Avaya Solution & Interoperability Test Lab

Application Notes for configuring Amcom Speech Auto Attendant Version 7.0 with Avaya Communication Server 1000E Release 7.5 and Avaya Aura® Session Manager 6.1 – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Amcom Speech Auto Attendant with Avaya Communication Server 1000E and Avaya Aura® Session Manager. The solution used Avaya Aura® Session Manager to route calls between Avaya Communication Server 1000E 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 Communication Server 1000E over 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 Communication Sever 1000E via a SIP trunk configured on Avaya Aura® Session Manager. The Avaya Communication Server 1000E that was used for the testing is a co-resident system, which has a Call Server, Signaling Server and Element Manager applications residing on the CPPM card. Avaya Aura® Session Manager provides SIP trunking and network routing service to route calls between Avaya Communication Server 1000E and the Amcom Speech Auto Attendant server.

2. General Test Approach and Test Results

The general test approach was to verify test calls made from Avaya Communication Server 1000E (hereafter referred to as Avaya CS1000) to Amcom Speech server to navigate basic features on the speech server 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 Avaya CS1000: hold and retrieve call, voice mail.
- Transfer calls off-net via SIP trunk and via simulated PSTN using T1/ISDN.
- Codec negotiation: G.711 and G.729.

2.2. Test Results

All test cases passed. There is one important note for this testing.

- There are two required patches that need to be installed on the CS1000 system to address the ring back tone issue on the CS1000 phone when this phone is transferred by Amcom Speech server to another phone: the first one is **MPLR32248** that is installed on CS1000 Call server and the second one is **cs1000-vtrk-7.50.17.16-125.i386.000.ntl** installed on the Linux base of CS1000 SIP Gateway which is used to have SIP trunk with Session Manger and Amcom Speech server.

2.3. Support

For technical support on the Amcom Speech Auto Attendant product, contact Amcom software support via telephone and 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 CS1000 A is considered as the main switch for the compliance test with the Amcom Speech server. Avaya CS1000 A and CS1000 B and the Amcom Speech server have SIP trunks to Avaya Aura® Session Manager. Avaya CS1000 A also has a T1/ISDN PRI trunk connected to a simulated PSTN.

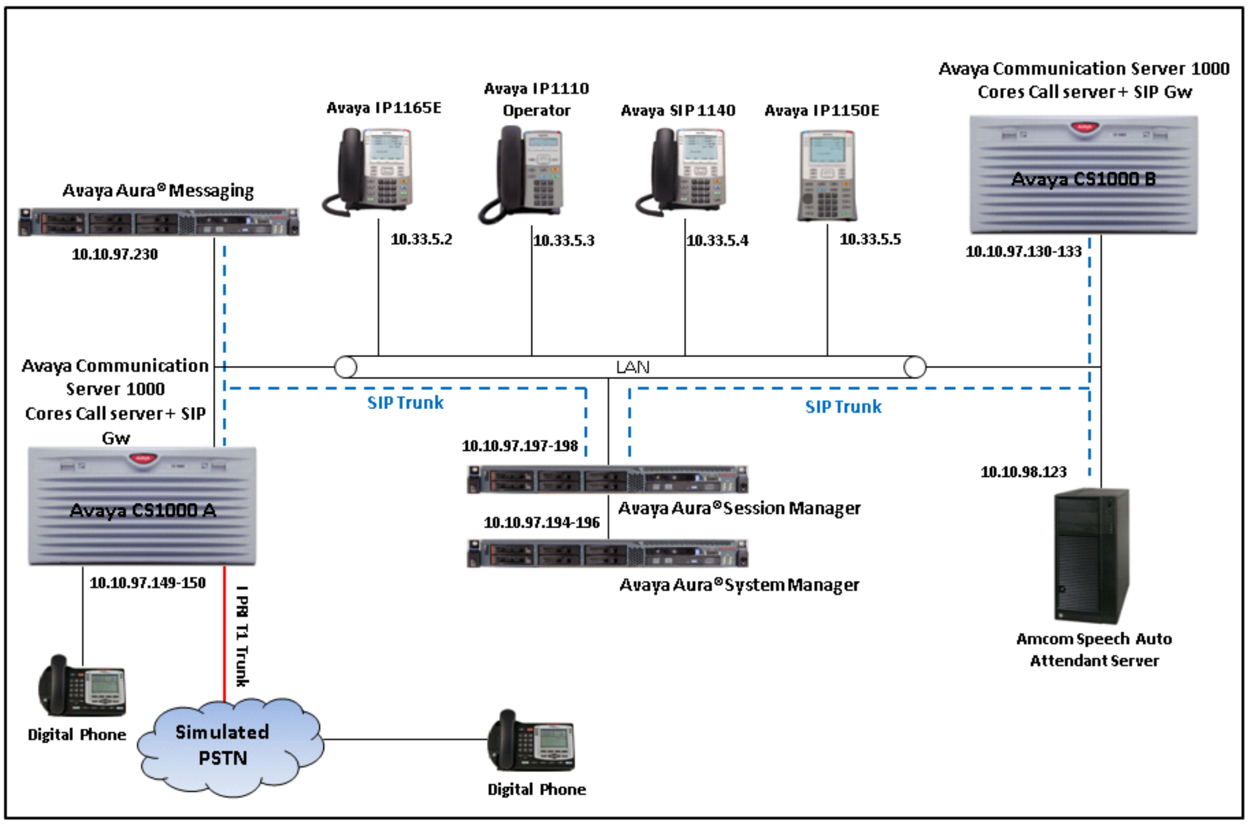


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment / Software	Software
Avaya S8800 server running Avaya Aura® Session Manager Server	Avaya Aura® Session Manager 6.1 SP6 (Build No 6.1.6.0.616008)
Avaya S8800 server running Avaya Aura® System Manager Server	Avaya Aura® System Manager 6.1 SP6 (Build No: 6.1.0.0.7345-6.1.5.606 Software Update Revision No: 6.1.10.1.1774)
Avaya Communication Server 1000E/CPPM	Avaya Communication Server Release 7.5 Q+ Deplist 1 (created: 2012-07-23) and Service Update 1 (Created: 2012-0708)
Avaya S8800 Server	Avaya Aura® Messaging
Avaya IP SIP Phone 1140E	4.3
Avaya IP Unistim Phone 1165E	0x25C8J
Avaya IP Unistim Phone 1150E	0x27C8J
Avaya IP Unistim Phone 1110	0x23C8J
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 Communication Server 1000

This document assumes that the Avaya Communication Sever 1000 system was properly installed and configured per the product documentation. This section provides the steps on how to provision the CS1000 to work with the Amcom Speech Auto Attendant server. For more information about how to install and configure Communication Server 1000, please refer to **Section 10 [1]**.

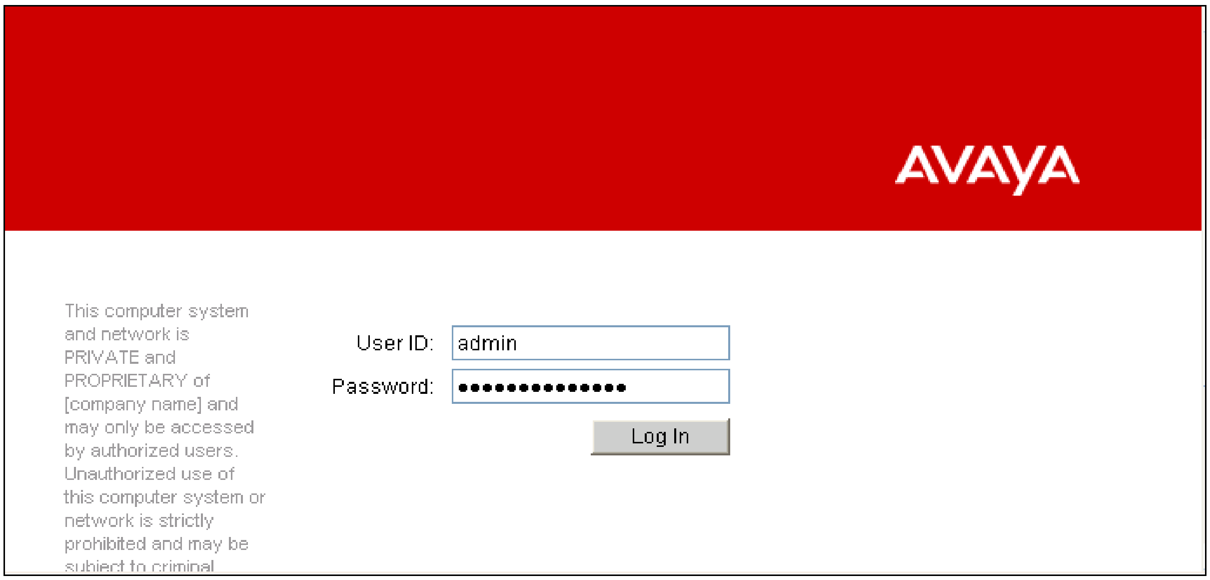
The following summarizes the tasks which need to be done on the CS1000 System:

- Configure Avaya CS1000 SIP gateway.
- Configure D-Channel for SIP Trunk.
- Configure Zone for Route and Trunk.
- Configure SIP Route.
- Configure SIP Trunks.
- Configure CDP Dialing plan.
- Configure IP Phone.

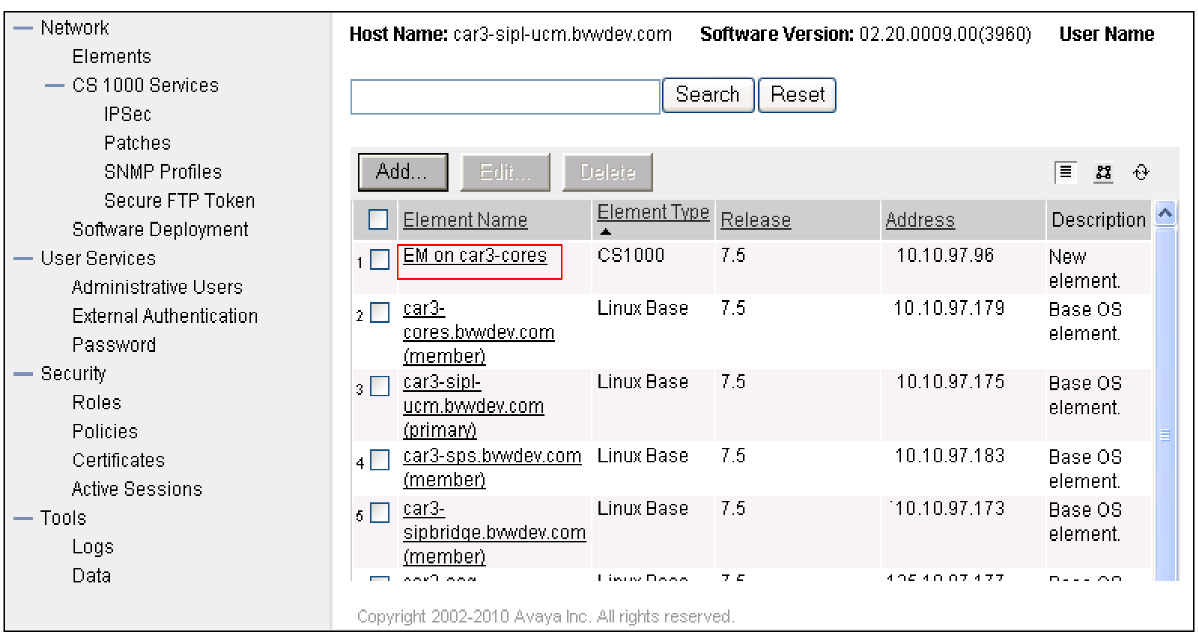
5.1. Configure Avaya Communication Server 1000 SIP Gateway

This section provides the steps to configure SIP trunks between Avaya CS1000 SIP gateway and Session Manager.

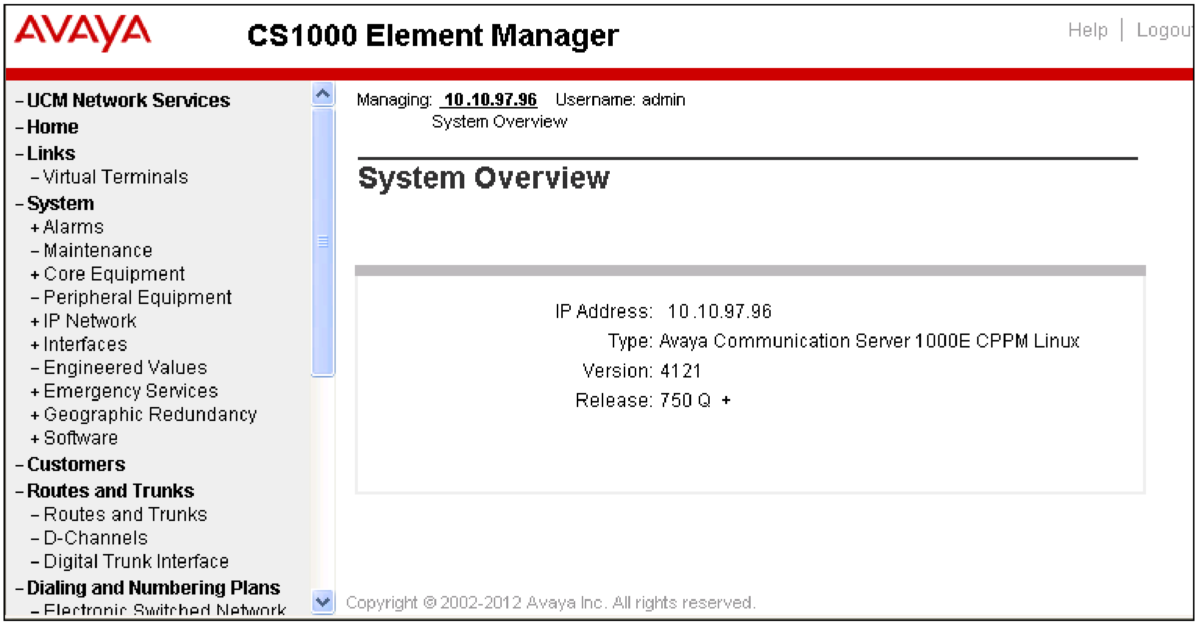
Avaya CS1000 system is managed by Avaya Unified Communication Manager (UCM). In order to log in to the Element Manager of CS1000 system, first log in to the UCM system and then access the CS1000 Element Manager.
The screen below shows the UCM login page. Enter the username "**admin**" and its password in the **User ID** and **Password** boxes and click on the **Log In** button.



