Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Experience Portal 7.0, Aura® Communication Manager 6.3, Aura® Session Manager 6.3, Avaya Session Border Controller for Enterprise 6.2 with AT&T IP Flexible Reach-Enhanced Features Service SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Experience Portal 7.0, Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.2.1 with the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **MIS/PNT** transport connections.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Experience Portal 7.0, Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.2.1 (referred to in the remainder of this document as Avaya SBCE) with the AT&T IP Flexible Reach-Enhanced Features SIP trunking service (referred to in the remainder of this document as IPFR-EF). The AT&T IP Flexible Reach-Enhanced Features SIP trunking service utilizes AVPN[1] or MIS/PNT[2] transport connections.

Avaya Aura® Experience Portal 7.0 is a speech-enabled Interactive Voice Response (IVR) system that allows an enterprise to provide multiple self and assisted service resources to their customers, in a flexible and customizable manner. In addition, Avaya Proactive Outreach Manager (POM) was installed on the Experience Portal platform. Avaya Proactive Outreach Manager is a managed application of Avaya Aura® Experience Portal, providing a solution for unified, outbound calling capabilities.

Avaya Aura® Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® System Manager 6.3 is used to provision and manage Avaya Aura® Session Manager.

Avaya Aura® Communication Manager 6.3 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager.

The Avaya Session Border Controller for Enterprise 6.2.1 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach-Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T Flexible Reach service is one of the many SIP-based Voice over IP (VoIP) services offered to enterprises for their voice communication needs. The AT&T IP Flexible Reach-Enhanced Features service is a SIP based service which includes additional network based features to the IP Flexible Reach service.

2. General Test Approach and Test Results

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

[1] AVPN supports compressed RTP (cRTP).
[2] MIS/PNT does not support cRTP.

The interoperability compliance testing focused on verifying inbound call flows from IPFR-EF to the Customer Premises Equipment (CPE) containing the Avaya platforms (see **Section 3.2** for call flow examples). The test environment consisted of:

- A simulated enterprise with Experience Portal (including Proactive Outreach Manager for outbound calling), System Manager, Session Manager, Communication Manager, Avaya SBCE, Avaya Aura® Messaging, and Avaya telephones.
- An IPFR-EF production circuit, to which the simulated enterprise was connected via AVPN transport.

2.1. Interoperability Compliance Testing

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the IPFR-EF network. Calls were made from the PSTN across the IPFR-EF network, to the CPE.

Note – Avaya Experience Portal utilizes application scripts to define interactive capabilities (e.g., menus, call routing, etc), between Experience Portal, the service provider, and the rest of the CPE. Customers may develop their own applications to meet their specific needs, or consult Avaya Professional Services and/or authorized Avaya Business Partners. The programming and testing of such applications are beyond the scope of this document.

In the reference configuration, basic Experience Portal functionality used in the SIP trunk testing described in this document was provided by sample VXML and CCXML test scripts, included as part of the Experience Portal installation.

The following features were tested and verified as part of this effort:

- Verification of SIP Trunking between Experience Portal, System Manager, Session Manager, Communication Manager, Avaya SBCE, Avaya Aura® Messaging, and the IPFR-EF service.
- Experience Portal inbound and outbound (utilizing Proactive Outreach Manager) call processing.
- Inbound caller interaction with Experience Portal applications, including prompting, caller DTMF input, wait treatment (e.g., announcements), Automatic Speech Recognition, and Text to Speech.
- Experience Portal Call Forward (Bridged Transfer feature) with Diversion Header (see **Section 2.2, item 7**).
- Experience Portal Blind Transfer to Communication Manager. In this call flow, Experience Portal sends Refer to the Avaya SBCE. *The Avaya SBCE processes the Refer* and generates a new Invite to a Communication Manager extension for call termination (see **Section 2.2, item 4a**).
- Experience Portal Blind Transfer to PSTN (an IPFR-EF feature). In this call flow Experience Portal sends a Refer to the SBCE. *The Avaya SBCE passes the Refer through to*

AT&T for processing. The AT&T network then redirects the call to the new destination (see **Section 2.2, item 4b**).
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729A, G.729B, and G.711mu codec support.
- Inbound T.38 fax (to Communication Manager).

Note – Many IPFR-EF network features require DTMF interaction with the caller for these features to be activated. The sample Experience Portal applications used during testing did not have outbound DTMF capability[3]. Therefore, the following IPFR-EF service features were not accessed by Experience Portal as part of this testing effort[4]:

- Network based Simultaneous Ring.
- Network based Sequential Ring (Locate Me).
- Network based Call Forwarding Always (CFA/CFU).
- Network based Call Forwarding Ring No Answer (CF-RNA).
- Network based Call Forwarding Busy (CF-Busy).
- Network based Call Forwarding Not Reachable (CF-NR).

2.2. Test Results

The test objectives stated in **Section 2.1**, with limitations as noted below, were verified.

Note – As indicated in **Section 3.2.6**, Avaya SBCE 6.2.1 loads Q07 and Q16 were used during testing, and some behavior differences are noted. Issue 2 existed in load Q07, but is fixed in load Q16. Issue 3 is specific to the Q16 load only. All other items listed in this section are common to loads Q07 and Q16.

1. **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block headers containing private CPE information), the Avaya SBCE is provisioned to remove SIP headers not required by AT&T. The following headers are removed; *P-Location, Alert-Info, Endpoint-View, AV-Correlation-ID, Remote-Party-ID, AV-Global-Session-ID,* and *P-AV-Message-ID* (see **Section 9.4.3**).

2. **Avaya SBCE inserts Remote-Address header containing local CPE addressing**. The Avaya SBCE adds the Remote Address header, (even though the option to perform this action is not enabled), advertizing local CPE addressing to AT&T.
   a) The workaround is to have the Avaya SBCE remove this header (see **Section 9.3.9**).

---

[3] Custom Experience Portal applications could be written to perform these DTMF based interactions with IPFR-EF.

[4] If Experience Portal redirects the call to a Communication Manager station/Agent, then the IPFR-EF features could be successfully accessed manually. See these documents for more information; *Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 4.0.5, with AT&T IP Flexible Reach - Enhanced Features – Issue 1.0* - or - *Application Notes for Avaya Aura® Communication Manager/Local Survivable Processor 6.3, Avaya Aura® Branch Session Manager 6.3, and Avaya Session Border Controller for Enterprise 6.2.1, with AT&T IP Flexible Reach - Enhanced Features Service – Issue 1.0*

b) An MR has been opened with the Avaya SBCE team.
    - **UPDATE** – This issue is fixed in the Avaya SBCE 6.2.1 Q16 release.

