leave the others at default:

- **Group Type**: Set to "**sip**".
- **Transport Method**: Set to "**tcp**".
- **Peer Detection Enabled?**: Set to "**y**".
- **Peer Server:** Set to "**SM**". Note: To change this field to "**SM**", the default is "**others**". Firstly set "**n**" in the field **Peer Detection Enabled?** and then change from "**others**" to "**SM**" and go back to the **Peer Detection Enabled?** field set to "**y**".
- **Near-end Node Name**: Set to "**procr**".
- **Near-end Listen Port**: Set to "**5060**".
- **Far-end Node Name**: Set to "**interopsm**" as defined in **Section 5.2**.
- **Far-end Listen Port**: Set to "**5060**".
- **Far-end Network Region**: Set to "**1**" as configured in **Section 5.4**.
- **Far-end Domain Name**: Set to "**bvwdev.com**" as the same as configured in the IP Network region.

```
add signaling-group 1                                            Page   1 of   2
                                SIGNALING GROUP

 Group Number: 10             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                     Far-end Node Name: interopsm
 Near-end Listen Port: 5060                    Far-end Listen Port: 5060
                                            Far-end Network Region: 1
                                       Far-end Secondary Node Name:
Far-end Domain: bvwdev.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

5.6. Configure Trunk Group

To administer SIP trunk group, enter "**add trunk-group <t>**" command, where **t** is an unallocated trunk group, configure the following fields and leave others at default:

- **Group Type**: Set to "**sip**".
- **Group Name**: Give a descriptive name, e.g. "**SIP Trunk to Interop SM**".
- **TAC**: Set to "**#01**". This value must be consistent with the existing dialplan.
- **Service Type**: Set to "**tie**".
- **Signaling Group**: Set to "**1**" as configured in **Section 5.5**.
- **Number of Members**: Set to "**15**".

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

Group Number: 10                   Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to Interop SM     COR: 1        TN: 1        TAC: #01
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                            Member Assignment Method: auto
                                                    Signaling Group: 1
                                                  Number of Members: 15
```

Go to Page 3, and set "**private**" in the Numbering Format as this trunk group is used as part of private dialing plan.

```
add trunk-group 1                                             Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n             Measured: none
                                                      Maintenance Tests? y



                     Numbering Format: private
                                              UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y

 DSN Term? n
```

5.7. Configure Route Pattern

To configure a route pattern corresponding to the newly added SIP trunk group. Use the "**change route-pattern <n>**" command, where "**n**" is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields. Submit these changes.

- **Pattern Name**: Enter a descriptive name, e.g., "to **SM**".
- **Grp No**: Set to the trunk group "**1**" as configured in **Section 5.6**.
- **Numbering Format**: Set to "**lev0-pvt**".

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 10  Pattern Name: to SM
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1   0                                                               n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               lev0-pvt  none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

5.8. Configure Dial Plan and AAR Analysis Table

This section provides sample Uniform dial plan and Automatic Alternate Routing (AAR) used for routing calls with dialed digits 720x to the Amcom Speech server. Note that other methods of routing may be used. Use the "**change dialplan analysis**" command, and add an entry to specify use of UDP dial plan for routing of digits **720x**. 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 "**720**".
- **Total Length:** Length of the full dialed number, in this case "**4**"
- **Call Type:** "**udp**"

```
change dialplan analysis                                           Page   1 of  12
                              DIAL PLAN ANALYSIS TABLE
                                   Location: all              Percent Full: 3

   Dialed     Total  Call       Dialed     Total  Call       Dialed     Total  Call
   String     Length Type       String     Length Type       String     Length Type
  33            5    ext       #             2    fac
  400           5    ext       #             3    fac
  505           6    udp       #10           3    dac
  53            5    udp
  54            5    udp
  58            5    udp
  600           5    udp
  720           4    udp
  730           4    udp
  75            5    udp
  8             1    fac
  *             1    fac
  *             2    fac
  *             3    fac
  *             4    dac
```

Use the "**change uniform-dialplan 0**" command and add an entry of prefix **720** and specify "**aar**" as the routing method in the **Net** column for this dial pattern.

```
change uniform-dialplan 0                                          Page   1 of   2
                         UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                       Insert               Node
  Pattern          Len  Del      Digits     Net  Conv Num
 33                 5    0                  aar   n
 505                6    0                  aar   n
 53                 5    0                  aar   n
 54                 5    0                  aar   n
 58                 5    0                  aar   n
 600                5    0                  aar   n
 720                4    0                  aar   n
 730                4    0                  aar   n
 75                 5    0                  aar   n
                                                  n
```

Use the "**change aar 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 "**720**".
- **Total Min:** Minimum number of digits, in this case "**4**".
- **Total Max:** Maximum number of digits, in this case "**4**".
- **Route Pattern:** The route pattern number from **Section 5.7**. i.e., "**1**".
- **Call Type:** "**aar**".

```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all             Percent Full: 3

          Dialed                Total      Route      Call    Node   ANI
          String              Min   Max   Pattern     Type    Num    Reqd
    2                         7     7      254        aar            n
    33                        5     5      10         aar            n
    4                         7     7      254        aar            n
    400                       5     5      10         aar            n
    505                       6     6      10         aar            n
    53                        5     5      10         aar            n
    54                        5     5      10         aar            n
    58                        5     5      10         aar            n
    600                       5     5      10         aar            n
    7                         7     7      254        aar            n
    720                       4     4      10         aar            n
    730                       4     4      10         aar            n
```