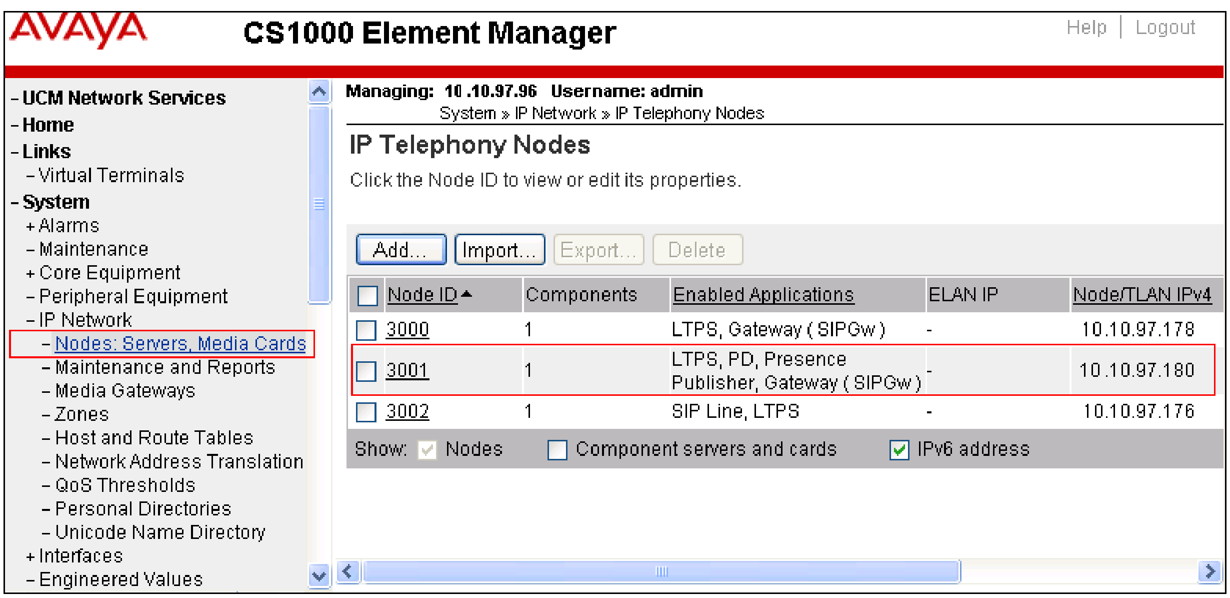
The homepage of the UCM is displayed as shown below.



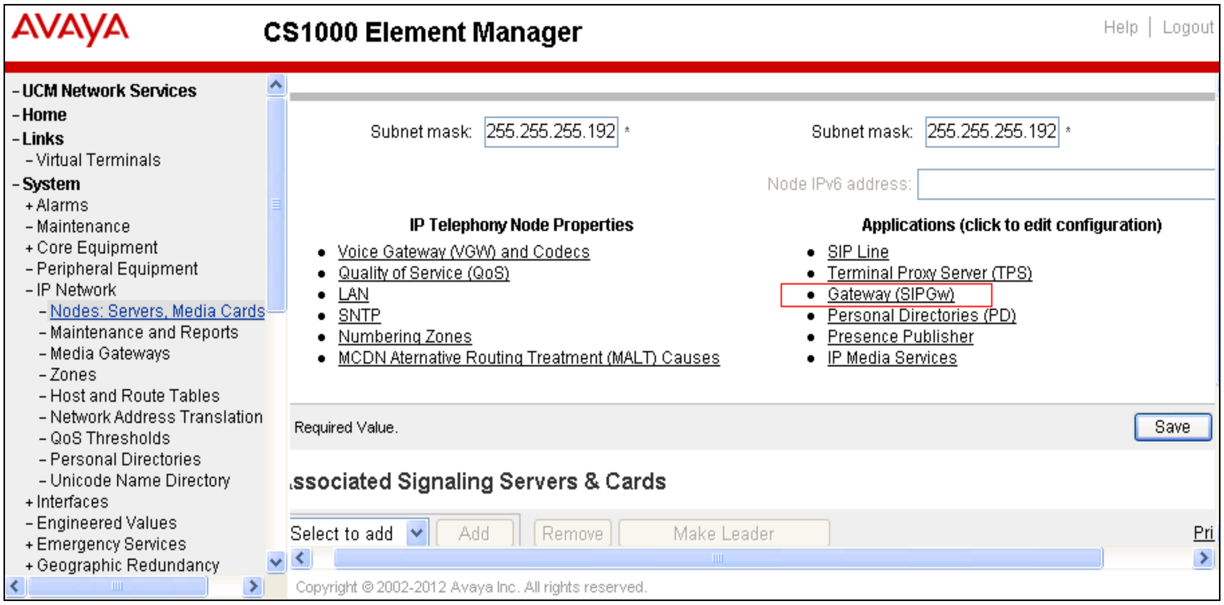
In the UCM homepage, click on the EM on car3-cores in the **Element Name** column that manages the CS1000 system, the **CS1000 Element Manager** window is displayed as shown below.



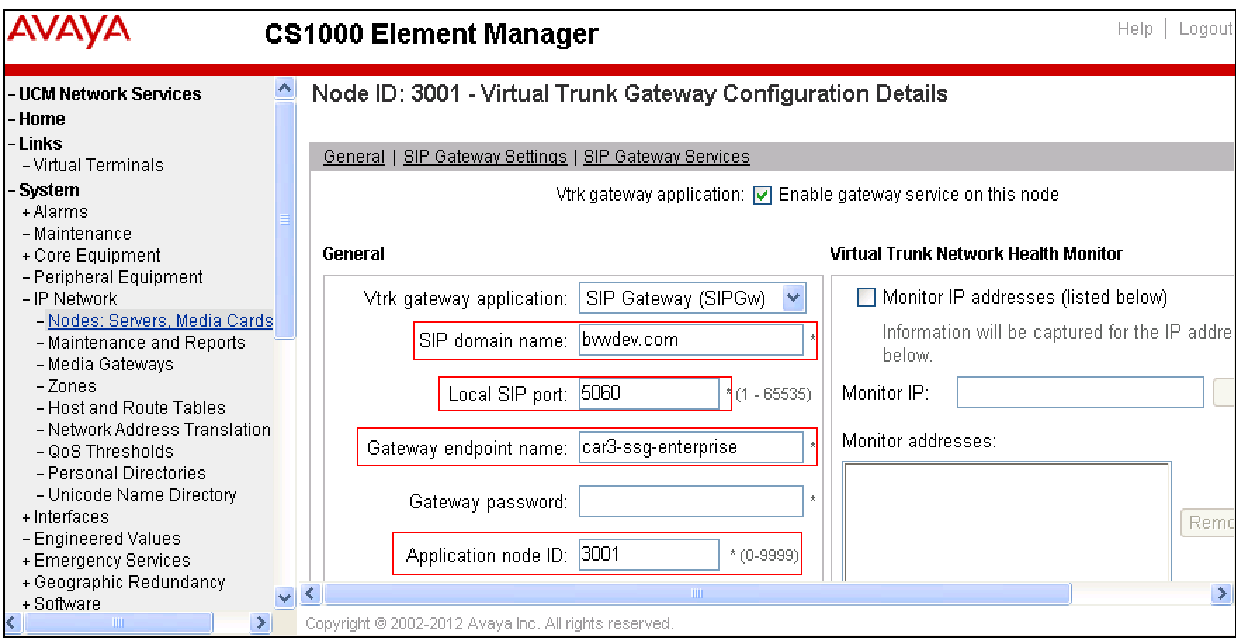
On the left-hand side of the Element Manager window and under the **System** tab, expand **IP Network** > **Nodes: Servers and Media Cards**, to display **IP Telephony Nodes** in the right-hand side of the window. Click on the **Node ID 3001,** which has the **Gateway (SIPGw)** application enabled and was used for the compliance test.



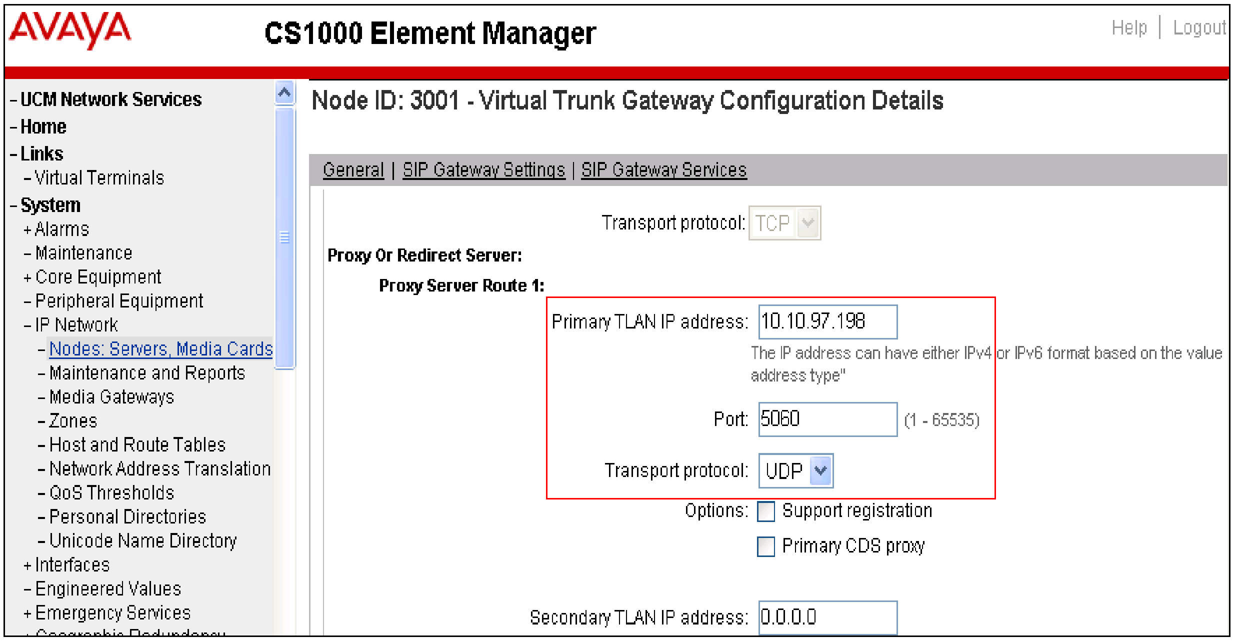
The **Node 3001** detail is displayed as shown below. Under the **Applications (click to edit configuration)** section, click on the **Gateway (SIPGw)** link.



The **Node ID: 3001 – Virtual Trunk Gateway Configuration Details** is displayed.I In the **General** section, enter the domain **bvwdev.com** in the **SIP Domain Name** box, port **5060** in **Local SIP Port** , name **car3-ssg-enterprise** in the **Gateway Endpoint Name** and **3001** in the **Application Node ID** as shown below.

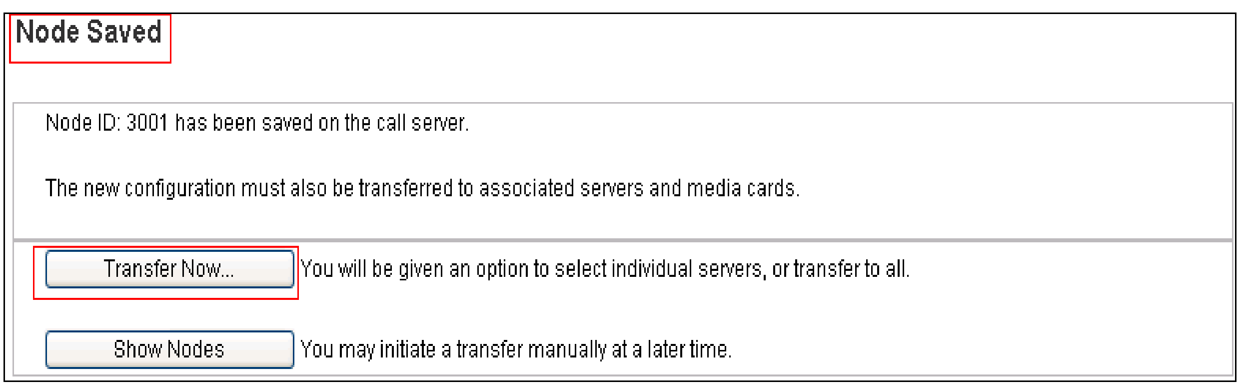


Scroll down to the **SIP Gateway Settings** section. In the **Proxy Or Redirect Server** sub-section, enter the signaling IP address of Session Manager **10.10.97.198** in the **Primary TLAN IP address** field, port **5060** in the **Port** field, and **UDP** in the **Transport** field.

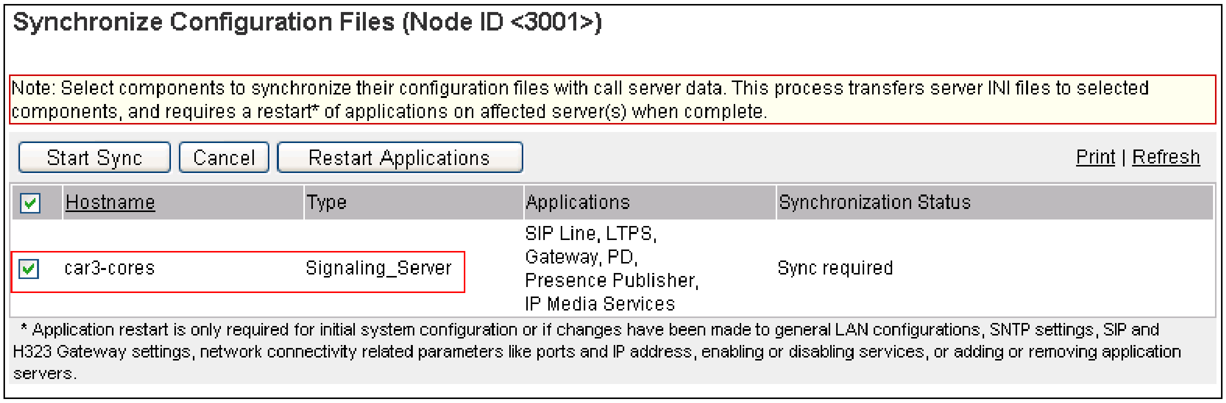


Click on **Save** button at the bottom of the **Node ID: 3001 - Virtual Trunk Gateway Configuration Details** page (screen not shown) to save the changes. The **Node ID: 3001 – Virtual Trunk Gateway Configuration Details** page is closed and the user is returned to the **Node Detailed (ID 3001, Gateway (SIP Gw))** page.