3. **Avaya SBCE 6.2.1 Signaling Manipulation Sigma script %BODY parameter not executed in load Q16**. Avaya SBCE signaling manipulation Sigma scripts are used to modify the contents of SIP messages, either sent by the CPE or AT&T (see **Section 9.3.9**). These scripts either modify contents to fix interoperability issues, or to remove unwanted/unsupported headers.
   Testing found that when Avaya SBCE 6.2.1 load Q16 is used, signaling manipulation script statements containing the %BODY parameter were not executed, (these scripts statements work correctly in previous loads, such as Q07).
   a) If load Q16 is used, any scripts utilizing the %BODY parameter must be rewritten using alternate methods.
      - An MR has been opened with the SBCE team.
        - **UPDATE** 9/29/14 – This issue is fixed in the Avaya SBCE 6.2.1 Q18 release.

4. **Avaya SBCE Refer Handling/URI Group not functioning.** The Avaya SBCE feature *Refer Handling*, when enabled, causes the Avaya SBCE to process any SIP Refer messages received on the associated interface (this option is disabled by default, causing the Avaya SBCE to pass all Refer messages through). As an additional option, the Refer Handling feature can also specify *URI Group* criteria as a discriminator, whereby Refer messages matching the URI Group criteria are processed by the Avaya SBCE, while Refer messages that do not match the URI Group criteria, are passed through.
   Testing found that the Avaya SBCE does *not* discriminate Refer messages based on the URI Group criteria. ***As a result of this issue, the following Refer based call redirection scenarios are mutually exclusive***:
   a) For Experience Portal "Blind Transfer" call redirection to CPE platforms, (e.g., to Communication Manager, see **Section 3.2.2**), where Experience Portal generates a Refer to the Avaya SBCE, for *processing by the Avaya SBCE*, the Refer Handing feature must be *enabled* (see **Section 9.3.2**). As a result, *the Avaya SBCE will process all Refer messages* received on the specified interface.
   b) For Experience Portal "Blind Transfer" network call redirection back to the IPFR-EF network, (see **Section 3.2.3**), where Experience Portal generates a Refer to the Avaya SBCE for *processing by the IPFR-EF service*, the Refer Handing feature must be *disabled*. As a result, *the Avaya SBCE will pass all Refer messages* received on the specified interface, on to AT&T.
      - No workaround for this issue is currently available.
      - An MR has been opened with the Avaya SBCE team.
        - **UPDATE** 9/29/14 – This issue is fixed in the Avaya SBCE 6.2.1 Q18 release.

5. **Experience Portal *ptime* value provisioning only applies to Experience Portal initiated dialogs, resulting in an RTP packet interval of 20ms for inbound calls.** The AT&T network guidelines specify that an RTP packet interval of 30ms be used (*ptime=30*). In addition, the AT&T network only specifies a *maxptime=30* parameter for inbound Invites. Therefore, CPE equipment must specify *ptime=30* in their response SDP (e.g., 200ok). Testing found that Experience Portal did not send a *ptime* parameter in the responses (which implies *ptime=20*). As a result the IPFR-EF network used *ptime=20* as well.
    a) While Experience Portal can be provisioned to include *ptime=30* (see **Section 6.6**), this will only occur for dialogs originated by Experience Portal (e.g., Invites). Experience Portal responses to AT&T initiated dialogs (e.g., 200ok), will use the AT&T packet interval value. Since a ptime value is not specified by AT&T, a value of *ptime=20* is assumed, and Experience Portal uses an RTP packet interval of 20ms. This is expected behavior for Experience Portal.
        - A SIP header manipulation is applied to the Avaya SBCE, to add a *ptime=30* parameter to the AT&T *maxptime=30* parameter already in the Invite. The result is Experience Portal uses an RTP packet interval of 30ms (*ptime=30*) in responses (see **Section 9.3.9**).

6. **Loss of Music on Hold for IPFR-EF customers, if Network Call Redirection (NCR) is enabled on Communication Manager SIP trunks used for call access to/from AT&T**. If NCR is enabled on a SIP trunk used for calls to/from AT&T, Communication Manager will use *SendOnly* to signal Mute/Hold. The IPFR-EF network responds to this with *Inactive* (instead of *RecvOnly*). Therefore whenever Communication Manager sends Music On Hold (e.g., during Hold, Transfers, and Conference sequences), the IPFR-EF network will not send the audio, and the PSTN endpoint does not hear the Music on Hold.
    a) The workaround for this issue is to have the Avaya SBCE remove the *SendOnly* parameter (see **Section 9.3.9**). This causes AT&T to reply with *SendRecv*.
    b) **UPDATE** 7/13/14 – A fix for this issue has been implemented in the IPFR-EF network, so the Avaya SBCE signaling manipulation is no longer required.

7. **Experience Portal does not support Diversion Header.** The AT&T IPFR-EF service requires that a Diversion header is included in new Invites to the network, generated by Call Forward scenarios. The Experience Portal "Bridged Transfer" function is such a scenario (see **Section 3.2.4**).
    a) The Avaya SBCE is used to insert the Diversion header (see **Section 9.3.9**).

8. **Emergency 911/E911 Services Limitations and Restrictions** – Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) documented in these Application Notes will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is the customer's responsibility to ensure proper operation with the equipment/software vendor.

    While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when the E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions**.**

2.3. Support

For more information on the AT&T IP Flexible Reach service visit: http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/. AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

The reference Customer Premises Equipment (CPE) configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- **Experience Portal 7.0** is a speech-enabled Interactive Voice Response (IVR) system that allows an enterprise to provide multiple self and assisted service resources to inbound callers. Experience Portal consists of one or more Media Processing Platform (MPP) servers and an Experience Portal Manager (EPM) server. A single "server configuration" was used in the reference configuration, consisting of a single MPP and EPM, running on a VMware environment. This VMware environment also included an Apache Tomcat Application Server hosting the VXML and CCXML application scripts that provide the directives to Experience Portal for handling the inbound calls. In addition, a Speech Server, (Windows 2008 server), consisting of Nuance Recognizer and Nuance Vocalizer provided Automatic Speech Recognition (ASR) and Text-To-Speech (TTS) capabilities to Experience Portal.
- **Proactive Outreach Manager 3.0** is installed on Experience Portal, and provides outbound dialing capabilities.
- **Session Manager 6.3** provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, (e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc.) across the enterprise. Avaya SIP endpoints register to Session Manager.
- **System Manager 6.3** provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- **Communication Manager 6.3** provides the voice communication services for a particular enterprise site, including Agent login and queuing. Avaya H.323 endpoints register to Communication Manager.