6. Configure Avaya Aura® Session Manager

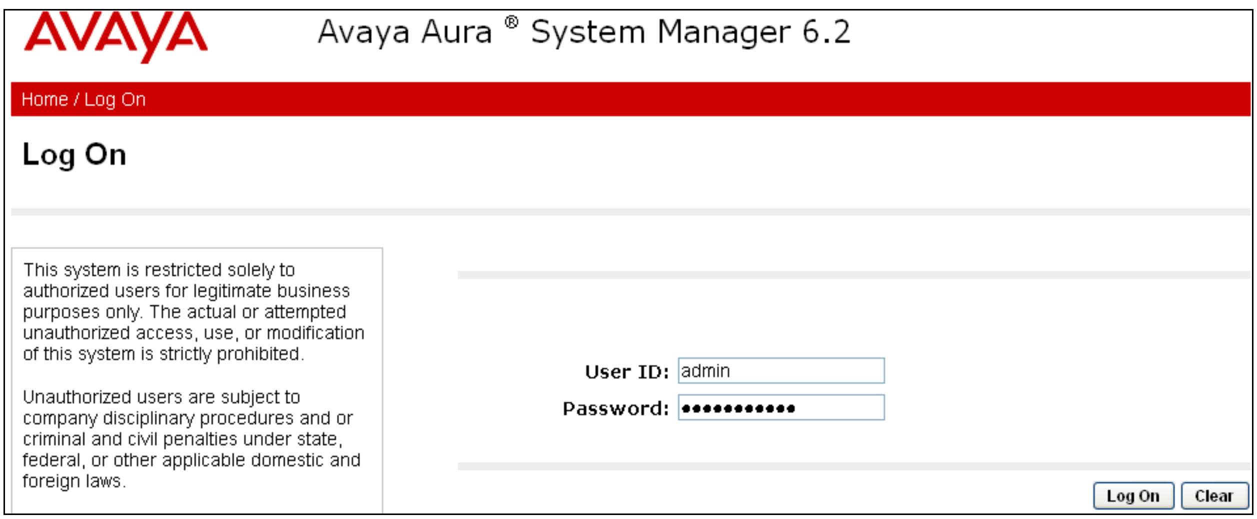
This section provides the procedures for configuring Session Manager. Session Manager is comprised of two functional components: The Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager web interface and is then downloaded into Session Manager.

This section assumes that Session Manager and System Manager have been installed, and network connectivity exists between the two platforms. The following steps describe the configuration needed for Session Manager.

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Routing Policy
- Dial Patterns
- Manage Element

6.1. Configure SIP Domain

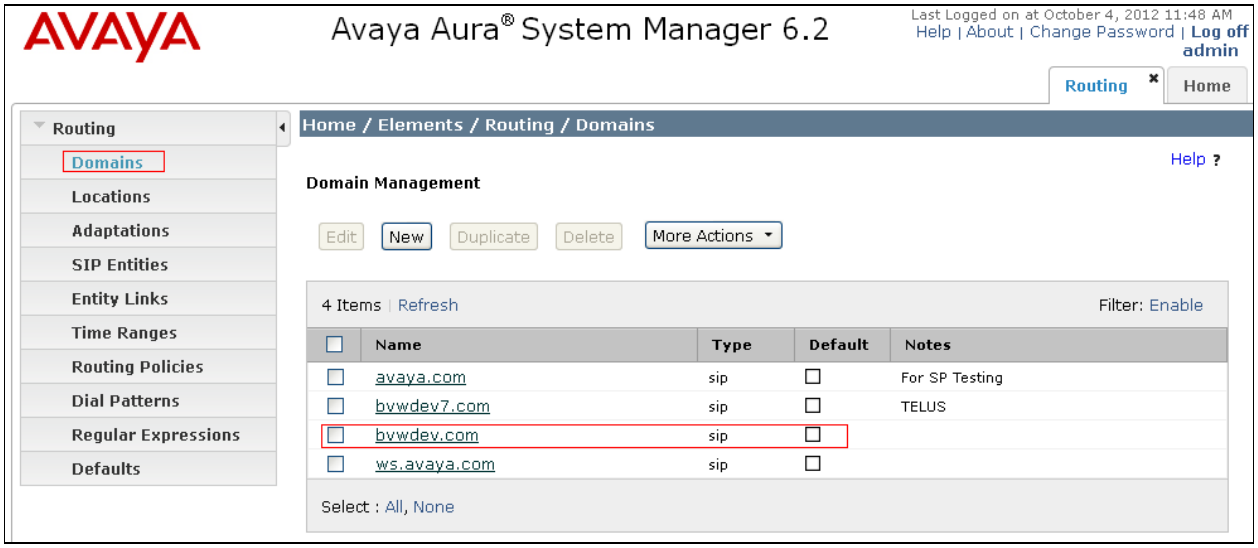
Launch a web browser, enter **https://<IP address of System Manager>** in the URL, and log in with the appropriate credentials.



Navigate to **Elements→Routing→Domains** and click on the **New** button to create a new SIP Domain (screen not shown). Enter the following values and use defaults for the remaining fields:

- **Name** –Enter the Authoritative Domain name specified in the signaling group of Communication Manager in **Section 5.5**, which is "**bvwdev.com**".
- **Type** – Select **SIP**

Click **Commit** to save. The following screen shows the Domains page, listed is the newly created domain that was used during the compliance test.



6.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. This is used for bandwidth management or location-based routing.