In the **Node Detailed (ID 3001, Gateway (SIP Gw))** page, click on the **Save** button to save the changes that were made for **Node 3001** (screen not shown). The **Node Saved** page is displayed as below. Click on the **Transfer Now** button to transfer the changes to associated servers and media cards.



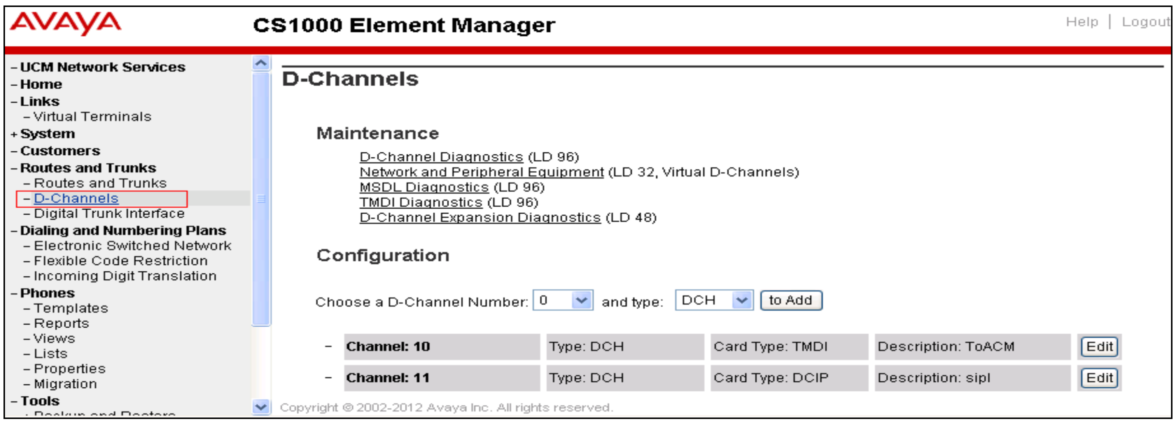
The **Synchronize Configuration Files (Node ID <3001>)** page is displayed. Click on the associated signaling server **car3-cores** and then click **Start Sync** button to synchronize the new configuration to the server **car-cores**.



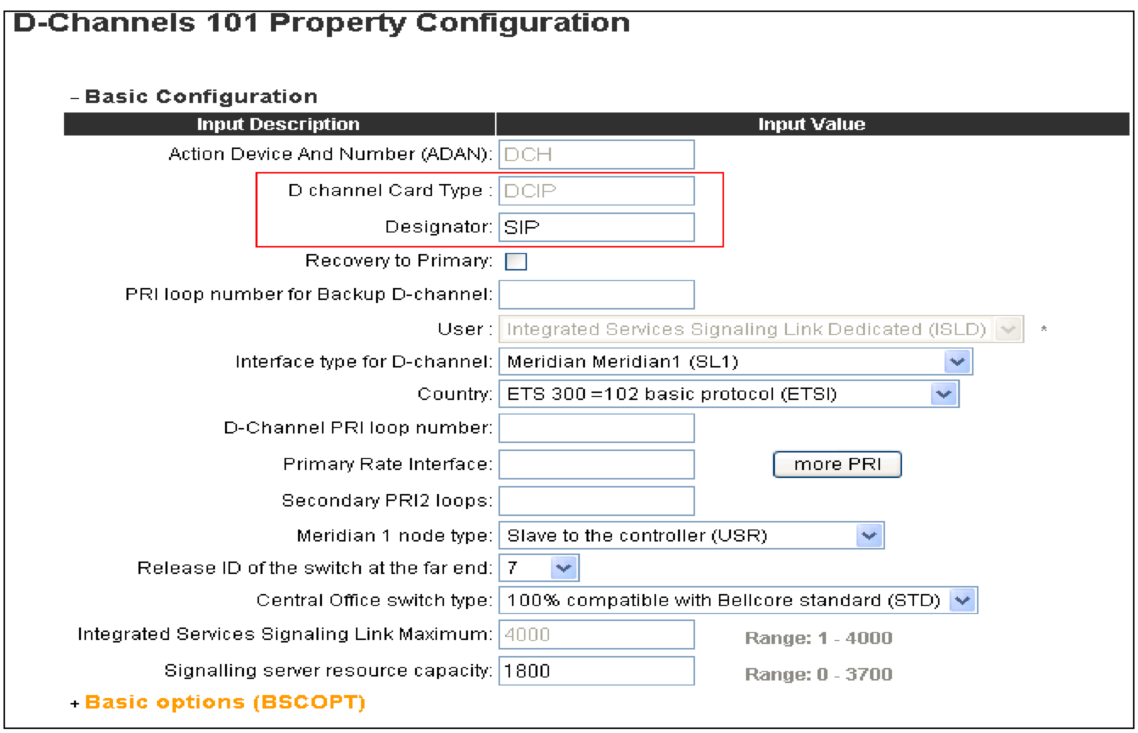
5.2. Configure D-Channel for SIP Trunk

From the homepage of Element Manager, expand the **Routes and Trunks > D-Channels** menu and select the **D-Channels** tab. The **D-Channel** page is displayed on the right-hand side as shown below.

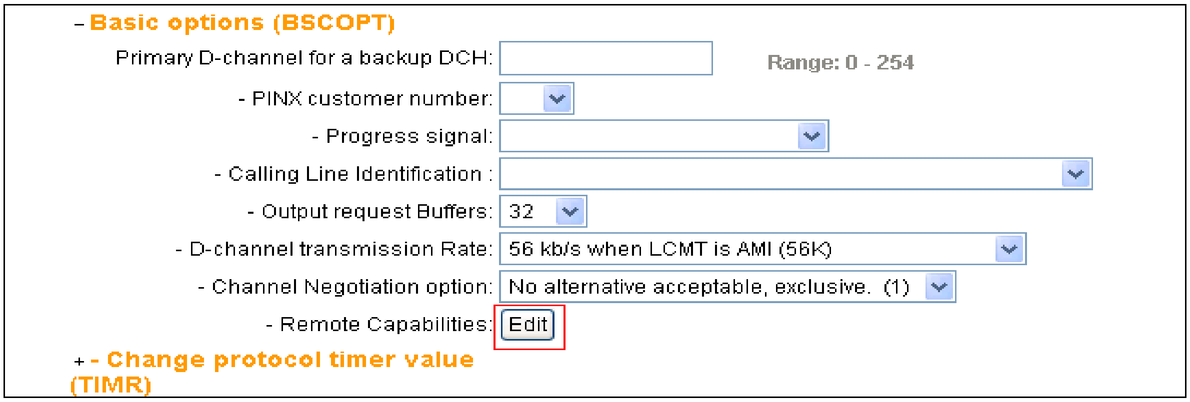
In the **Configuration** section, select an available D-Channel number in the **Choose a D-Channels Number** dropdown list, select the type of D-Channel as **DCH** and click on the "**to Add**" button. In the compliance test, the **D-channel 101** was used for SIP trunk.



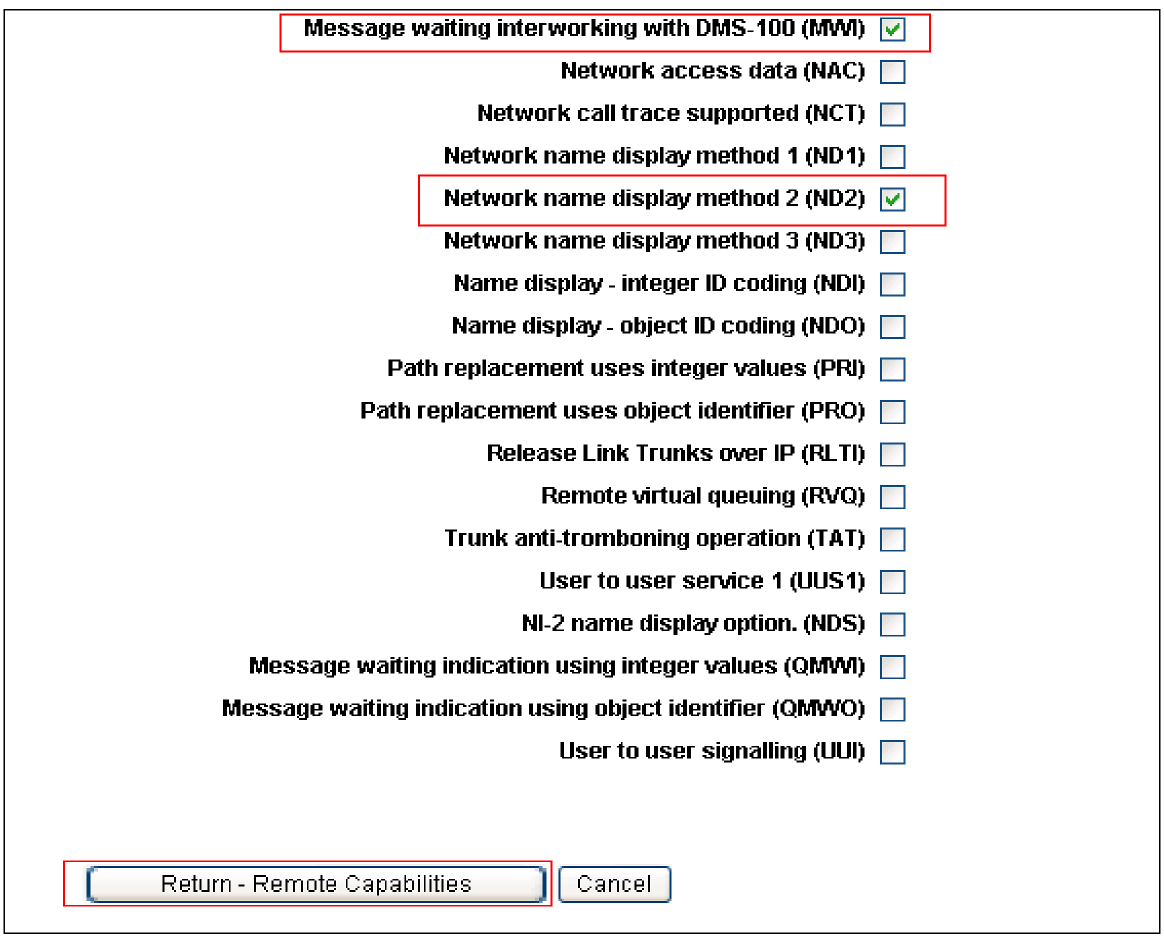
The screen below shows the **Basic Configuration** section of this D-channel. Select **D-Channel is over IP (DCIP)** in the **D-Channel Card Type**, enter a description in the **Designator** box and keep all other values at their defaults.



Expand the **Basic options (BSCOPT)** section. Keep all fields at default and click on the **Edit** button in the **Remote Capabilities** field.



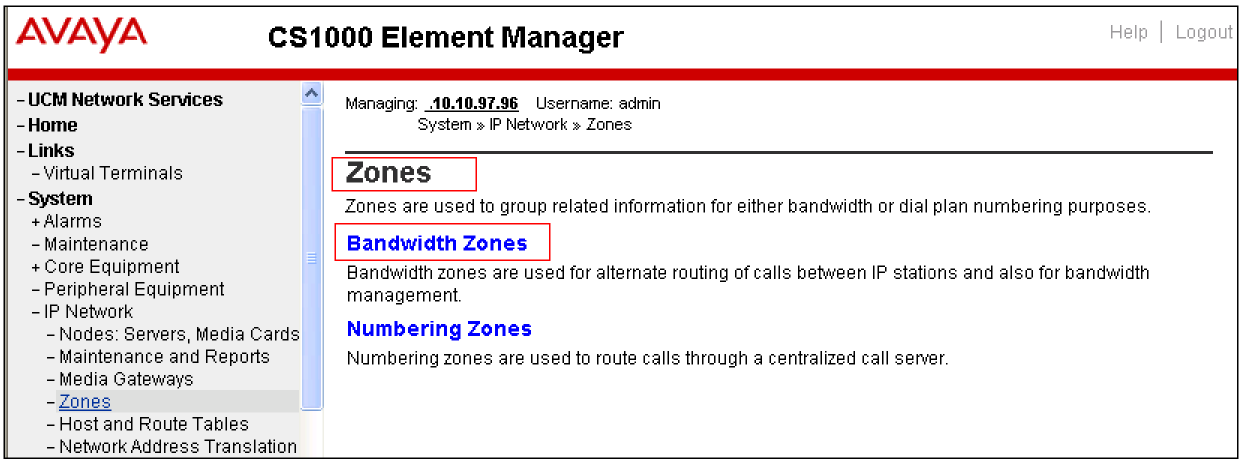
The **Remote Capabilities Configuration** page is displayed. Make sure that **Message waiting interworking with DMS-100 (MWI)** and **Network name display method 2 (ND2)** check boxes are checked**.** Click on **Return – Remote Capabilities** button to return to the D-Channel page.



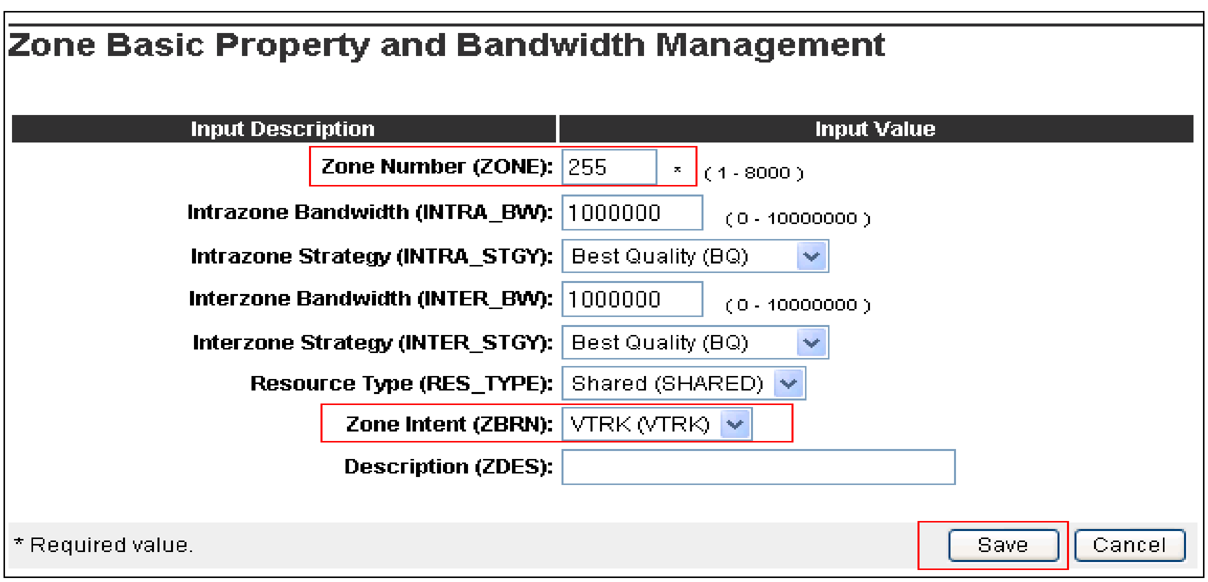
Keep all values at default for the **Change protocol time value (time)** and **Advanced options (ADVOPT)** sections. Click on the **Submit** button at the bottom of the D-channel configuration page to save and complete.