- **Avaya SBCE 6.2.1** provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPFR-EF service and the enterprise internal network. In the reference configuration the Avaya SBCE also processes SIP Refer messages generated by Experience Portal, to direct inbound calls to their associated destinations on Communication Manager.
- **Avaya G430 Media Gateway** provides media resources for Communication Manager (Music on Hold, announcements, etc) and telephones. This solution is extensible to other Avaya Media Gateways.
- **Avaya Aura® Messaging 6.3** is used in the reference configuration to provide voice messaging capabilities during testing. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Avaya desk telephones are represented with Avaya 96x1 Series IP Telephones (running H.323 or SIP firmware).
- UDP and TCP transport protocols are used in the reference configuration. The IPFR-EF service specifies SIP over UDP to communicate with enterprise edge SIP devices, (e.g., the Avaya SBCE). In the reference configuration, SIP over TCP was used to communicate between Session Manager, the Avaya SBCE, Experience Portal, and Avaya Aura® Messaging, as well as to the Communication Manager public SIP trunk. This was done to facilitate protocol trace analysis. TLS transport was used between Session Manager and the Communication Manager local trunk (Avaya SIP telephones access). However, Avaya best practices call for TLS to be used as the transport protocol whenever possible.
- Inbound and outbound calls were placed via an IPFR-EF production AVPN circuit.

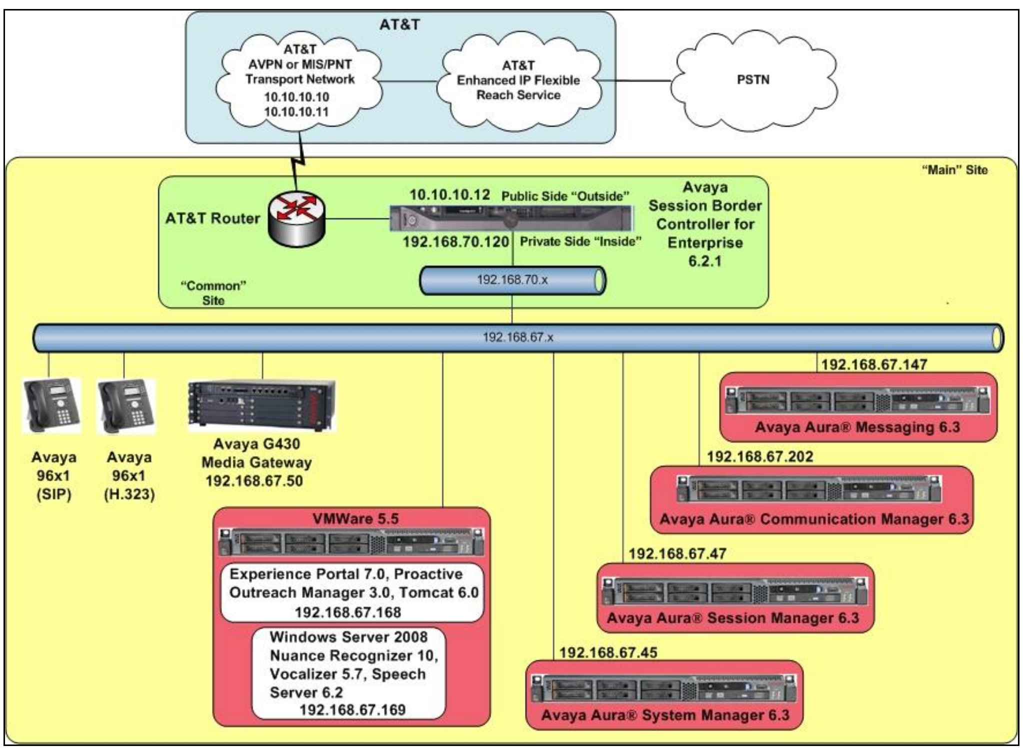


Figure 1: Reference C

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference 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
Main Site	
Avaya Aura® System Manager	
IP Address	192.168.70.45
Avaya Aura® Session Manager	
Management IP Address	192.168.67.46
Network IP Address	192.168.67.47
Avaya Aura® Communication Manager	
IP Address	192.168.67.202
Avaya Aura® Communication Manager extensions	19xxx (stations) 4xxxx (Agents and VDNs)
Avaya Experience Portal/Proactive Outreach Manager	
Network IP Address	192.168.67.168
Avaya Aura® Messaging	
IP Address	192.168.67.147
Windows 2008 Server/Nuance	
Network IP Address	192.168.67.169
Common Site	
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Outside (Public) Interface	10.10.10.12 (see note below)
IP Address of Inside (Private) Interface	192.168.70.120

Table 1: Illustrative Values Used in these Application Notes

NOTE – The Avaya SBCE Outside interface communicates with AT&T Border Elements (BEs) located in the AT&T IPFR-EF network. For security reasons, the IP addresses of the AT&T BEs are not included in this document. However as placeholders in the following configuration sections, the IP addresses **10.10.10.12** (Avaya SBCE public interface), **10.10.10.10,** and **10.10.10.11** (AT&T BE IP addresses), are specified. In addition, AT&T DID/DNIS numbers shown in this document are examples as well. AT&T Customer Care will provide the actual Border Element IP addresses and DID/DNIS numbers as part of the IPFR-EF provisioning process.

Note – Documents used to provision the test environment are listed in **Section 13**. References to these documents are indicated by the notation **[x]**, where *x* is the document reference number.