Navigate to **Routing→Locations**, and click on the **New** button to create a new SIP Entity location (screen not shown).

General section

Enter the following values and use default values for the remaining fields.

- Enter a descriptive Location in the **Name** field (e.g. **Belleville**).
- Enter a description in the **Notes** field if desired.

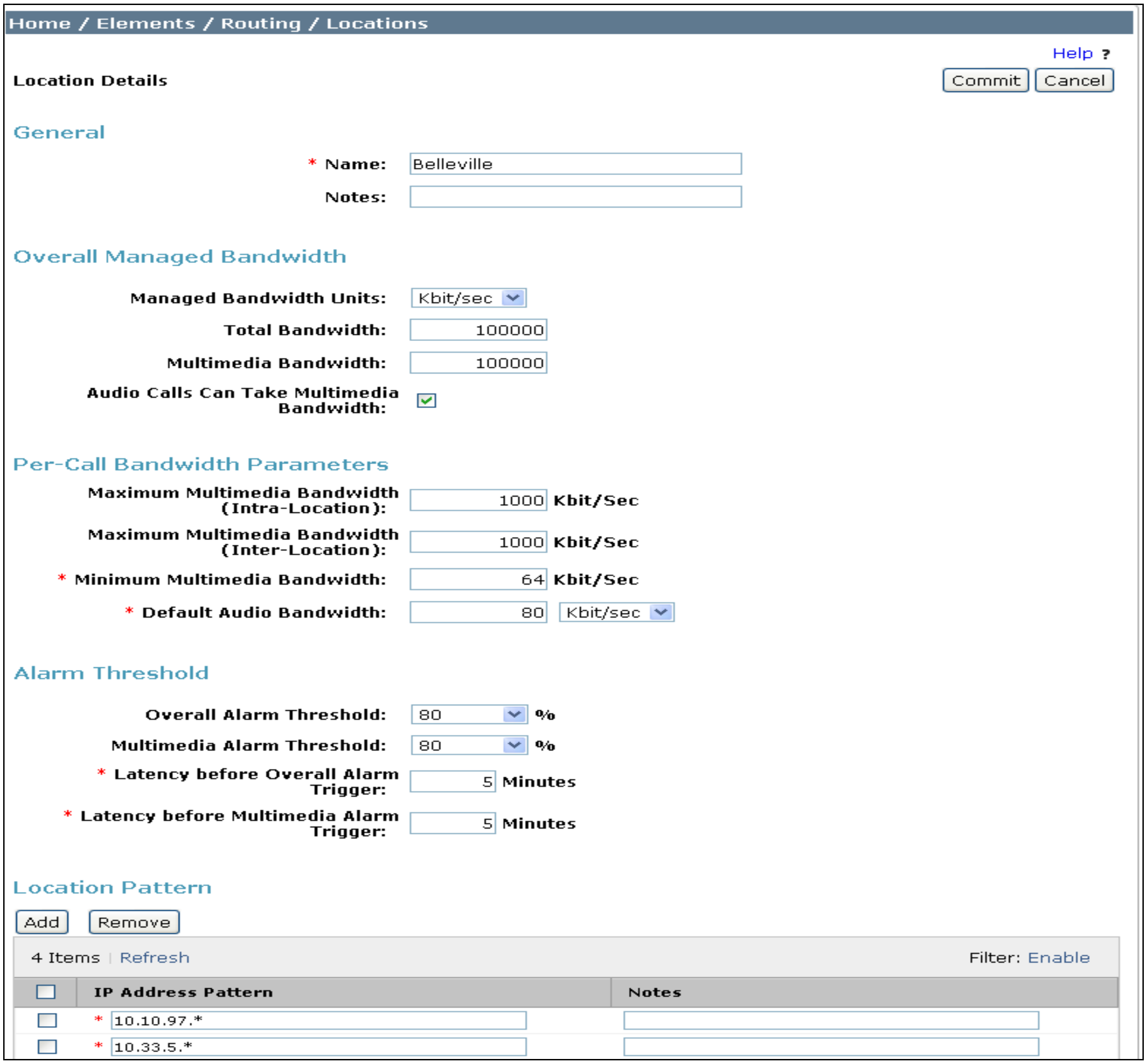
Location Pattern section

Click **Add** and enter the following values:

- The IP address information for the **IP address Pattern** (e.g. **10.10.97.***).
- A description in the **Notes** field if desired.

Repeat these steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button.

Repeat all the steps for each new Location. The following screen shows the **Location** used during the compliance test.



6.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk. During the compliance test the following SIP Entities were configured:

- Session Manager
- Communication Manager
- Amcom Speech server

Navigate to **Routing →SIP Entities** and click on the **New** button to create a new SIP entity (screen not shown). Provide the following information:

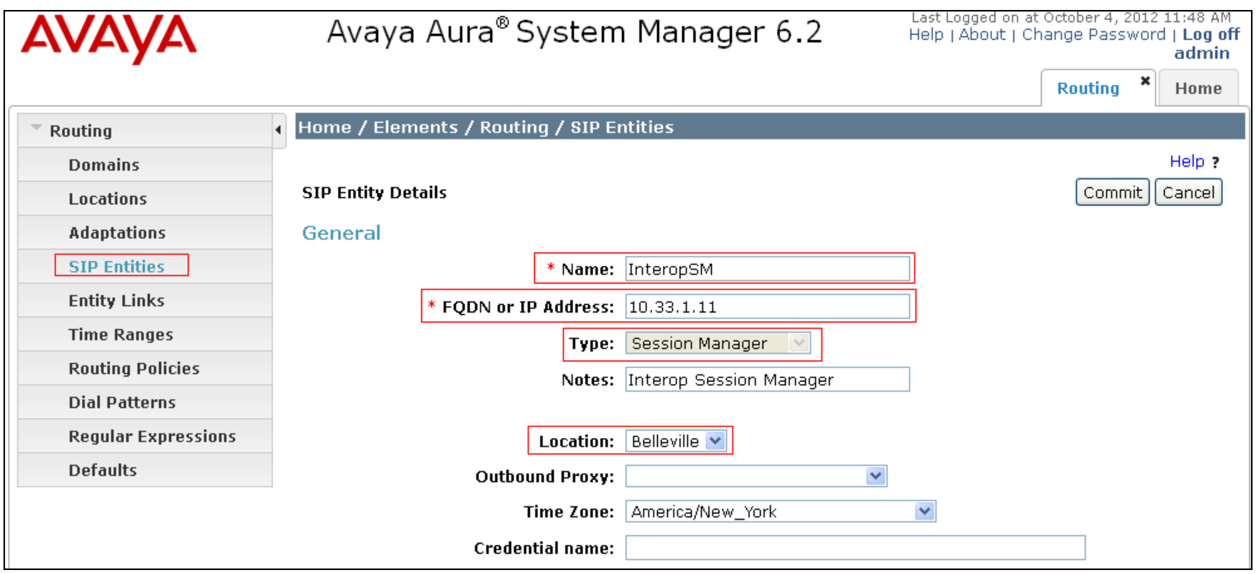
General section

Enter the following and use default values for the remaining fields:

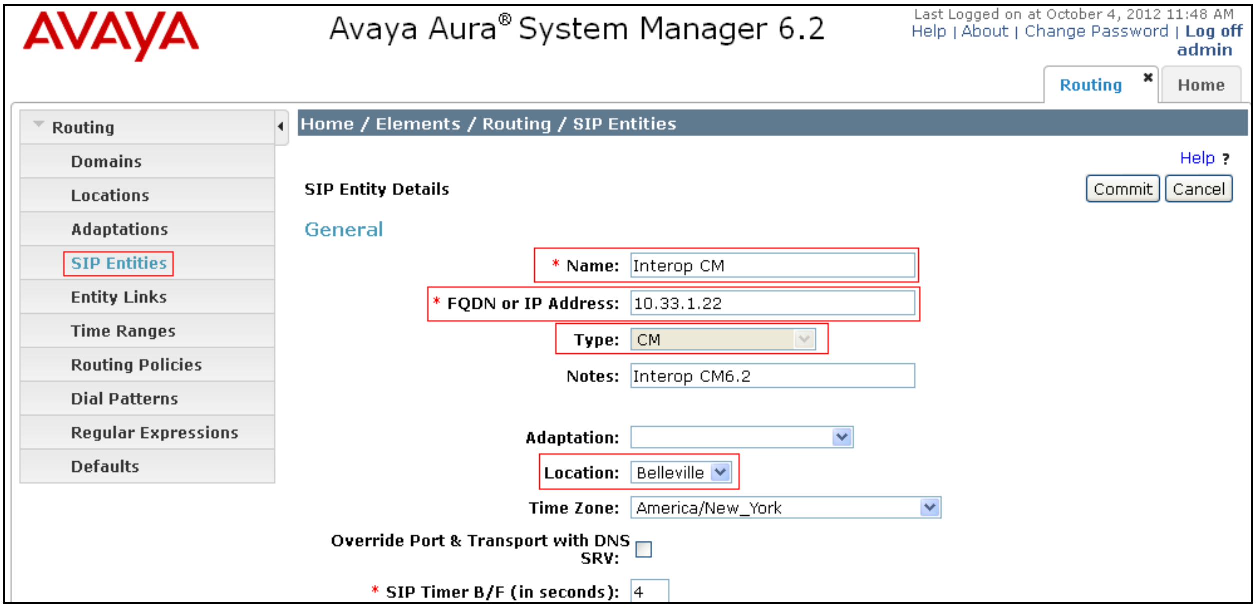
- **Name**: Enter a descriptive name.
- **FQDN or IP Address:** Enter the IP address of the signaling interface on each:
  - Communication Manager: **10.33.1.22**
  - Signaling Session Manager: **10.33.1.11**
  - Amcom Speech server: **10.10.98.124**
- From the **Type** drop down menu, select a type that best matches the SIP Entity:
  - For Communication Manager Gateway: select "**CM**"
  - For Session Manager, select "**Session Manager**"
  - For Amcom Speech Server, select "**Other**"
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Port (only available in the SM SIP Entity): Add port **5060** for **TCP** and **UDP**, and **5061** for **TLS** protocols, and select the sip domain "**bvwdev.com**" in the Default Domain column for each added port.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. Repeat all the steps for each new entity.