5.3. Configure Zone Bandwidth

To configure a Zone, from the homepage of Element Manager expand the menu **System > IP Network > Zones** and select the **Zones** tab. The **Zones** page is displayed on the right-hand side as shown below.

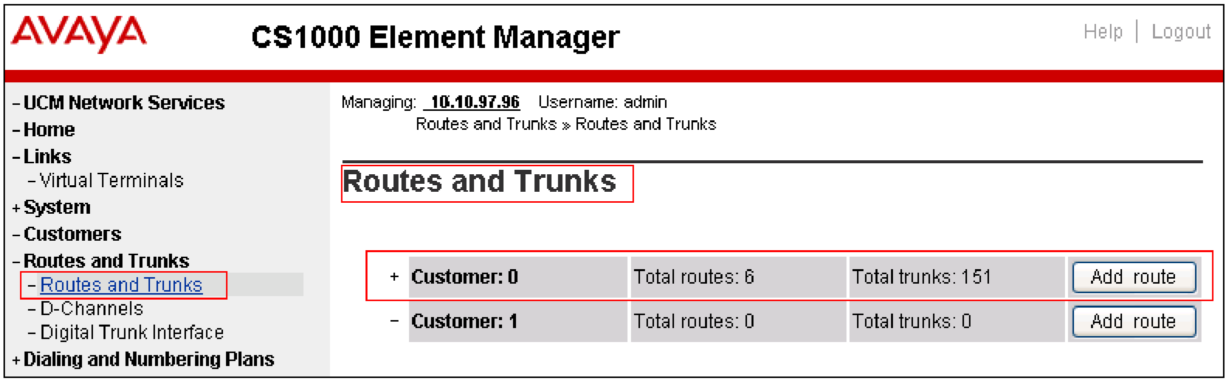


Click on the **Bandwidth Zones** link. The **Bandwidth Zones** page is dispalyed (screen not shown) and click on the **Add** button to add a new zone. The **Zone Basic Property and Bandwidth Management** page is displayed. Enter an available number from **1** to **255** in the **Zone Number (ZONE)** field, e.g. **255**, set **Zone Intent (ZBRN)** field to **VTRK** (this zone is intended to use for virtual trunks) and keep other fields at their defaults. Click the **Save** button to save changes and complete the addition of the new zone.

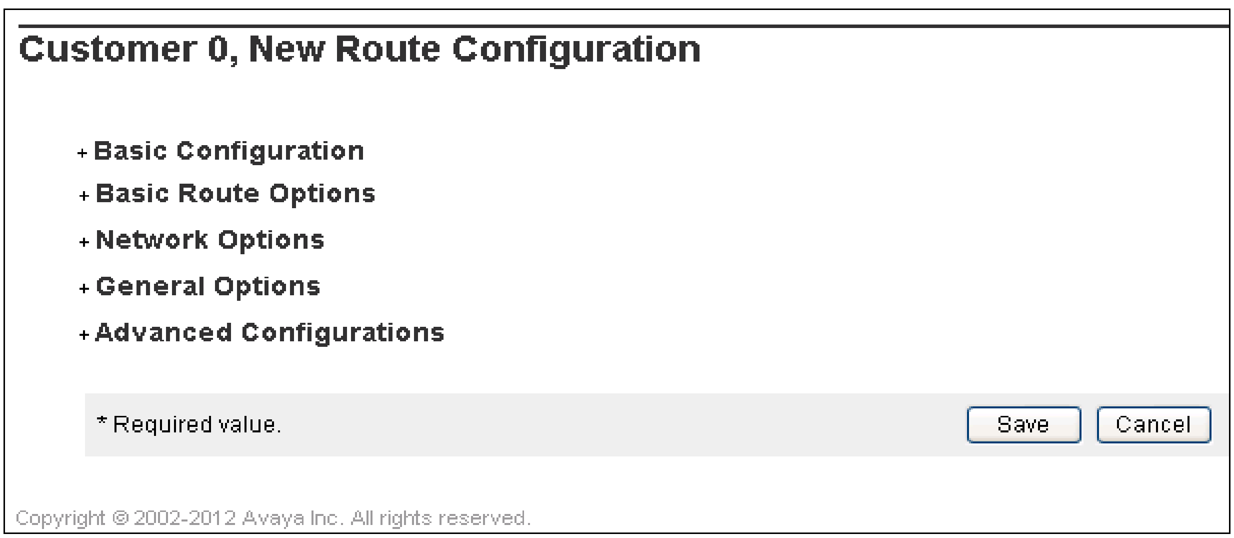


5.4. Configure SIP Route

To configure a SIP Route from the homepage of Element Manager, navigate to **Routes and Trunks > Routes and Trunks**. The **Routes and Trunks** page is displayed on the right-hand side. In the compliance test, the route and trunks were created in the **Customer 0**.

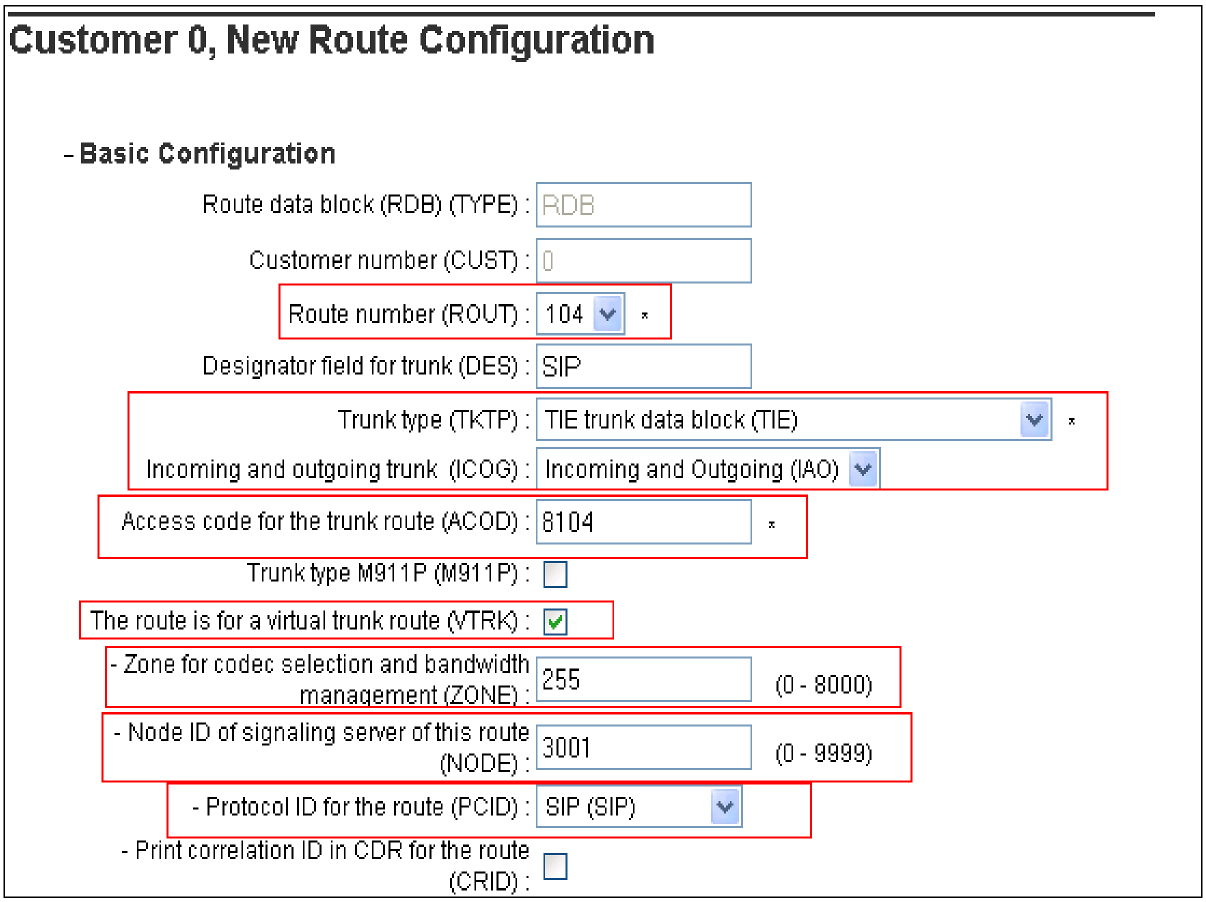


Click on **Add route** button in the **Customer: 0**. The **New Route Configuration** page is displayed and consists of 5 sections: **Basic Configuration**, **Basic Route Options**, **Network Options**, **General Options**, and **Advanced Configurations**.



Expand the **Basic Configuration** section; enter the information as shown in the screen below:

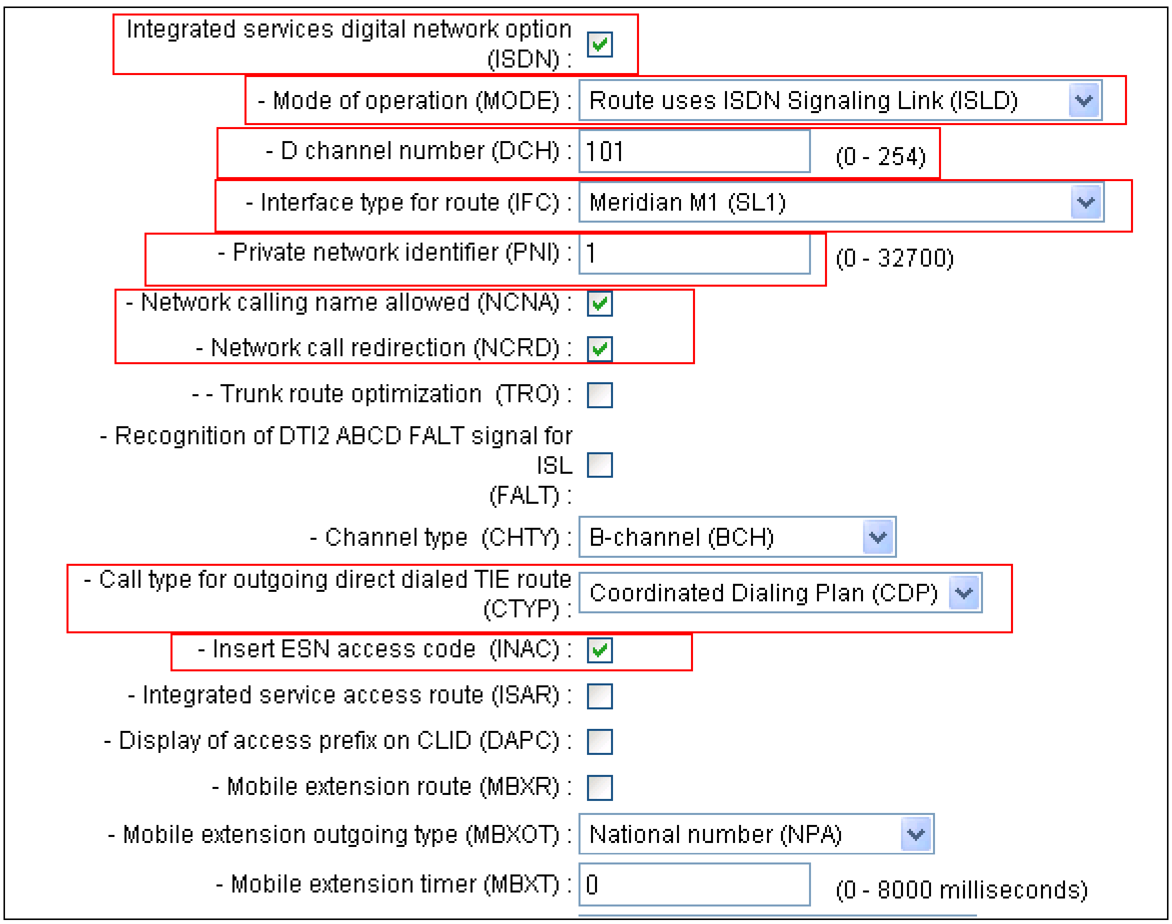
- **Route number (ROUT)**: **104**
- **Trunks type (TKTP)**: TIE trunk data block (TIE)
- **Incoming and outgoing trunk (ICOG)**: select Incoming and Outgoing (IAO)
- **Access code for the trunk route (ACOD)**: 8104
- **The route if for a virtual trunk route (VTRK)**: Checked
- **Zone for codec selection and bandwidth management (ZONE)**: **255** as configured in the Section **5.3**
- **Node ID of signaling server of this route (NODE)**: **3001** as configured in **Section 5.1** that have SIP trunk to Session Manager.
- **Calling number dialing plan (CPND)**: **Coordinated dialing plan (CDP)** as the CDP dialing plan was used for this route.



Check **Integrated services digital network option (ISDN)** in the **Basic Configuration** section. The screen below shows the sub-options for this feature enabled. The important values are entered as shown below.

- **Mode of Operation (MODE)**: Route uses ISDN Signaling Link (ISLD)
- **D Channel number (DCH)**: **101** as defined in the **Section 5.2**
- **Interface Time For Route (IFC)**: Meridian 1 (SL1)
- **Private Network Identifier (PNI)**: 1
- **Network Calling Name Allowed (NCNA)**: Checked.
- **Network call redirection (NCRD)**: Checked
- **Call type for outgoing direct dialed TIE Route (CTYP)**: select Coordinated Dialing Plan (CDP)
- **Insert ESN access code (INAC)**: Checked.

Keep other values as default as shown in the screen below.