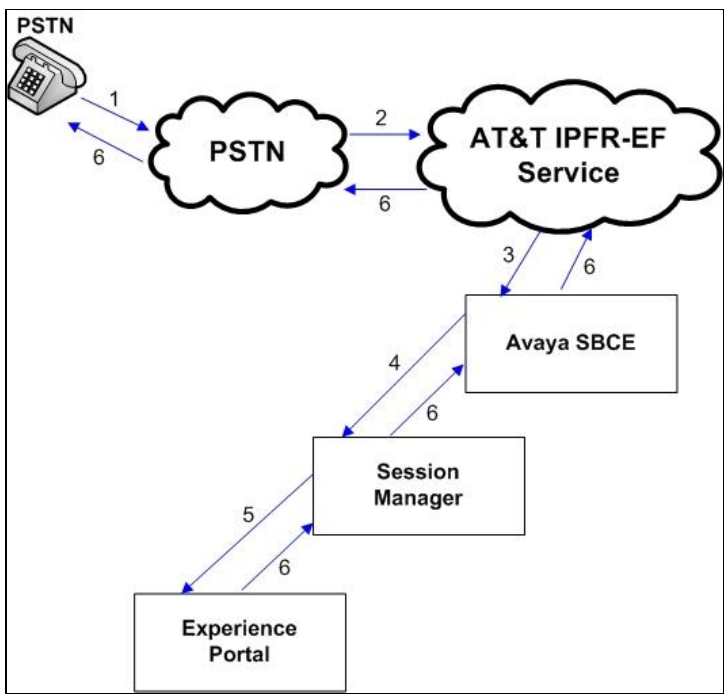
3.2. Call Flows

To understand how IPFR-EF service calls are processed in an Experience Portal environment, several basic call flows are described in this section.

3.2.1. Inbound call To Experience Portal only.

The call scenario illustrated below is an inbound call arriving and remaining on Experience Portal.

1. A PSTN phone originates a call to an AT&T IPFR-EF service number.
2. The PSTN routes the call to the AT&T IPFR-EF service network.
3. The AT&T IPFR-EF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and/or digit conversions, and based on configured Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Experience Portal.
6. Experience Portal matches the called party number to an application script, answers the call, and handles the call according to the directives specified in the application. In this scenario, the application sufficiently meets the caller's needs or requests, and thus the call does not need to be transferred to another platform.

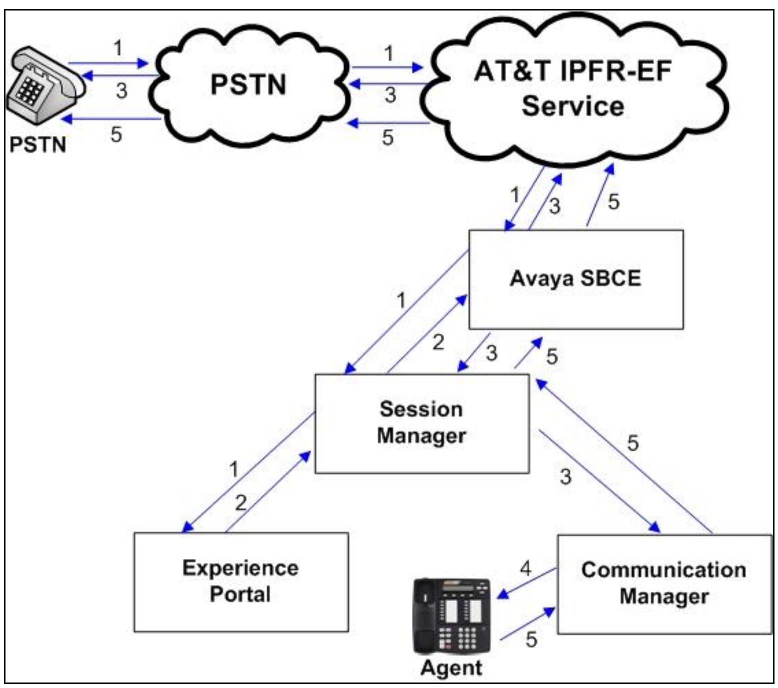


Inbound Call processed Entirely by Experience Portal

3.2.2. Experience Portal "Blind Transfer" to Communication Manager (Refer)

This call scenario describes the call flow for an Experience Portal "Blind Transfer" to a CPE destination, (e.g., Communication Manager). In this Blind Transfer scenario, Experience Portal responds to an inbound call with a redirection to a Communication Manager Agent/skill extension. This new destination number is specified in the Refer that is processed by the Avaya SBCE (see **Section 2.2, Item 4a**).

1. Same as the first five steps from the first call scenario in **Section 3.2.1**.
2. When the caller selects an option requesting an Agent, Experience Portal redirects the call by sending a Refer (containing a Communication Manager Agent/skill extension) to the Avaya SBCE.
3. In this scenario, ***the Avaya SBCE processes the Refer***, and sends an Invite to the Communication Manager (via Session Manager) for the selected Communication Manager extension (e.g., to a Skill VDN queue, directly to an Agent, etc). In addition, the Avaya SBCE places the inbound call on hold.
4. Communication Manager routes the call to the Agent.
5. When the Agent answers, the Avaya SBCE takes the call off hold and the caller is connected to the Agent. Experience Portal is disconnected from the call.

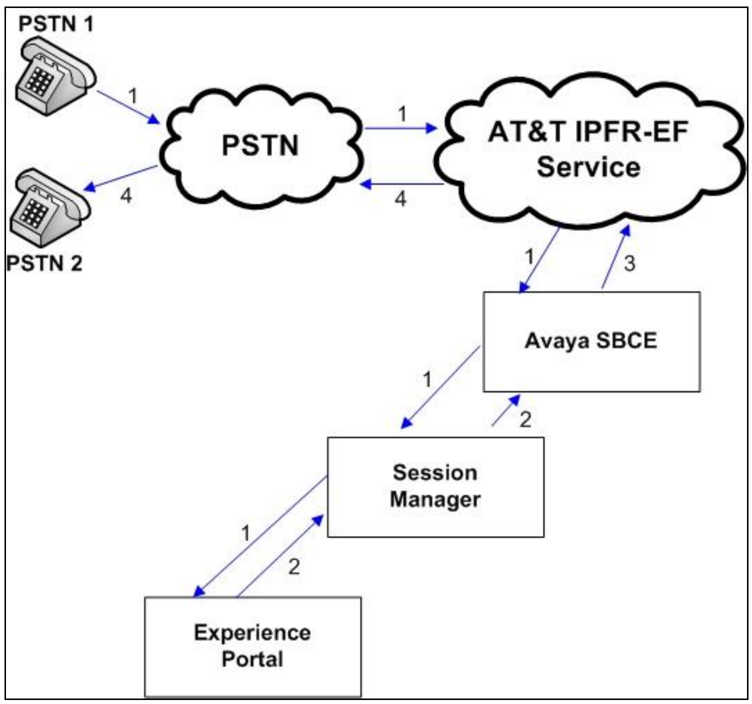


Experience Portal Blind Transfer to Communication Manager

3.2.3. Experience Portal "Blind Transfer" to PSTN (Refer)

This call scenario describes the call flow for an Experience Portal "Blind Transfer" to another PSTN destination. However, unlike the scenario described in **Section 3.2.2**, the new destination number specified in the Refer, is passed by the Avaya SBCE to AT&T, for processing by the IPFR-EF service (see **Section 2.2, Item 4b**).