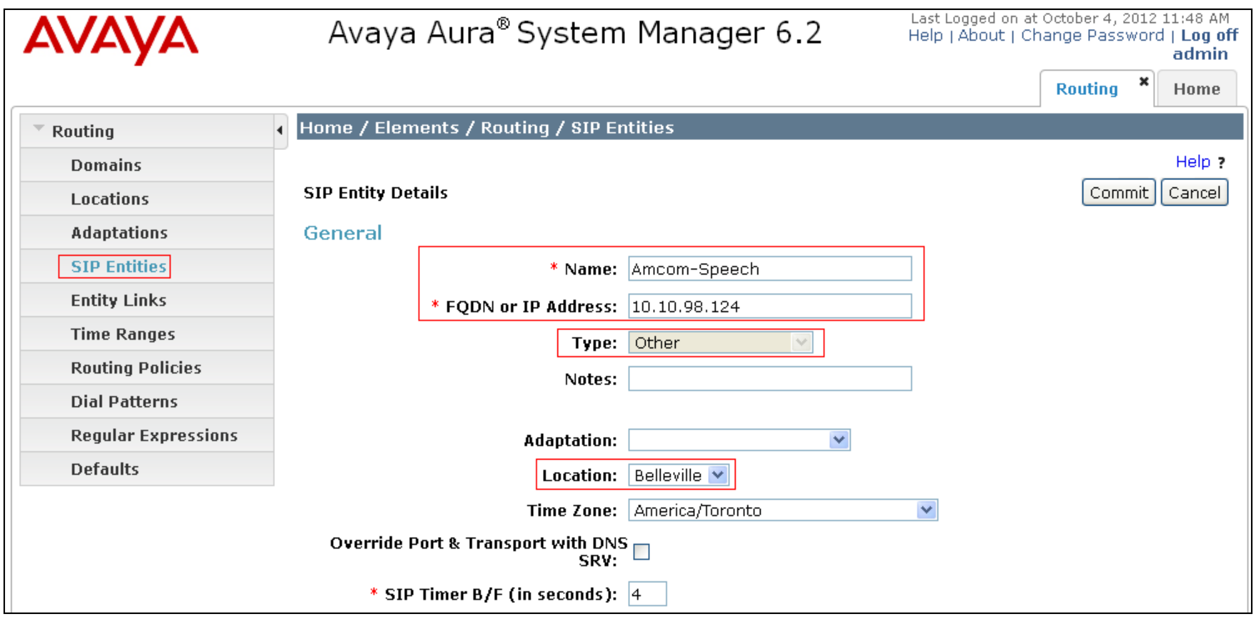
The screen below shows the detail of **Session Manger SIP Entity**.



The screen below shows the details of Communication Manager SIP Entity.



The screen below shows the detail of **Amcom Speech server** Sip Entity.



6.4. Configure Entity Links

Entity Links define the connections between the SIP Entities (in this case, Communication Manager SIP gateway and Amcom Speech server) and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Communication Manager

- Session Manager ⇔ Amcom Speech Server

Navigate to **Routing →Entity Links** and click on the **New** button to create a new entity link (screen not shown). Provide the following information:

- **Name**: Enter a descriptive name.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section** Error! Reference source not found. (e.g. **interopsm**).
- In the **Protocol** drop down menu, select the TCP and UDP protocols.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- In the **SIP Entity 2** drop down menu, select **Interop CM** for the entity links between Session Manager and Communication Manager SIP gateway and select **Amcom-Speech** for the entity links between Session Manager and Amcom Speech server.
- In the **Port** field, enter the port to be used (e.g. **5060**).
- In the **Connection Policy** column, select **Trusted** from the dropdown list.
- Enter a description in the **Notes** field if desired.

Click on the **Commit** button to save each Entity Link definition. Repeat all the steps for each new SIP Entity Link.
The newly created entity link between Session Manager and Communication Manager SIP gateway is shown below in the screen shot.

Entity Links

Add | Remove

1 Item | Refresh — Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
☐	InteropSM	TCP	* 5060	Interop CM	* 5060	Trusted

Select : All, None

The newly created entity links between Session Manager and Amcom Speech server is shown below in the screen shot.

Entity Links

Add | Remove

2 Items | Refresh — Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
☐	InteropSM	TCP	* 5060	Amcom-Speech	* 5060	Trusted
☐	InteropSM	UDP	* 5060	Amcom-Speech	* 5060	Trusted

Select : All, None

6.5. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 6.3**) and Dial Patterns (**Section 6.7**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.
- Inbound calls to Amcom Speech server.

To add a Routing Policy, navigate to **Routing →Routing Policies** and click on the **New** button on the right (screen not shown). Provide the following information:

<u>General section</u>

- Enter a descriptive name in the **Name** field (e.g. **InteropCM62**, **To-Amcom-Speech**).
- Enter a description in the **Notes** field if desired.