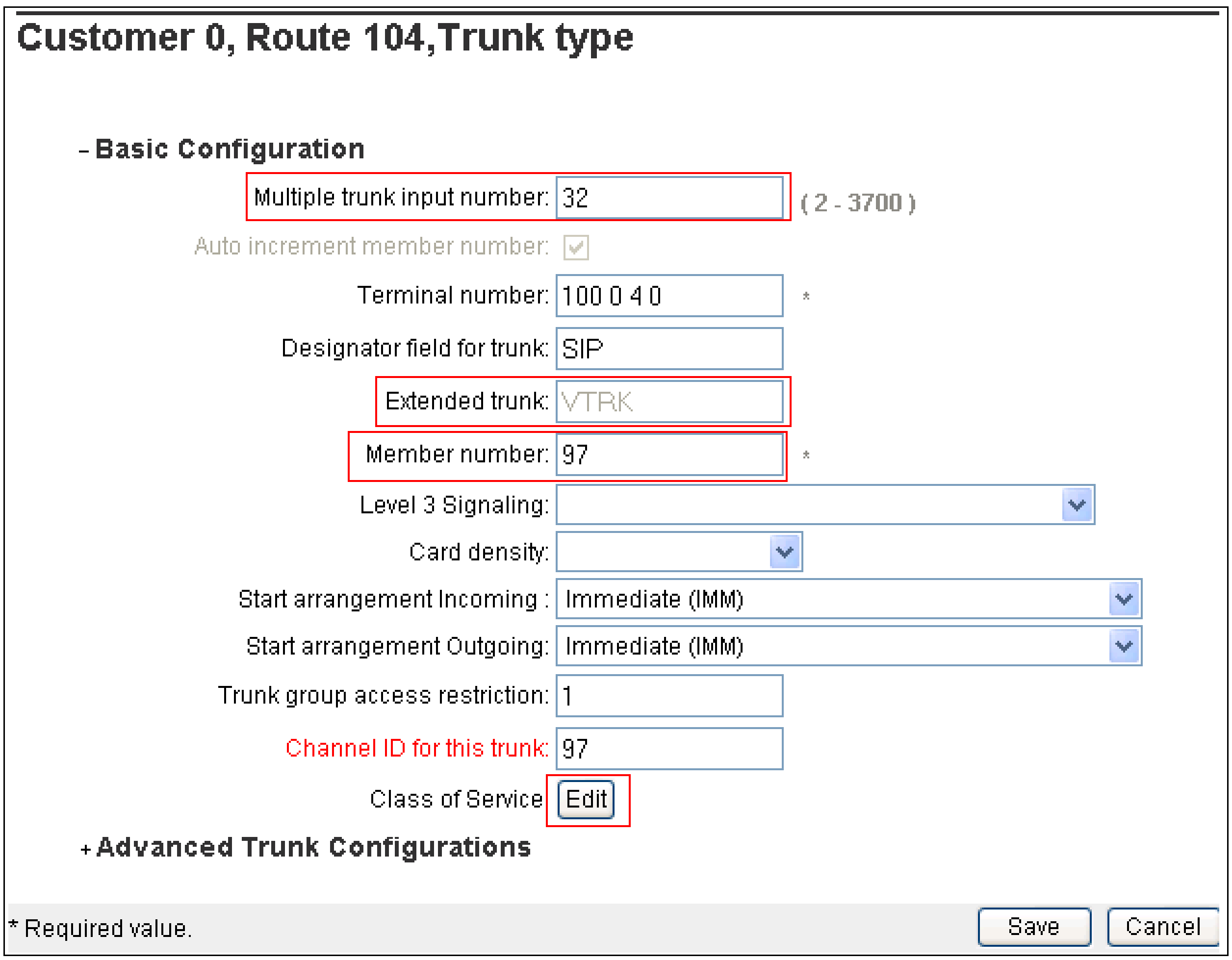
Keep all values at the default for the **Basic Route Options**, **Network Options**, **General Options**, and **Advanced Configurations** sections.

Click **Save** button at the bottom of the **New Route Configuration** page to save and create the new route.

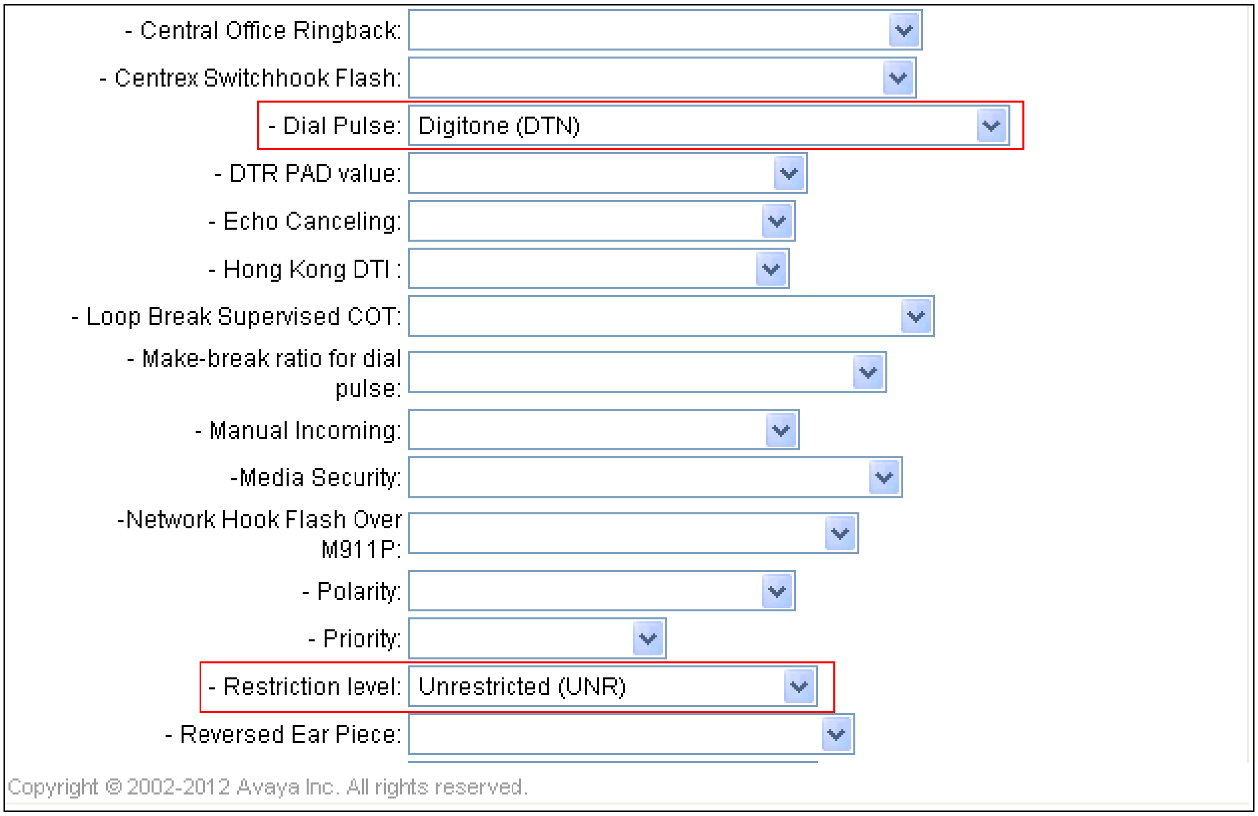
5.5. Configure SIP Trunks

From the homepage of Element Manager, navigate to **Routes and Trunks > Routes and Trunks**. The **Routes and Trunks** page is displayed on the right-hand side. Under the Customer number (Customer 0) expand the new SIP Route **104** which is configured in **Section 5.4** above and click on the **Add trunk** button (screen not shown). The new Trunk page is displayed as shown below.

In the **Basic Configuration** section, enter values as shown in the screen below. Virtual trunks can be created as single or multiple by entering a number in the **Multiple trunk input number** field which is normally an increment of 32. For the **Member number** and **Channel ID for this trunk** fields, enter 1 if this is a first virtual trunk of this Customer. In the testing, the number started from 97 since there are 96 SIP trunks already configured in Customer 0. This number is automatically incremented corresponding to the number of trunks created.



Click on the **Edit** button of **Class of Service** field to enable class of services **Digital Tone (DTN)** and **Unrestricted (UNR)** of new trunks as shown in the screen below. Click on the **Return Class of Service** button (not shown) at the bottom to return to the trunk configuration page.



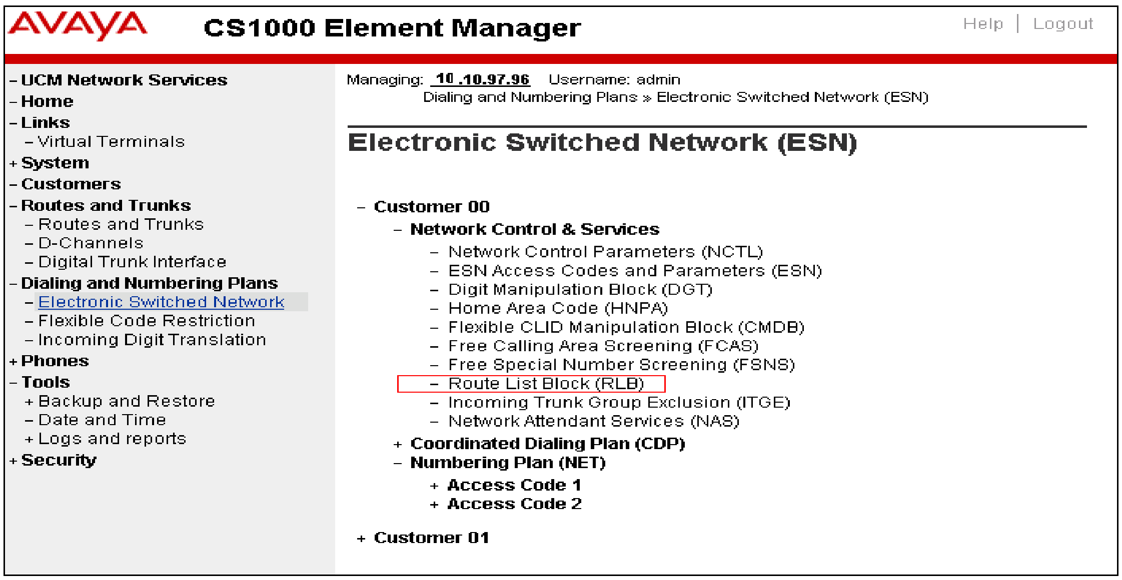
Keep all values at default for the **Advance Trunk Configurations** section. Click **Save** button at the bottom to save the changes.

5.6. Configure CDP Dialing Plan

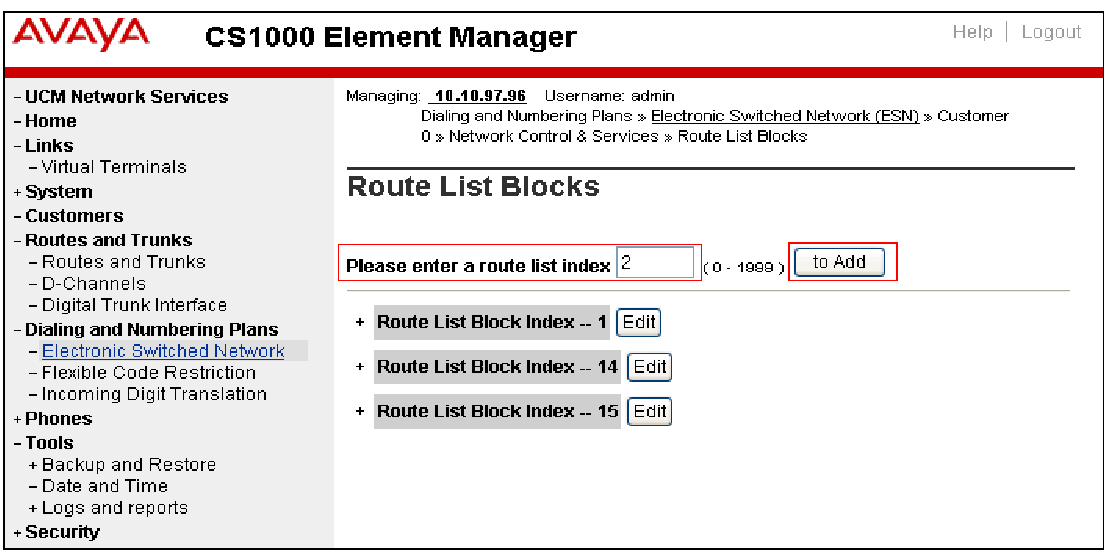
This section provides the steps on how to create a new Route List Index (RLI) and a new Distant Steering Code (DSC) for the Coordinated Dialing Plan (CDP) dialing plan.

5.6.1. Configure Route List Index (RLI)

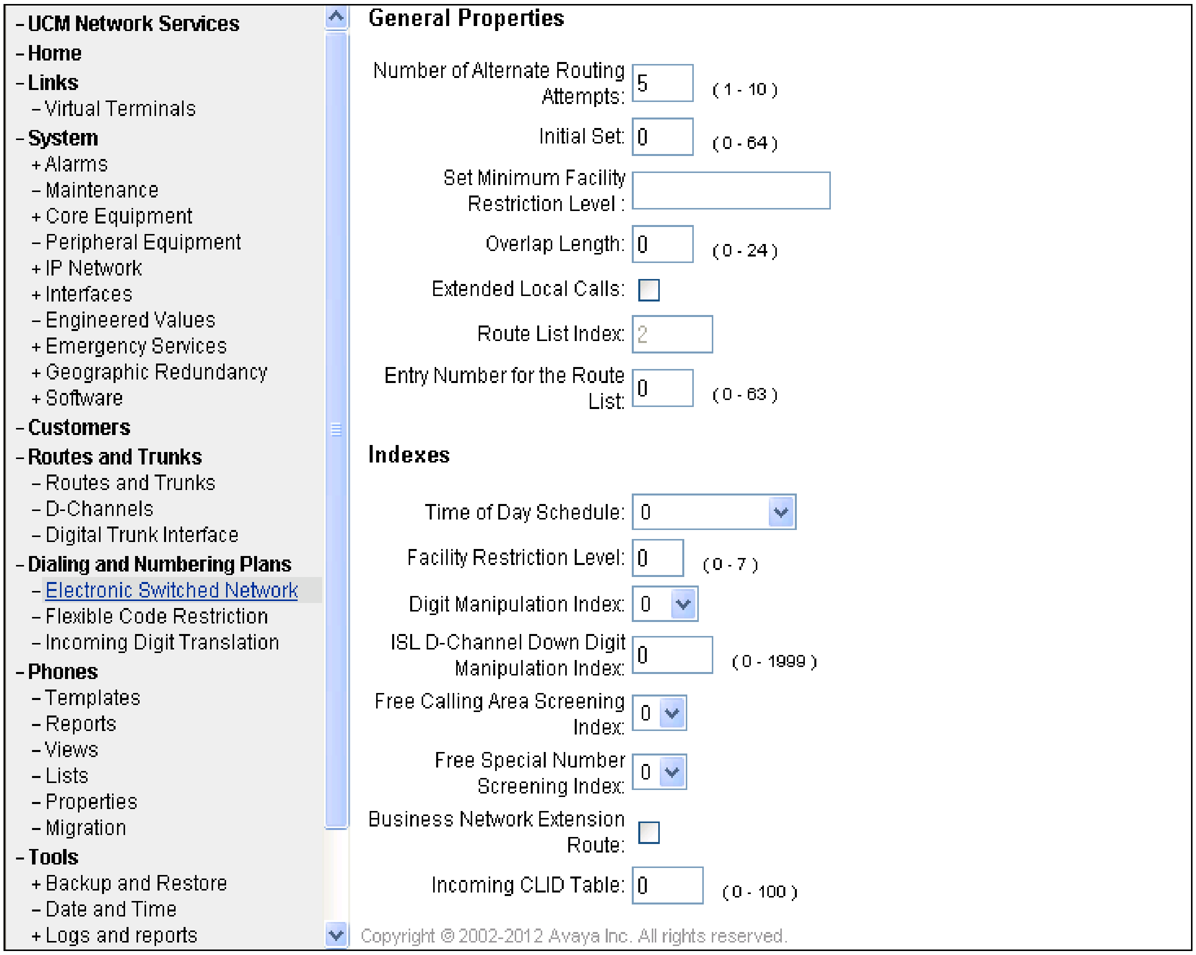
To configure Route List Index, from the home page of Element Manger, navigate to **Dialing and Numbering Plan > Electronic Switched Network**. The **Electronic Switched Network (ESN)** page is displayed as shown in the screen below.