1. Same as the first five steps from the first call scenario in **Section 3.2.1**.
2. Experience Portal redirects the call to a different PSTN destination by sending a Refer to the Avaya SBCE.
3. In this scenario, ***the Avaya SBCE does not process the Refer***, but instead sends it on to the IPFR-EF service for processing.
4. The AT&T IPFR-EF service redirects the call to the new PSTN destination, and Experience Portal is disconnected from the call.



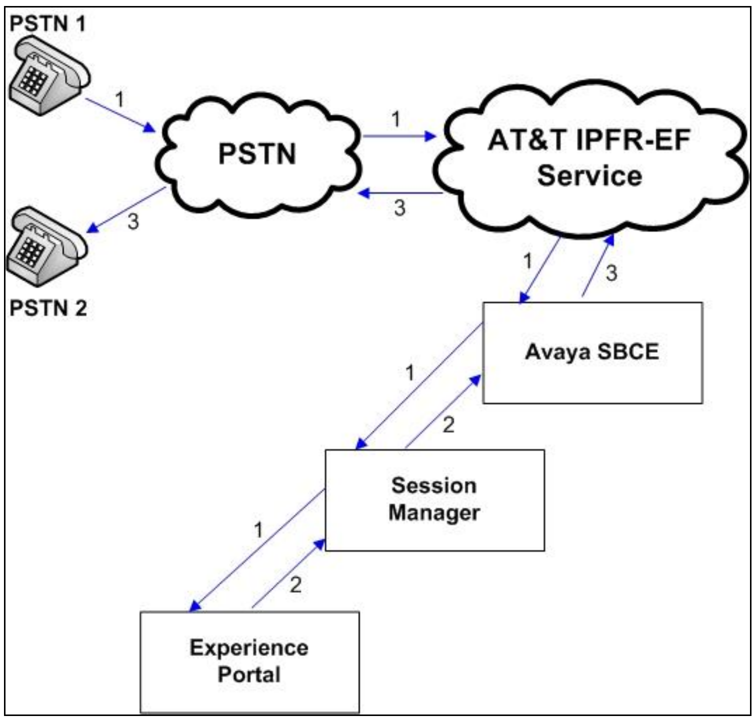
Experience Portal Blind Transfer to PSTN

3.2.4. Experience Portal “Bridged Transfer” (Diversion Header)

This call scenario describes the call flow for an Experience Portal “Bridged Transfer”. In this scenario, a PSTN call into an Experience Portal application prompts the caller to specify a different PSTN destination number. Experience Portal then issues an Invite back to AT&T for this new PSTN destination. The AT&T IPFR-EF service requires that this new Invite includes a Diversion header. However Experience Portal does not support Diversion header. As a result, the Avaya SBCE inserts a Diversion Header prior to sending the new Invite to AT&T (see **Section 9.3.9**).

Note – The Diversion header must contain a valid IPFR-EF DID number assigned to the CPE, or the new Invite will be denied.

1. Same as the first five steps from the first call scenario in **Section 3.2.1**.
2. After the caller specifies a number for PSTN 2, Experience Portal generates a new Invite.
3. The Avaya SBCE adds a Diversion header, and sends the Invite to AT&T.

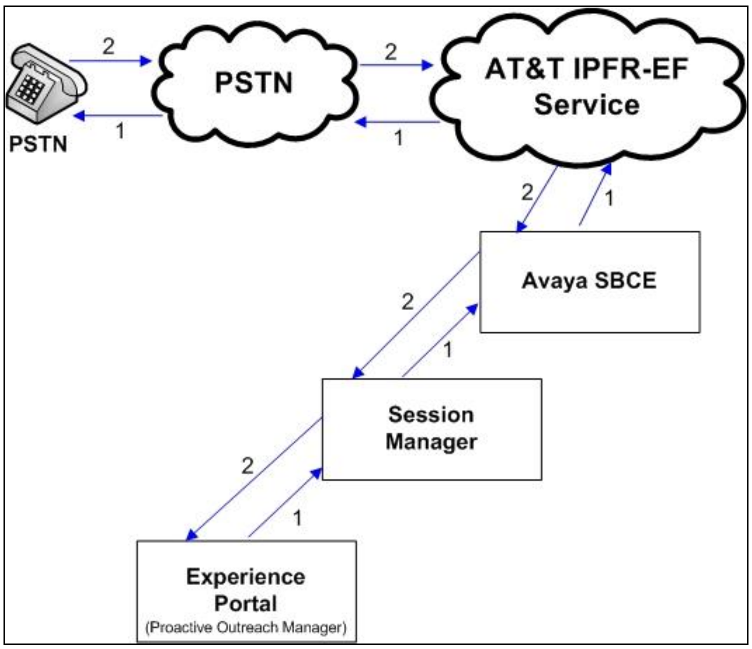


Experience Portal Bridged Transfer to PSTN

3.2.5. Experience Portal Outbound (using the Proactive Outreach Manager)

This call scenario describes an Experience Portal outbound call flow, utilizing the Proactive Outreach Manager application. Proactive Outreach Manager defines "campaign" scripts to provide the outbound calling capability for Experience Portal. Campaigns may be defined to do simple outbound announcement calls, or more complex ones that involve customer interaction.

1. In this scenario, a Proactive Outreach Manager campaign places a call to a customer. When the customer answers, the Proactive Outreach Manager campaign plays an announcement.
2. Alternatively, the Proactive Outreach Manager campaign may interact with the customer, requesting verbal and/or DTMF input.