<u>SIP Entity as Destination section</u>

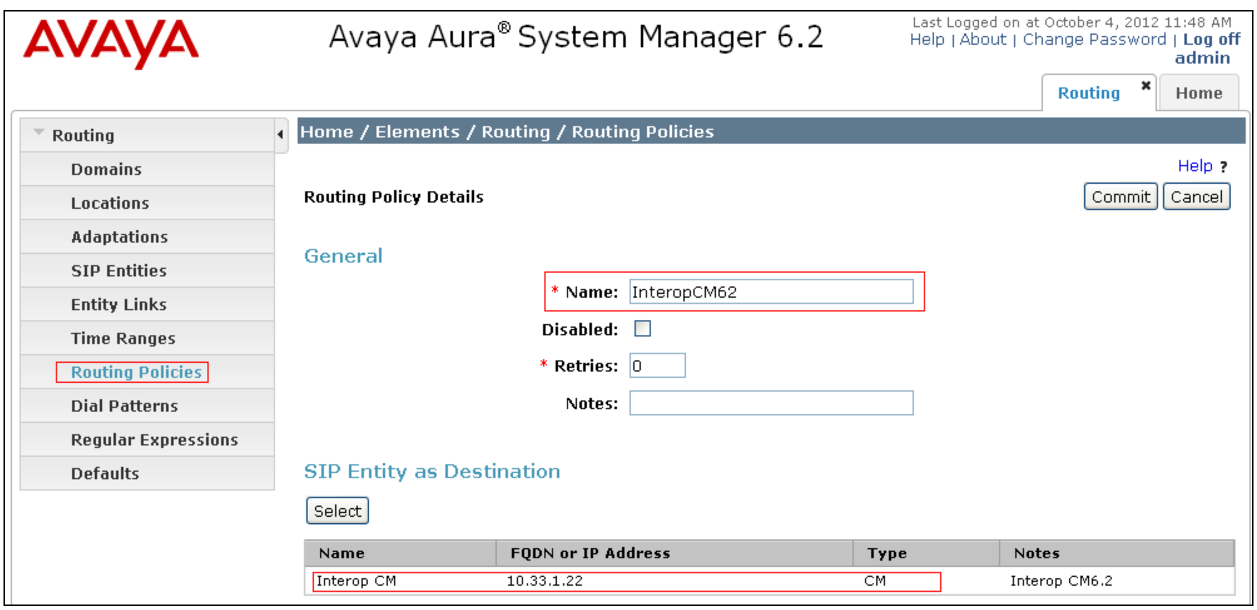
- Click the **Select** button.
- Select a SIP Entity that will be the destination for this call.
- Click the **Select** button and return to the Routing Policy Details form.

<u>Time of Day section</u>

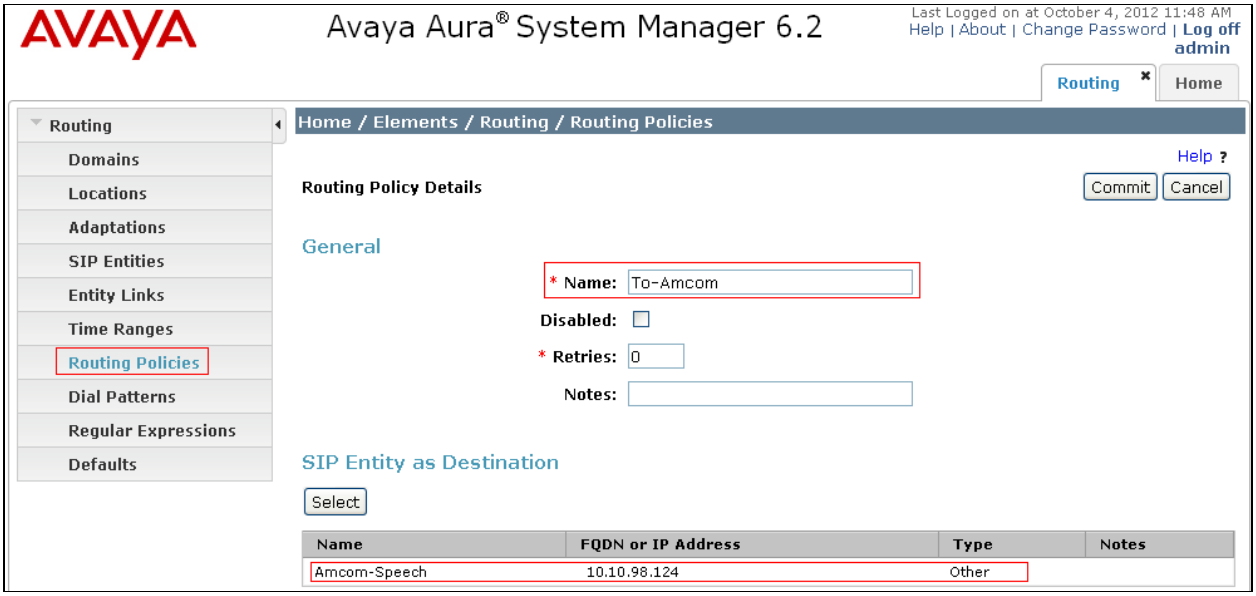
- Leave default values.

Click **Commit** to save Routing Policy definition. Repeat the steps for each new Routing Policy.

The following screen shows the Routing Policy used for Communication Manager during the compliance test.



The following screen shows the Routing Policy used for Amcom Speech server during the compliance test.



6.6. Configure Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In the compliance test, the following dial patterns are defined from Session Manager.

- **40xxx** – dial pattern used to route calls to Communication Manager.
- **720x** – dial pattern used to route to Amcom Speech server.

To add a Dial Pattern, select **Routing →Dial Patterns** and click on the **New** button (screen not shown) on the right pane. Provide the following information:

<u>General section</u>

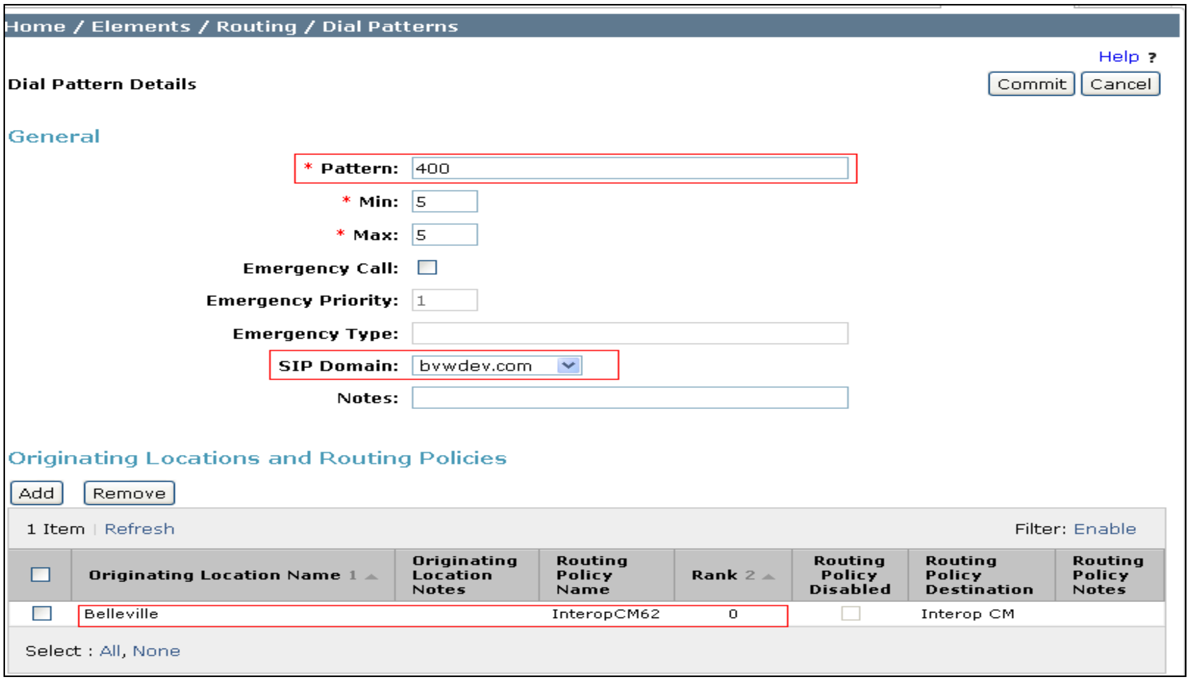
- Enter a unique pattern in the **Pattern** field (e.g. **40**).
- In the **Min** field enter the minimum number of digits (e.g. **4**).
- In the **Max** field enter the maximum number of digits (e.g. **4**).
- In the **SIP Domain** drop down menu select the domain **bvwdev.com** defined in **Section 6.1**.

<u>Originating Locations and Routing Policies section</u>

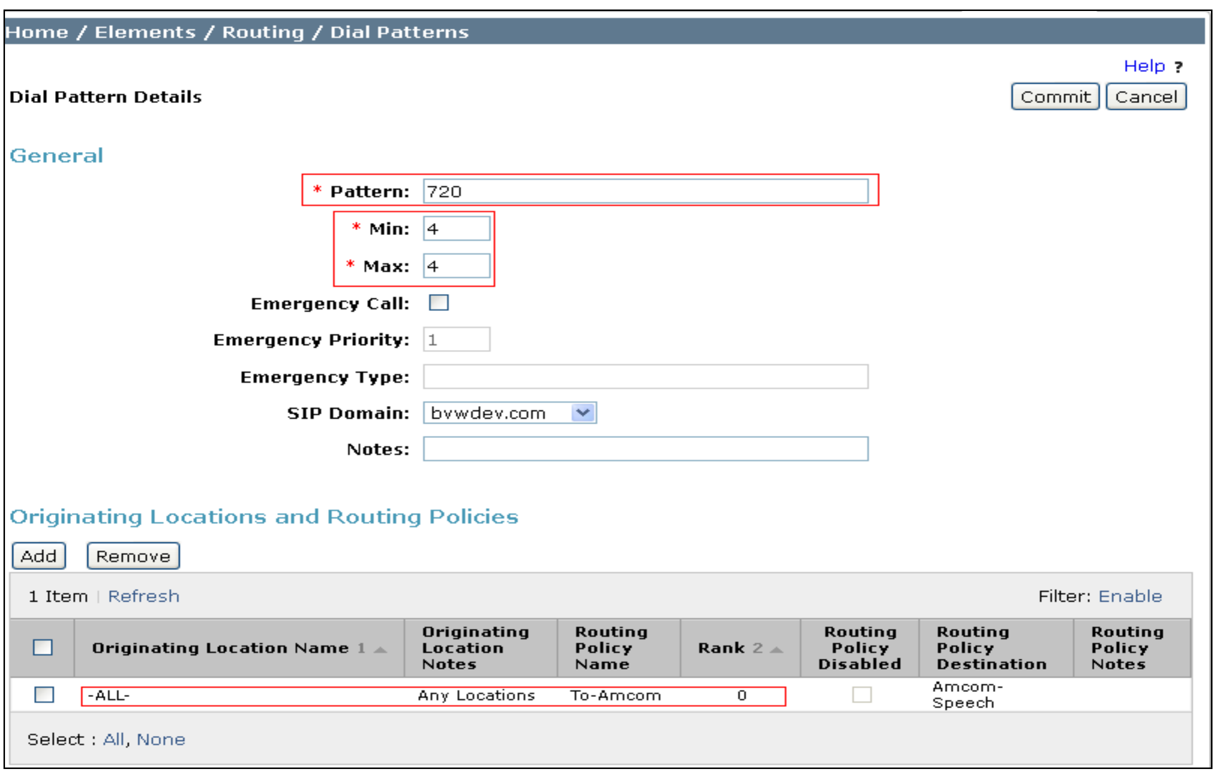
- Click on the **Add** button and a window will open (screen not shown).
- Click on the box for the appropriate Originating Locations, and Routing Policies (see **Section 6.7**) that pertain to this Dial Pattern.
    - Select the Originating Location to apply the selected routing policies to **All**.
    - Select appropriate Routing Policies.
    - Click on the **Select** button and return to the **Dial Pattern** page.