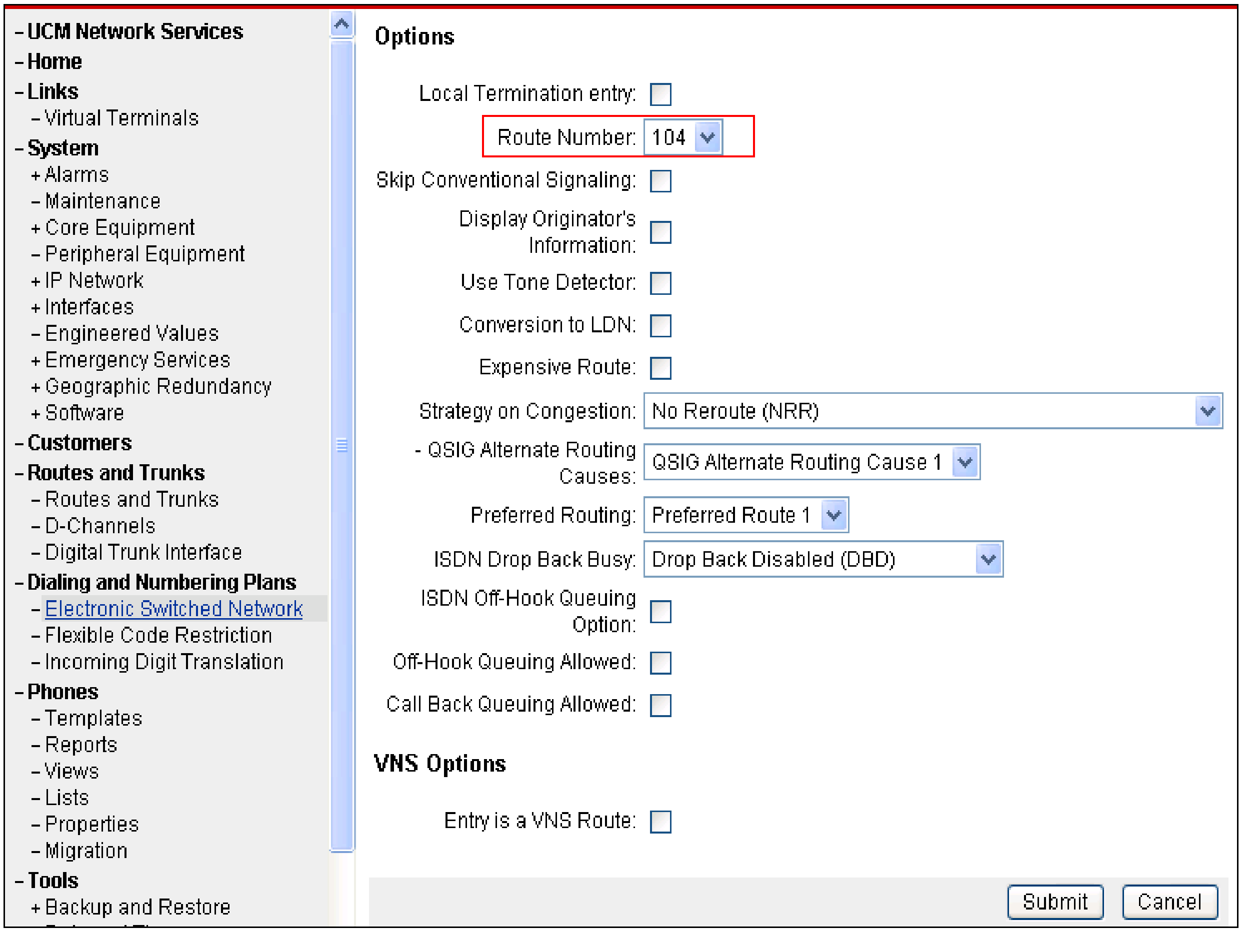
Click on the **Route List Block** (**RLB)** link from the screen above, the **Route List Blocks** page is displayed as the screen below. To create a new entry for route list index, enter a number, e.g. **2**, in the **Please enter a route list index** field and then click on **to Add** button.



The **General Properties** and **Indexes** sections of new route list index are displayed in the screen below. Keep all values at their defaults.



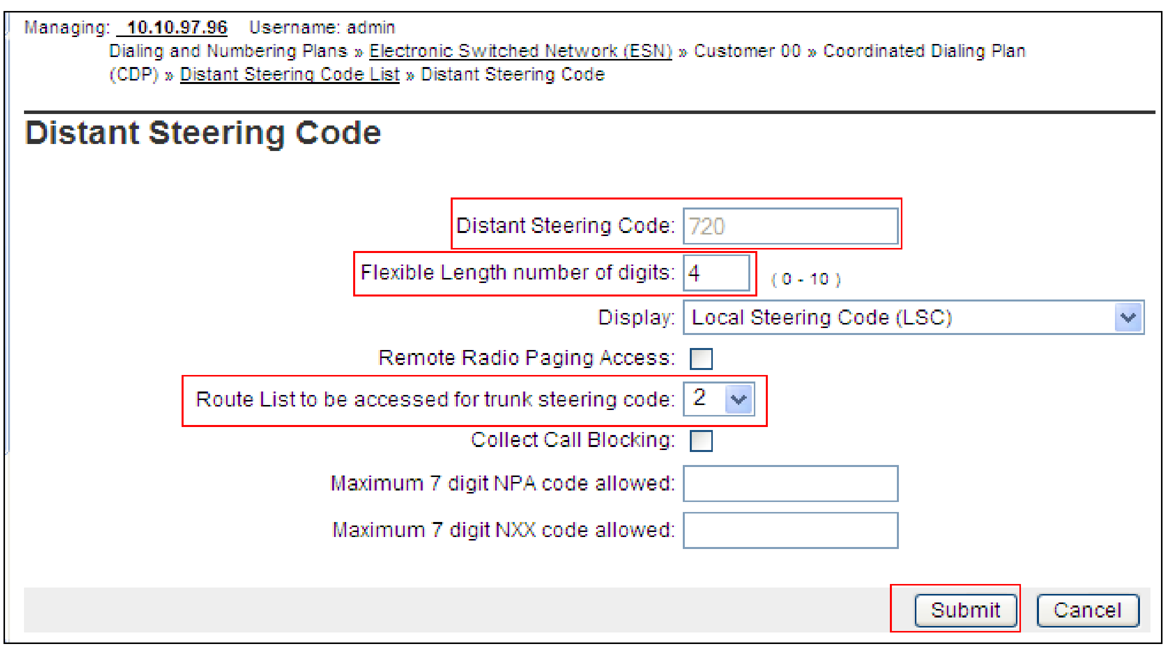
Scroll down to the **Options** and **VNS Options** section. Select the **Route Number 104** in the dropdown list corresponding with the SIP route created in **Section 5.5**. Keep all other values at their defaults. Click **Submit** button to complete the creation of the new route list index.



5.6.2. Create a Distant Steering Code (DSC)

From the home page of Element Manager, navigate to **Dialing and Numbering Plans → Electronic Switched Network → Coordinated Dialing Plan (CDP) → Distant Steering Code (DSC)**. The **Distant Steering Code List** page appears as shown in the screen below. Select **Add** in the dropdown menu, enter the DSC code **731** in the field **Please enter a distant steering code** and then click on to **Add** button.

The **Distant Steering Code** page is displayed as shown below. Enter **4** in the field **Flexible Length number of digits**, because the length of dialed number to Amcom Speech server is 5 digits. If 4 or 3 digits are planned, enter the corresponding length of digit in this field. Select the route list index **2** that is created above in the **Route List to be accessed for trunk steering code** dropdown list. Click on the **Submit** button to complete to add the new distant steering code **720**.



6. Configure Avaya Aura® Session Manager

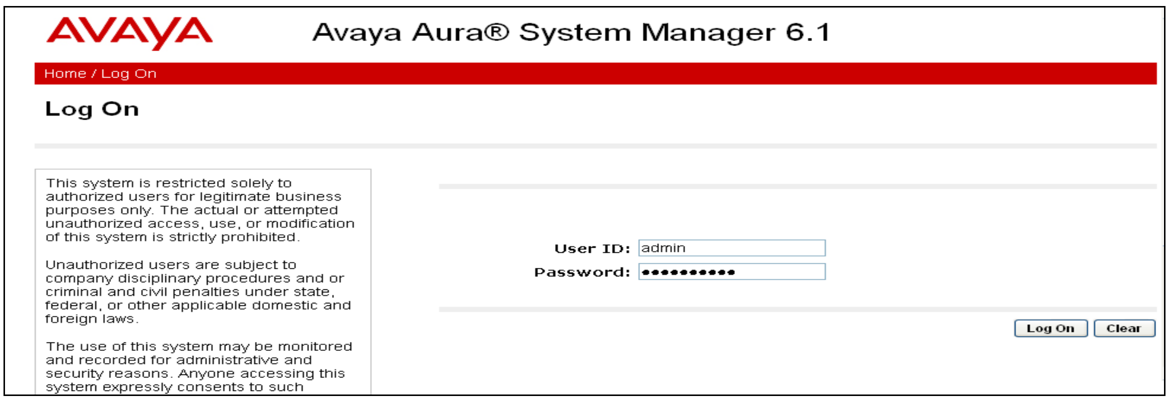
This section provides the procedures for configuring Session Manager. Session Manager is comprised of two functional components: The Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager web interface and is then downloaded 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
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element

6.1. Configure SIP Domain

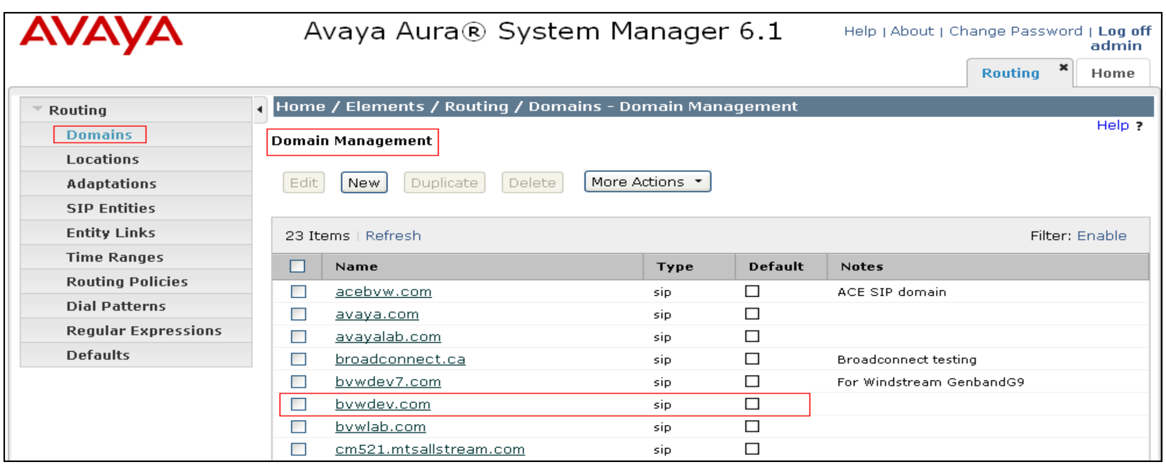
Launch a web browser, enter **https://<IP address of System Manager>** in the URL, and log in with the appropriate credentials.



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 CS1000 SIP Gateway in **Section 5.1**, 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.