Experience Portal/Proactive Outreach Manager Outbound Call

3.2.6. Equipment and Software Validated

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

Equipment/Software	Release/Version
HP Proliant DL360 G7 server • System Platform • Avaya Aura® System Manager	 • 6.3.0.0.18002 (with patch 08002) • 6.3.7 (r3702275)
IBM 8800 server • Avaya Aura® Session Manager	 • 6.3 SP7 (6.3.7.0.637008)
Dell S8510 server • System Platform • Avaya Aura® Communication Manager	 • 6.3.0.0.18002 • 6.3 SP5 (03.0.124.0-21460)
HP Proliant DL120 G7 server • VMWare ESXi • Experience Portal ○ Proactive Outreach Manager ○ Tomcat • Windows Server 2008 R2 ○ Nuance Recognizer ○ Nuance Vocalizer ○ Nuance Speech Server	 • 5.1.0 • 7.0 • 3.0 • 6.0.37 • 10.0 • 5.7 • 6.2
Dell R610 • System Platform • Avaya Aura® Messaging	 • 6.3.0.0.18002 (with patch 08002) • 6.3.0.0.11315
Avaya G430 Media Gateway	• 34.5.1
Dell R210 • Avaya Session Border Controller for Enterprise	 • 6.2.1 Q07 and 6.2.1 Q16[5]
Avaya 96x1 IP Telephones	• H.323 Version 6.3116 • SIP Version 6.3.1.13

Table 2: Equipment and Software Versions

[5] See the note in **Section 2.2** regarding these releases.

4. Configure Avaya Aura® Session Manager Release 6.3

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

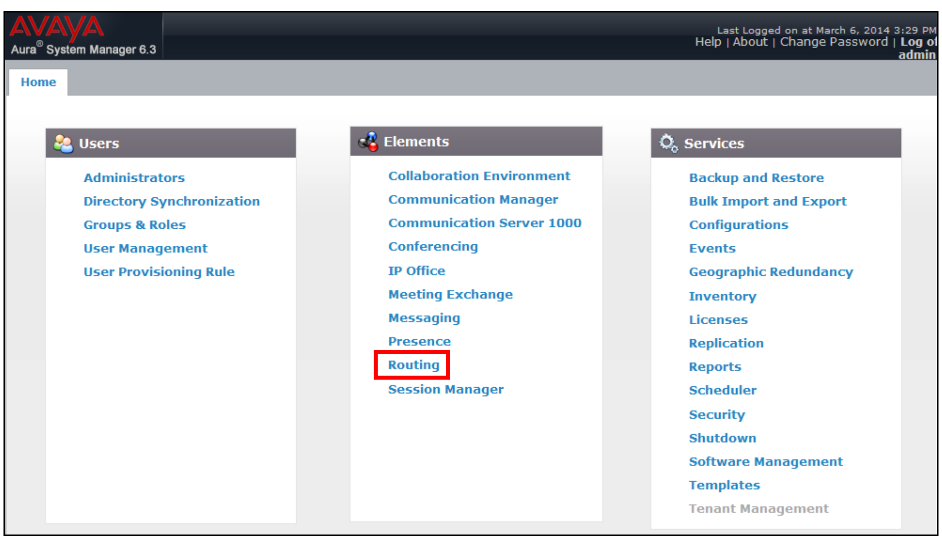
Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult documents **[5 & 6]** for further details if necessary.

This section provides the procedures for configuring Session Manager to receive calls from the AT&T IPFR-EF service (via the Avaya SBCE) and route these calls over the SIP trunks defined to Experience Portal, Communication Manager, and the Avaya SBCE.

The following administration activities will be described:

- Define SIP Domain.
- Define Locations.
- Define SIP Entities corresponding to Experience Portal, Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Define Entity Links between Session Manager and the various SIP Entities.
- Define Routing Policies associated with Experience Portal, Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



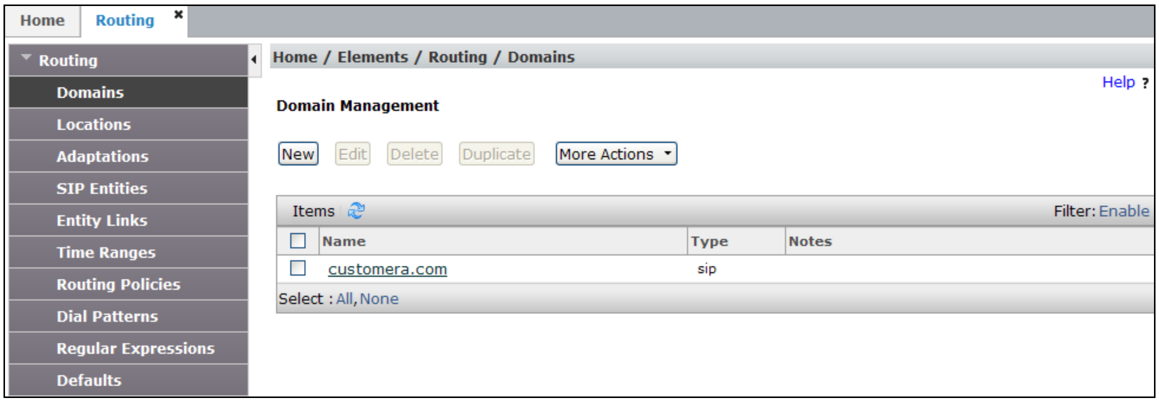
4.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration, domain **customera.com** was defined.

Step 2 - Click **New** (not shown)**.** Enter the following values and use default values for remaining fields**.**

- **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **customera.com** is shown.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description.

Step 3 - Click **Commit** to save.



4.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g., 192.168.67.x for all devices on a particular subnet), or individual devices (e.g., 192.168.67.46 for a device's specific IP address). In the reference configuration, two Locations are specified:

- **Main** (**192.168.67.***) – The Location defining the majority of the CPE equipment (e.g., System Manager, Session Manager, Experience Portal, Communication Manager, and Avaya Aura® Messaging).
- **Common** (**192.168.70.***) – The Location defining the Avaya SBCE.

Note – Two Locations are specified due to the specific network topology of the test reference configuration. A single Location, or more than two Locations, may be used as applicable.