Click the **Commit** button to save the new definition. Repeat steps for the remaining Dial Patterns.

The following screen shows the dial pattern **400xx** used to route calls to Communication Manager during the compliance test.



The following screen shows the dial pattern **720x** used to route calls to the Amcom Speech server during the compliance test.



7. Configure Amcom Speech Server

The following steps are required for Amcom Speech to properly accept calls from Session Manager and be able to transfer to the proper destination. The use of FreeSwitch as a middle tier SIP proxy is required to properly control the transfer requirements based on the Avaya Session Manager.

1. On the Amcom Speech server, navigate to "C:\Program.Files\FreeSWITCH\conf\autoload_configs\".
2. Open acl.conf.xml in a text editor and replace XXX.XXX.XXX.XXX with the IP address of the Session Manager.
3. Save acl.conf.xml (This permits FreeSwitch to accept traffic from Session Manager)
4. Navigate to "C:\Program Files\FreeSWITCH\conf\dialplan\".
5. Open Public.xml.
6. On line 18, replace [XXXXX] with the number being dialed from Session Manager to reach this SIP Trunk.
7. On line 19, replace [XXXXX] with the same number.
8. On line 24, replace [XXXXX] with the same number as in step 6.
9. On line 25, replace [XXXXX] with the same number.
10. Save Public.xml (This enables the external dialplan to properly route Session Manager inbound calls).
11. Open Default.xml in the same directory that Public.xml was in.
12. On line 17, replace [XXXXX] with the same number.
13. On line 18, replace [XXXXX] with the same number.
14. On line 25, replace [XXXXX] with the same number.
15. Replace [IPADDRESS] with the IP address of the Amcom Speech Server.
16. On line 28, replace [YYYYY] with a valid fail over number to transfer the inbound calls to incase Amcom Speech is not available. This usually can be a Pilot number to an Operator ACD queue.
17. On line 28, replace [IPADDRESS] with the IP of the Session Manager.
18. On line 24, replace [IPADDRESS] with the IP of the Session Manager.
19. Save Default.xml (This routes the traffic from the external dialplan to Amcom Speech).
20. On the speech server, open the Internet Browser to http://127.0.0.1:8080/ISPEECH6/admin/config.jsp and log in.
21. Change the SIP Gateway IP to 127.0.0.1.
22. Commit changes by clicking on "Commit Values" (This insures that transfers will route out through FreeSwitch).
23. On the speech server, open an Internet Browser to http://127.0.0.1:9090/portal/auth/portal/default/platform/Manage and log in.
24. Highlight Vcore VXML Browser and select Configuration.
25. Insert a DNIS record based on the inbound number being dialed from the Session Manager, insert the appropriate vxml start page usually (http://127.0.0.1:8080/ISPEECH6/IS4_Main.jsp).
26. Click Update and restart the Vcore VXML Browser (This routes the dialplan to the appropriate call flow that Amcom Speech should serve up).
27. Open the Windows Services Manager MMC.

28. Locate the FreeSwitch Service and restart it.(This restarts FreeSwitch allowing all changes made to take effect).
29. Configuration Complete.

8. Verification Steps

The following typical steps are used to verify that the Amcom Speech server works with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

- Verify the SIP trunk entity link status is up between Session Manager and Communication Manager by navigating to **Elements →Session Manger → System Status → SIP Entity Monitoring** and select the Communication Manager Entity link.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Interop CM

Summary View

1 Item | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	InteropSM	10.33.1.22	5060	TCP	Up	200 OK	Up

- Repeat the same procedure to verify the SIP entity link between Session Manager and Amcom Speech server.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Amcom-Speech

Summary View

2 Items | Refresh Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	InteropSM	10.10.98.124	5060	UDP	Up	200 OK	Up
▶ Show	InteropSM	10.10.98.124	5060	TCP	Up	200 OK	Up

- Place a call from H.323 Communication Manager Phone A to the Amcom Speech server by dialing 7200 which is the dial pattern of the Amcom Speech server.
- Phone A is connected to Amcom Speech server and hears a prompt from the Speech server. Phone A can either enter an extension or speak a name to which the speech server will transfer the call.
- Base on the input of Phone A, the speech server transfers the call to the desired destination, the destination can be on the same Communication Manager switch or

different switch. For example, the call is transferred to Phone B that is located on the same Communication Manager switch.

- Phone A will hear the ringing tone when waiting for Phone B to answer the call.
- Phone B answers the call and Phone A and B are connected.
- Check audio quality of the call and hold/un-hold calls on both phones are also verified.

9. Conclusion

These Application Notes described the administration steps required to integrate Amcom Speech Auto Attendant with the Avaya Aura® Communication Manager via SIP trunk configured on the Avaya Aura® Session Manager. All test cases are passed.

10. Additional References

The following Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, Release 6.2 July 2012, Issue 6.2, Document Number 03-300509

[2] *Administering Avaya Aura® Session Manager*, Release 6.2, July 2012, Document Number03-603324

[3] *Administering Avaya Aura® System Manager*, Release 6.2, July 2012.

[4] *Avaya Communication Installation and Commissioning*, Doc# NN43041-310, Date July 2012.

Product information for Amcom Speech Auto Attendant application can be found at http:// http://www.amcomsoftware.com

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.