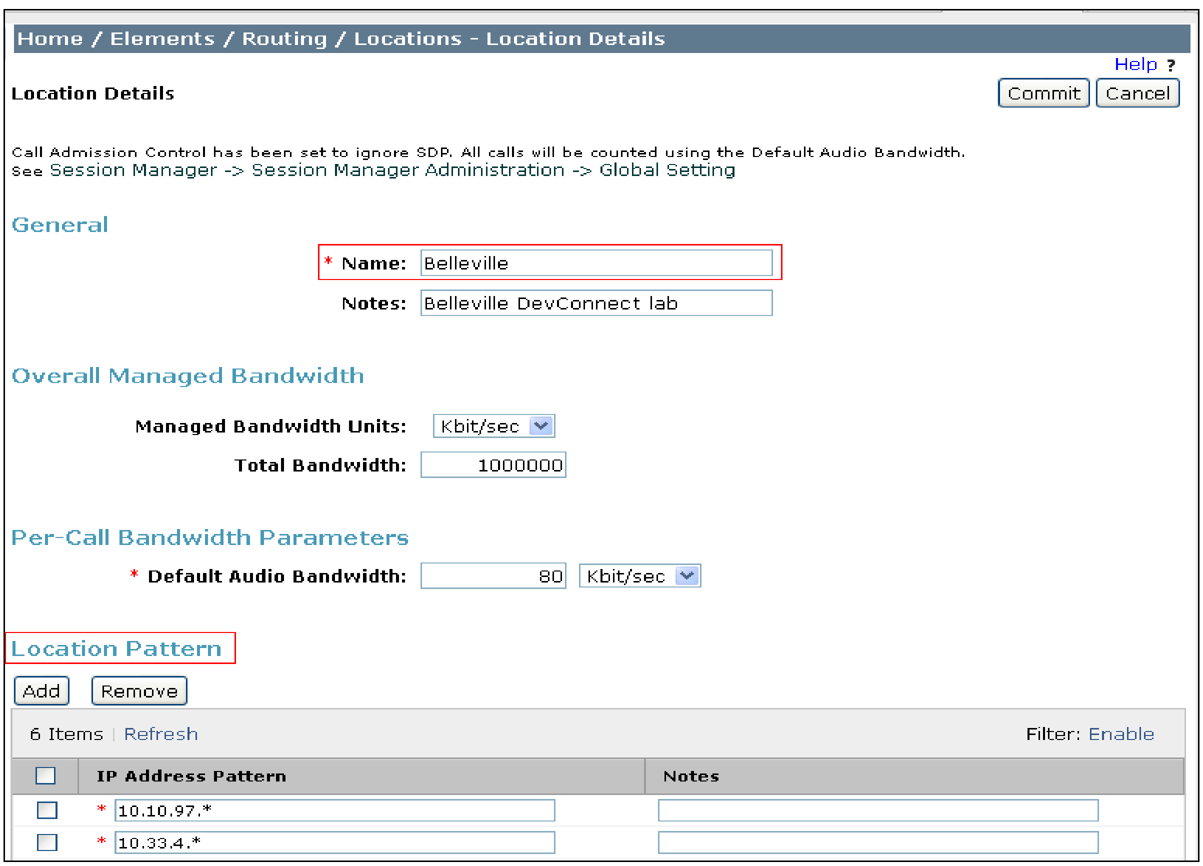
Location Pattern section

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.

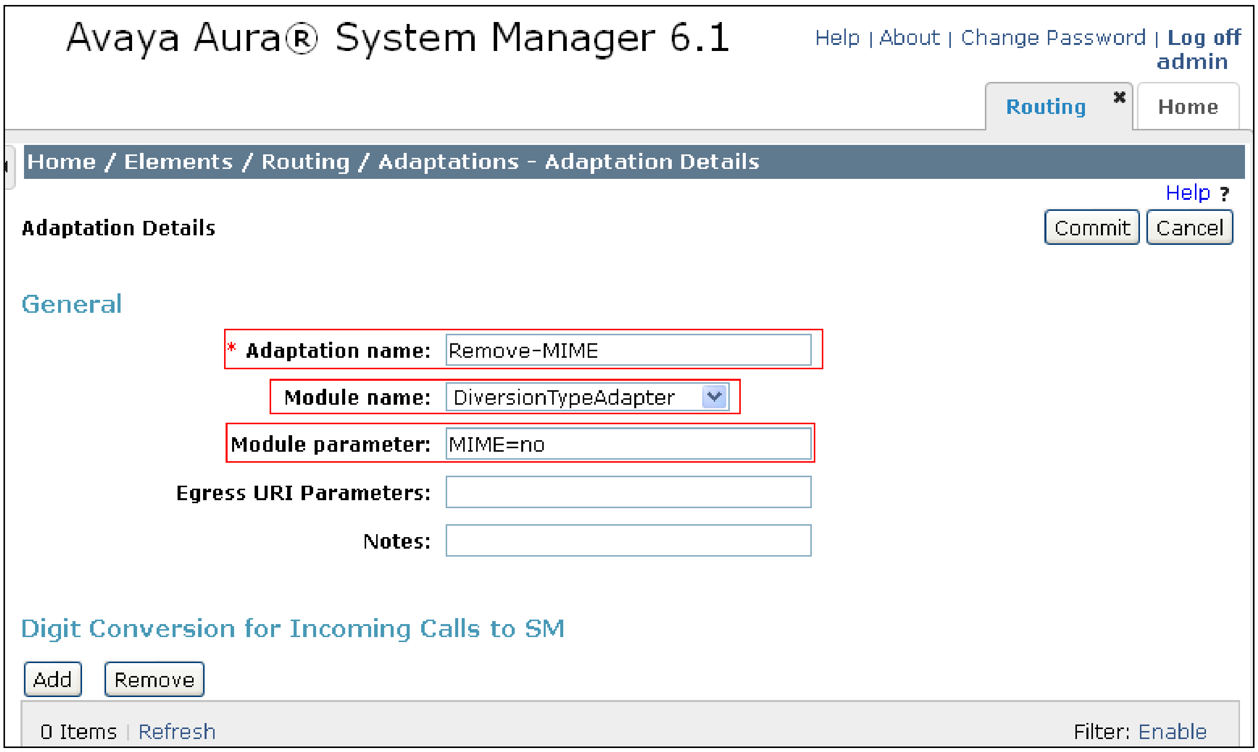


6.3. Configure Adaptations

An adaptation needs to be created to remove MIME part in the SIP INVITE message sent from CS1000. To create an adaptation, navigate to **Routing → Adaptations**. The Adaptations page is displayed on the right-hand (screen not shown). Click on **New** button to create a new adaptation.

In the Adaptation Details page, enter a descriptive name, e.g. **Remove-MIME**, in the Adaptation name field, select **DiversionTypeAdapter** in the **Module name** dropdown field and enter the string "**MIME=no**" in the Module **parameter** field. Click on the Commit button to save and finish creating a new adaptation.

Note that if the **Module name** dropdown list doesn't have **DiversionTypeAdapter**, select the **<click to add module>** option to add one. Enter the name **DiversionTypeAdapter**.



6.4. 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
- Avaya CS1000 SIP Gateway
- Amcom Speech server

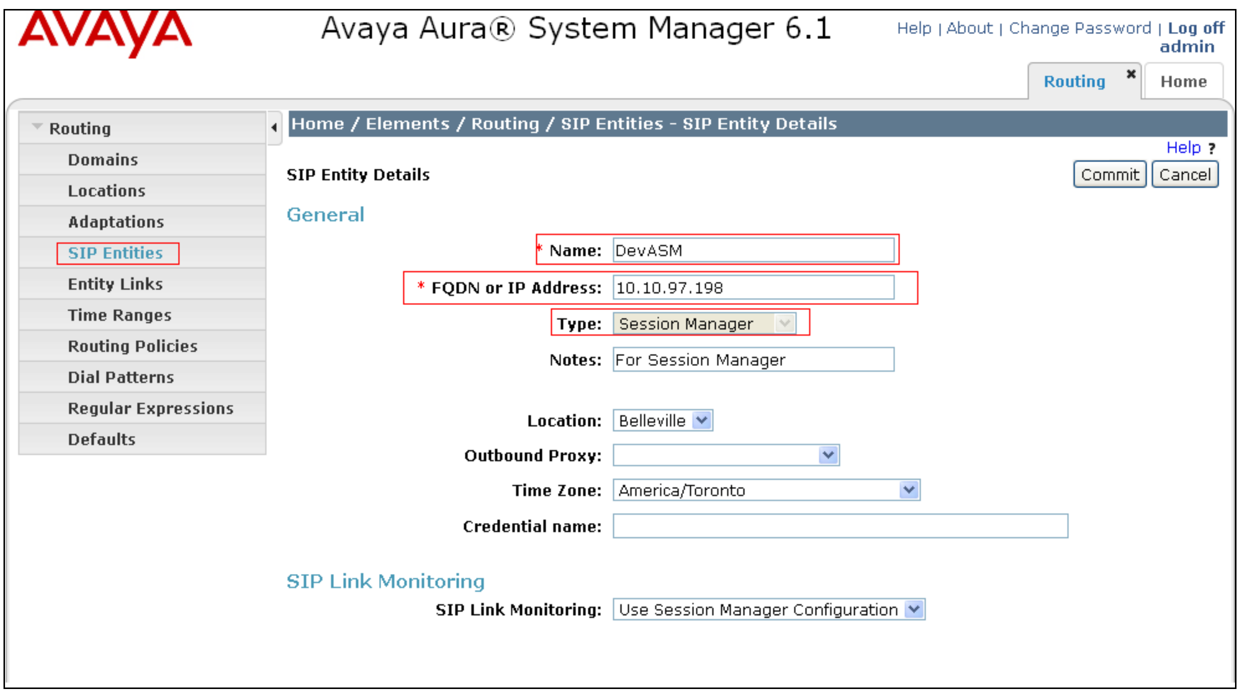
Navigate to **Routing →SIP Entities** and click on the **New** button to create a new SIP entity (screen not shown). Provide the following information:

<u>General section</u>
Enter the following and use default values for the remaining fields:

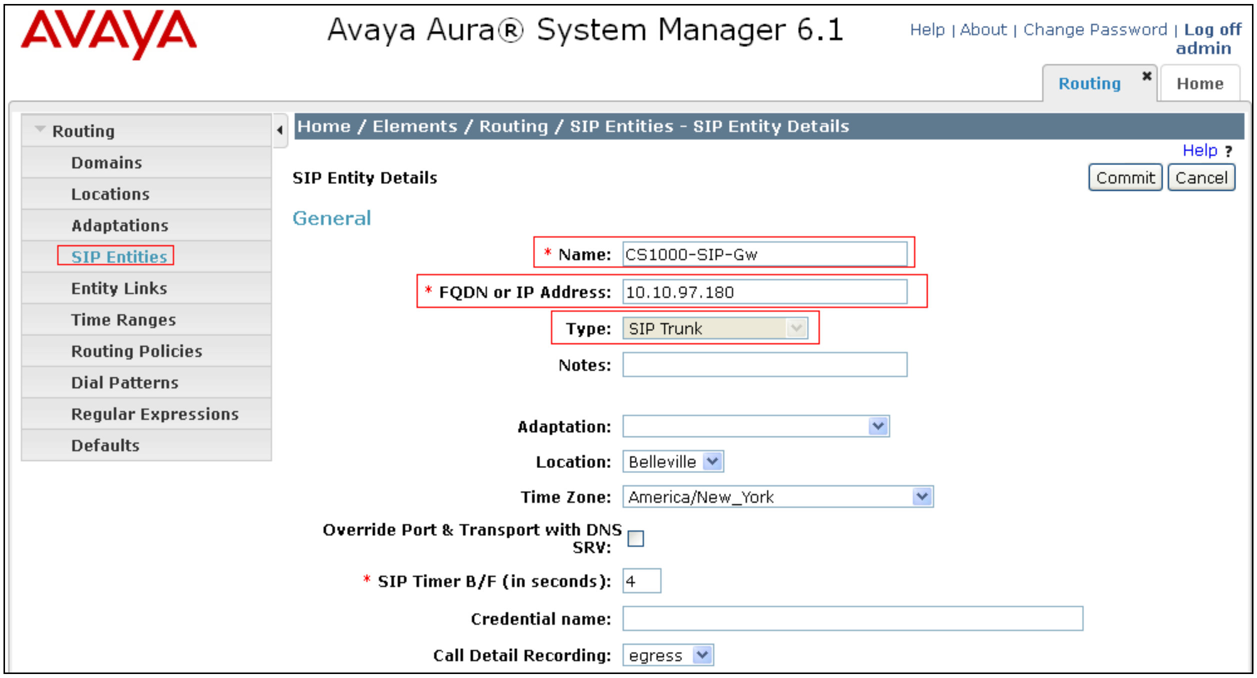
- **Name**: Enter a descriptive name.
- **FQDN or IP Address:** Enter the IP address of the signaling interface on each:
    - Avaya CS1000 SIP Gateway: **10.10.97.180**
    - Signaling Session Manager: **10.10.97.198**
    - Amcom Speech server: **10.10.98.123**
- From the **Type** dropdown list, select a type that best matches the SIP Entity:
    - For Avaya CS1000 SIP Gateway: select **SIP Trunk**
    - 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.

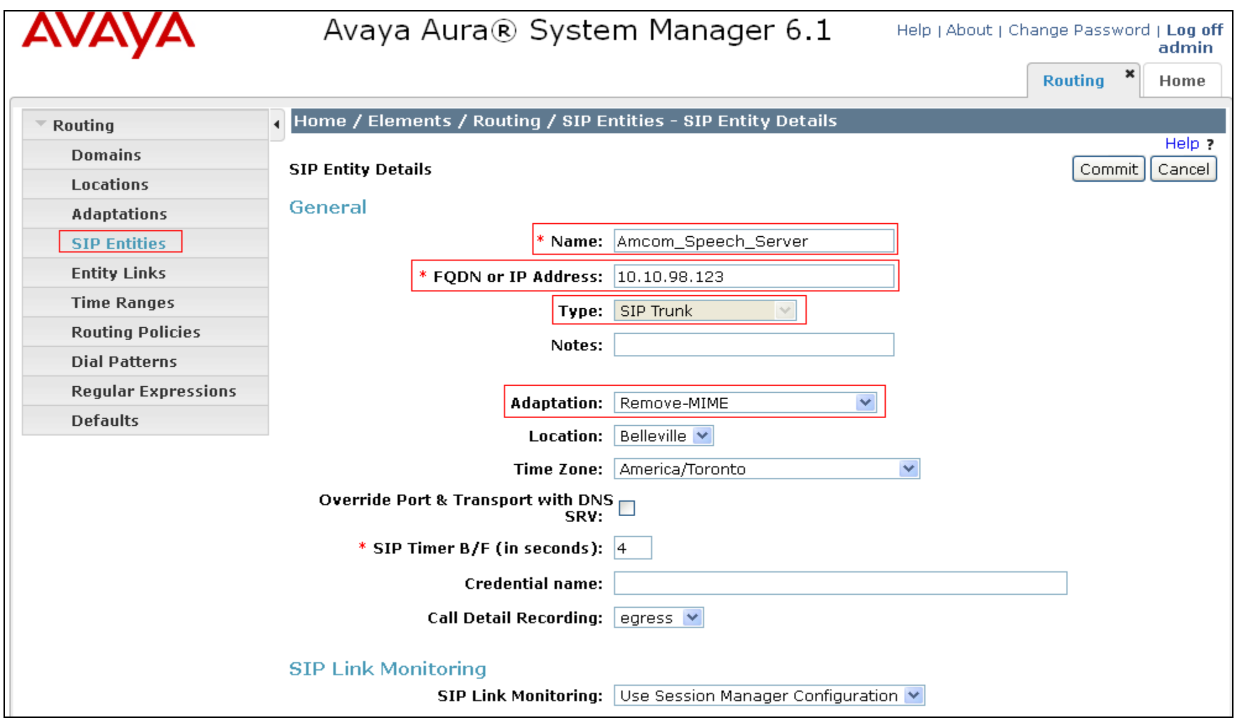
The screen below shows the detail of **Session Manger SIP Entity**.