4.2.1. Main Location

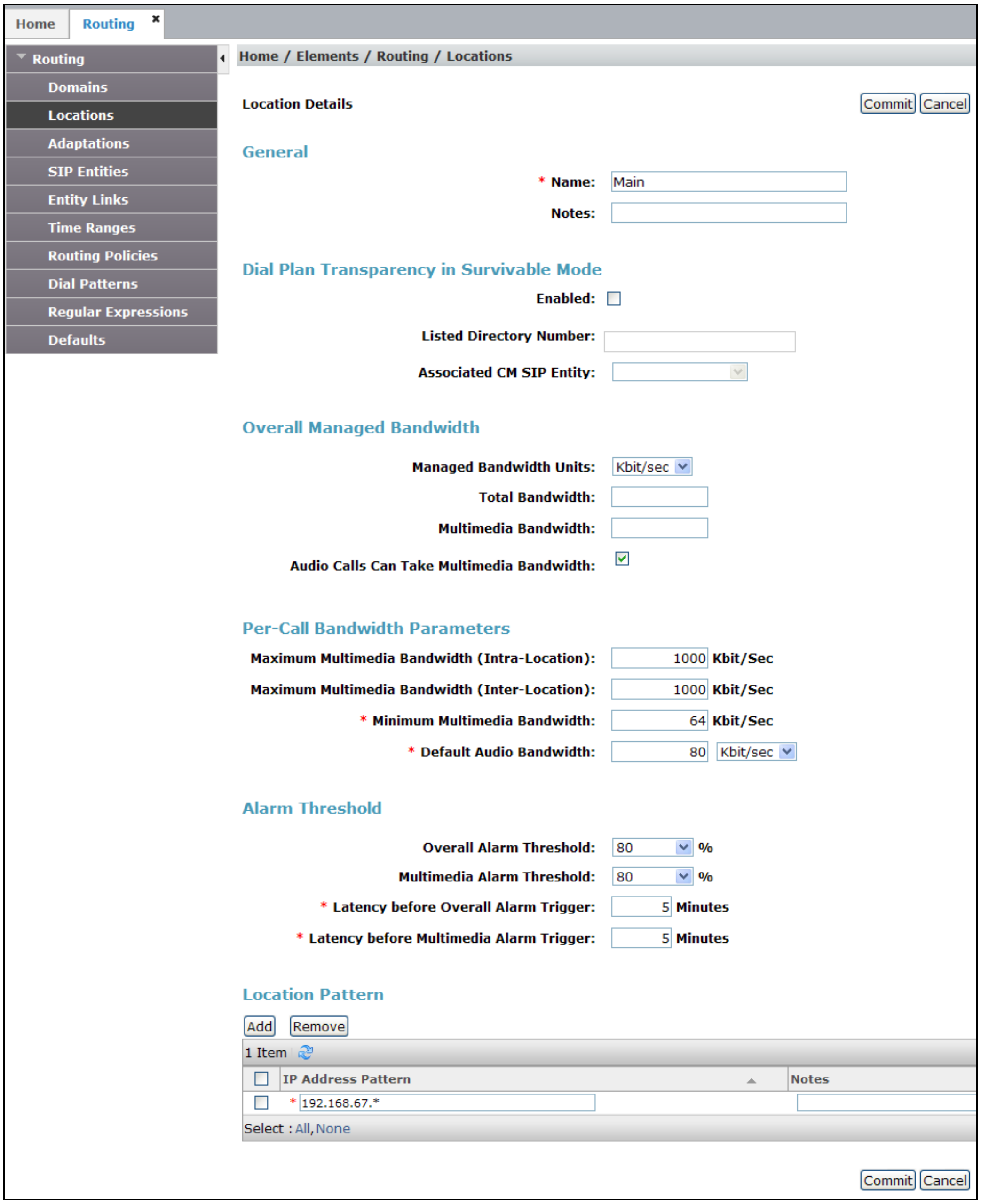
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the Location (e.g., **Main**).
- **Notes:** Add a brief description.

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern:** Enter the IP address of the CPE subnet (e.g., **192.168.67.***).
- **Notes:** Add a brief description if desired.

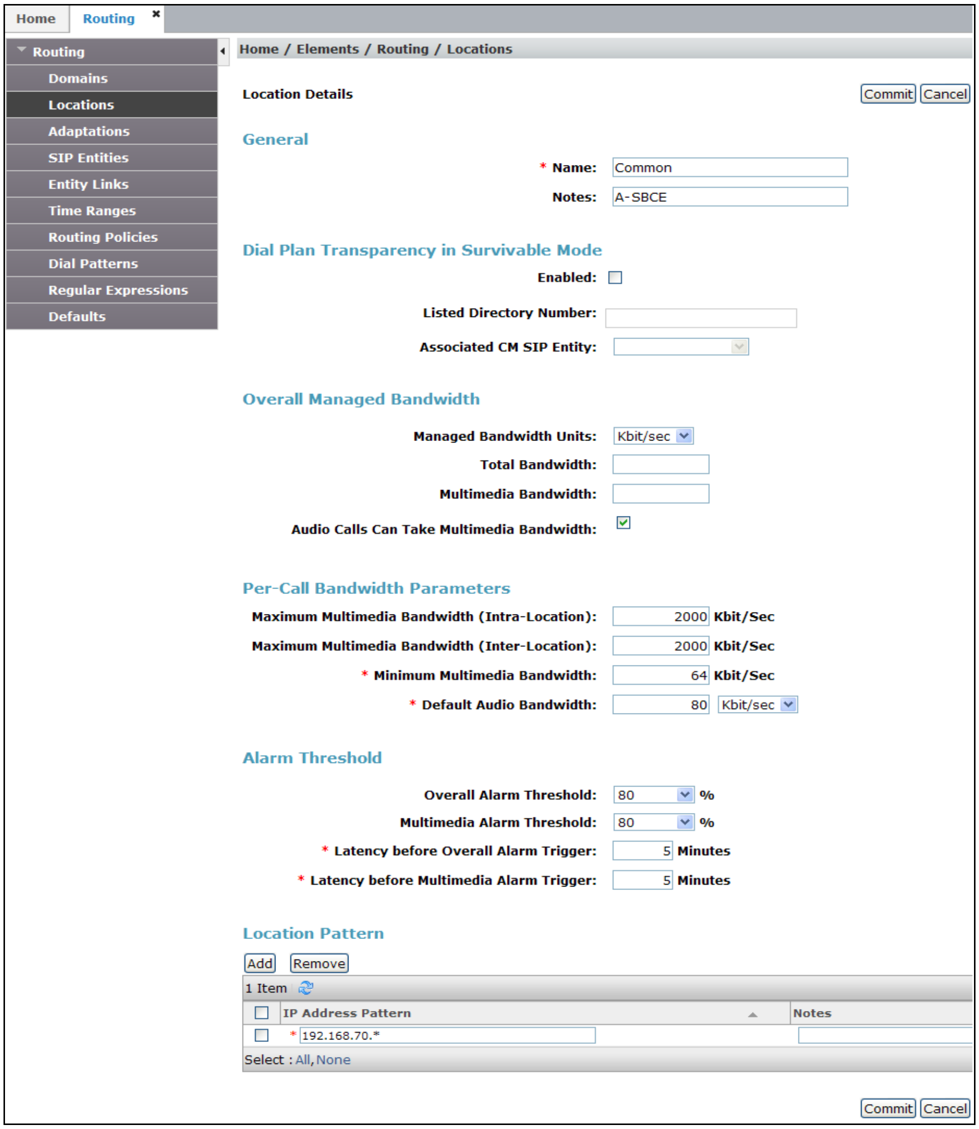
Step 3 - Click **Commit** to save.