The screen below shows the details of Avaya CS1000 SIP Entity.



The screen below shows the detail of **Amcom Speech server** SIP Entity. In the **Adaptation** field, select **Remove-MINE** adaptation as configured in **Section 6.3**.



6.5. Configure Entity Links

Entity Links define the connections between the SIP Entities (in this case, Avaya CS1000 SIP gateway and Amcom Speech server) and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Avaya CS1000 SIP Gateway
- 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. **DevASM**).
- 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 **CS1000-SIP-GW** for the entity links between Session Manager and Avaya CS1000 SIP gateway and select **Amcom_Speech_Server** 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 links between Session Manager and Avaya CS1000 SIP Gateway 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
☐	DevASM	TCP	* 5060	CS1000-SIP-Gw	* 5060	Trusted
☐	DevASM	UDP	* 5060	CS1000-SIP-Gw	* 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
☐	DevASM	TCP	* 5060	Amcom_Speech_Server	* 5060	Trusted
☐	DevASM	UDP	* 5060	Amcom_Speech_Server	* 5060	Trusted

Select : All, None

6.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section 6.4**) and Dial Patterns (**Section 6.8**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Avaya CS1000 SIP gateway.
- 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:

General section

- Enter a descriptive name in the **Name** field (e.g. **To-CS1000-SIPGw**, **To-Amcom-Speech**).
- Enter a description in the **Notes** field if desired.

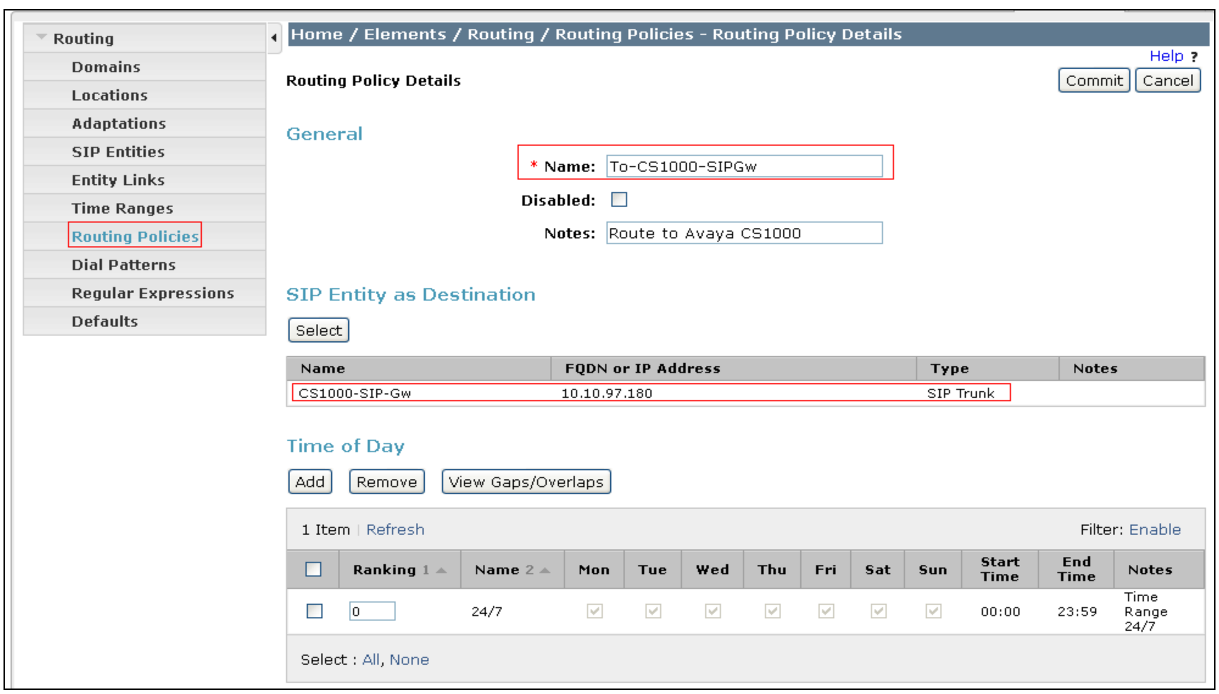
SIP Entity as Destination section

- 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.

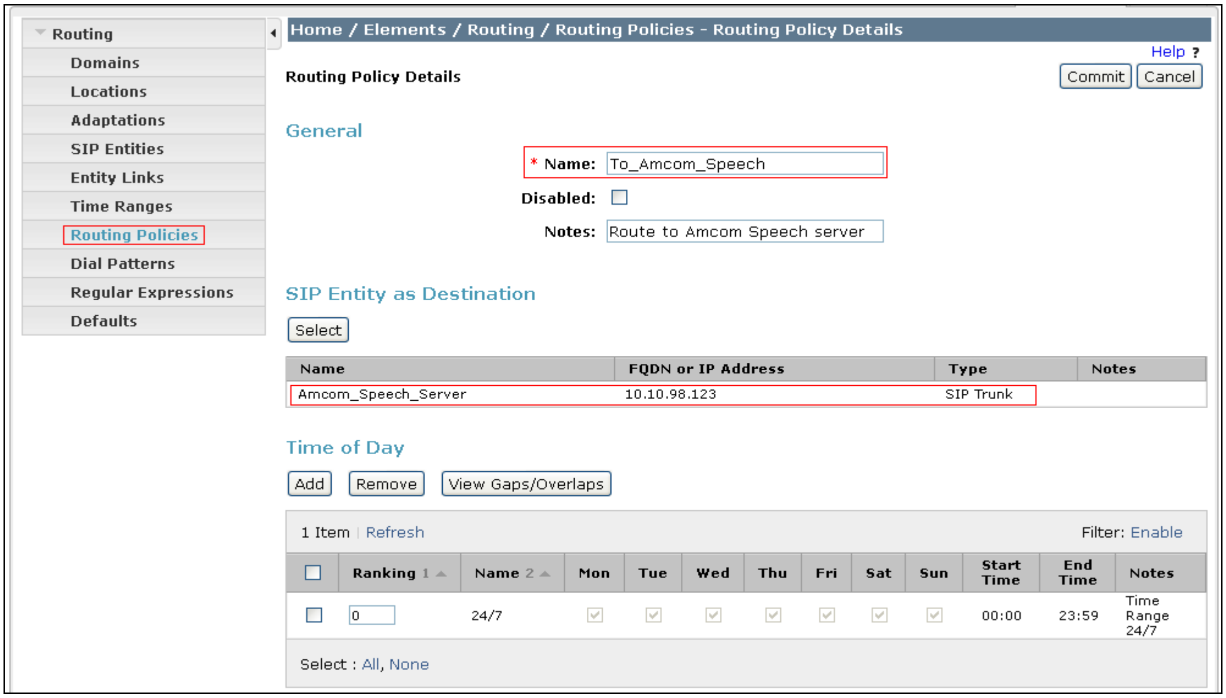
Time of Day section

- 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 Avaya CS1000 during the compliance test.



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



6.7. 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.

- **54xxx** – dial pattern used to route calls to Avaya CS1000.
- **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:

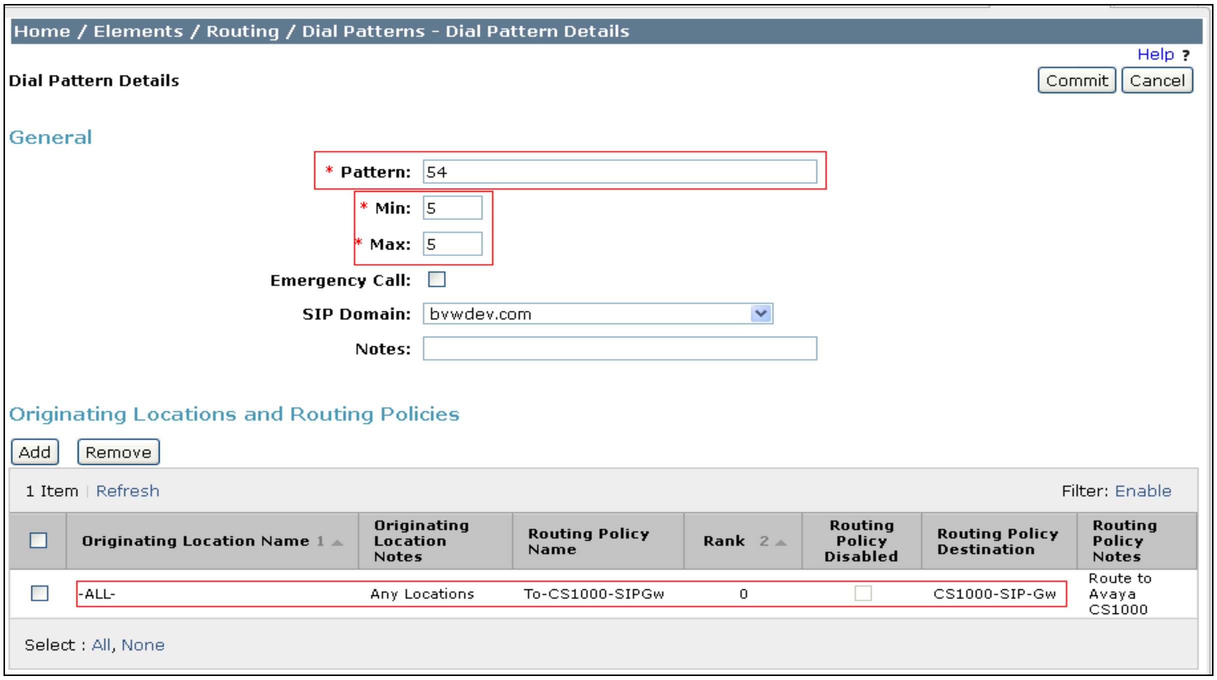
General section

- Enter a unique pattern in the **Pattern** field (e.g. **54**).
- 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**.

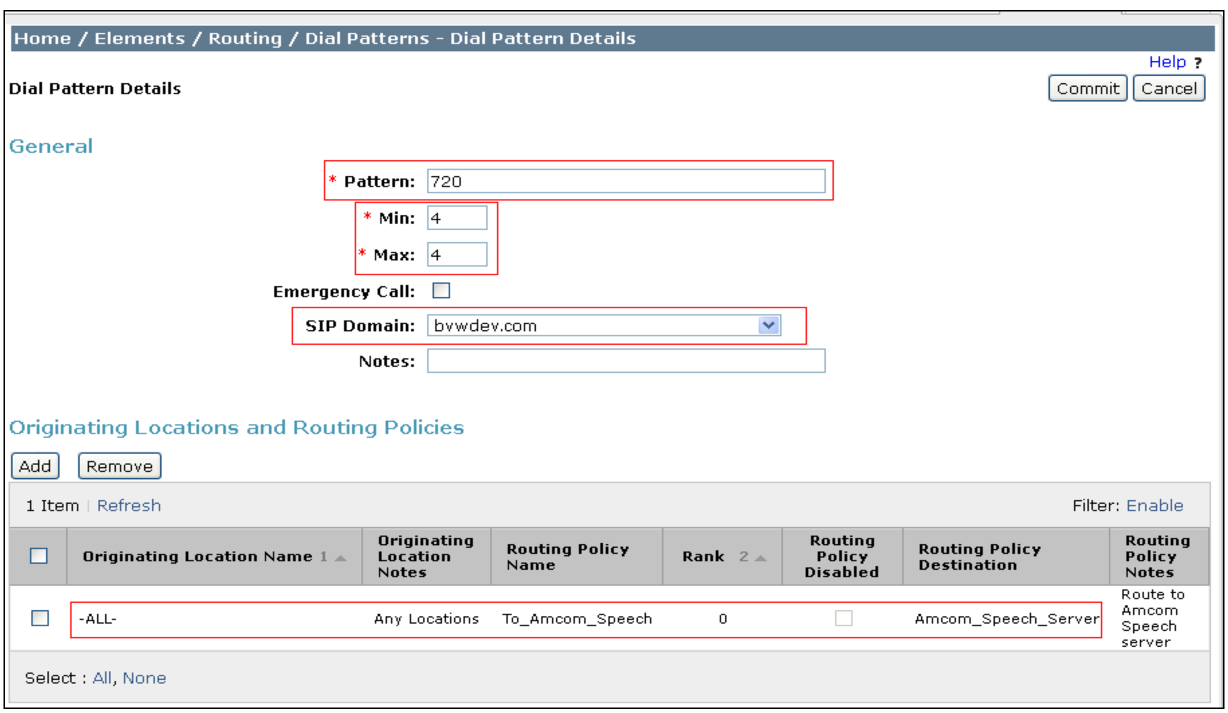
Originating Locations and Routing Policies section

- 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 **544xx** used to route calls to Avaya CS1000 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 a 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 login
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 Amcom Speech server to work with Avaya CS1000 and Avaya Aura® Session Manager.

- Verify the SIP trunk entity link status is up between Session Manager and Avaya CS1000 by navigating to **Elements →Session Manger → System Status → SIP Entity Monitoring** and select the CS1000 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: CS1000-SIP-Gw

Summary View

2 Items | Refresh   Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶Show	DevASM	10.10.97.180	5060	TCP	Up	200 OK	Up
▶Show	DevASM	10.10.97.180	5060	UDP	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_Server

Summary View

2 Items | Refresh   Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶Show	DevASM	10.10.98.123	5060	UDP	Up	200 OK	Up
▶Show	DevASM	10.10.98.123	5060	TCP	Up	200 OK	Up

- Place a call from CS1000 Phone A to the Amcom Speech server by dial 7200 which is the dial pattern of Amcom Speech server.
- Phone A is connected to the 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 CS1000 switch or different switch. For example, the call is transferred to Phone B that is located on the same CS1000 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 have described the administration steps required to integrate Amcom Speech Auto Attendant with the Avaya Communication Server 1000E via SIP trunk configured on the Avaya Aura® Session Manager. All test cases are passed with an important note in **Section Error! Reference source not found.**.

10. Additional References

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

[1] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Issue 1.1, Document Number03-603324
[2] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010
[3] *Avaya Communication Installation and Commissioning*, Doc# NN43041-310, Issue 05.04, Date May 2011.
[4] *Avaya Communication Server 1000 Unified Communications Management Common Services Fundamentals*, Doc # NN43001-116, Issue 05.11, Date June 2011.
[5] *Avaya Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals*, Doc # NN43001-509, Issue 03.02, Date June 2011.
[6] *Avaya Communication Server 1000 Element Manager System Reference - Administration*, Doc# NN43001-632, Issue 05.09, Date July 2011.

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.