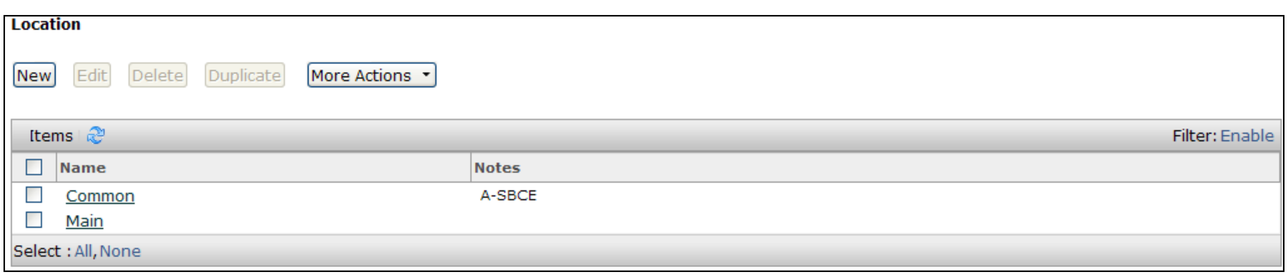


4.2.2. Common Location

Repeat the steps from **Section 4.2.1** with the following changes:

- **Name:** Enter a descriptive name for the Location (e.g., **Common**).
- **IP Address Pattern:** Enter the IP address of the Branch subnet (e.g., **192.168.70.***).





4.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from the AT&T IPFR-EF service, and for converting SIP headers sent between Communication Manager and Avaya Aura® Messaging. In the reference configuration the following adaptations were used.

- Calls from AT&T (**Section 4.3.1**) – The "DigitConversionAdapter" is used for calls to Communication Manager.
  - The AT&T called number digit strings in the Request URI is replaced with their associated Communication Manager extensions/VDNs.
- Calls to AT&T (**Section 4.3.2**) – The "AttAdapter" is specified for calls sent to AT&T.
  - This adapter removes the History-Info header, which is not supported by the IPFR-EF service.
- Calls to Avaya Aura® Messaging from AT&T/PSTN (**Section 4.3.3**)
  - The AT&T called number digit strings in the Request URI are replaced with the Avaya Aura® Messaging pilot number.

4.3.1. Adaptation for Calls to Avaya Aura® Communication Manager

The "DigitConversionAdapter" administered in this section is used to modify incoming AT&T IPFR-EF DNIS digits to their associated Communication Manager extensions.

Note – In the reference configuration, the AT&T IPFR-EF service delivered 10 digit DNIS numbers. Also note that the following entries are based on the DNIS digits delivered in the AT&T Request URI. These digits may not be the same as the dialed DID digits.

Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

Step 2 - In the **Adaptation Details** page, enter:

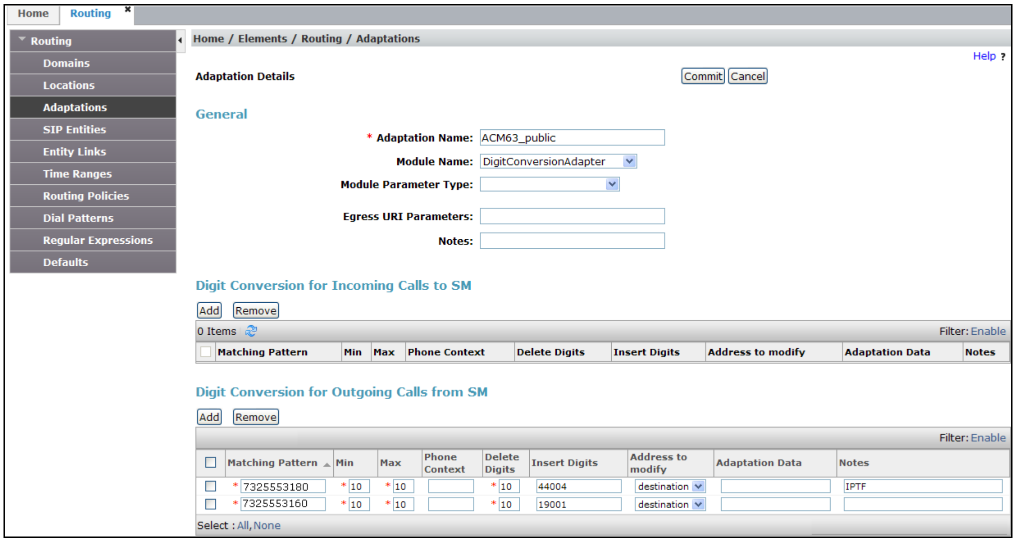
- A descriptive **Name**, (e.g., **ACM63_public**).
- Select **DigitConversionAdapter** fom the **Module Name** drop down menu (if no module name is present, select <click to add module> and enter **DigitConversionAdapter**).

Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* digits from AT&T that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager).

- Example: 7325553180 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Communication Manager Agent Skill2 access VDN 44004.
  - Enter **7325553180** in the **Matching Pattern** column.
  - Enter **10** in the **Min/Max** columns.
  - Enter **10** in the **Delete Digits** column.
  - Enter **44004** in the **Insert Digits** column.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

Step 4 – Repeat **Step 3** for all additional AT&T DNIS numbers.
Step 5 - Click on **Commit**.

Note – No **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.



4.3.2. Adaptation to Remove History-Info Headers

The AT&T network does not support History-Info headers, which Communication Manager sends by default (see **Section 5.8**). The **AttAdapter** administered in this section will automatically remove History-Info headers.

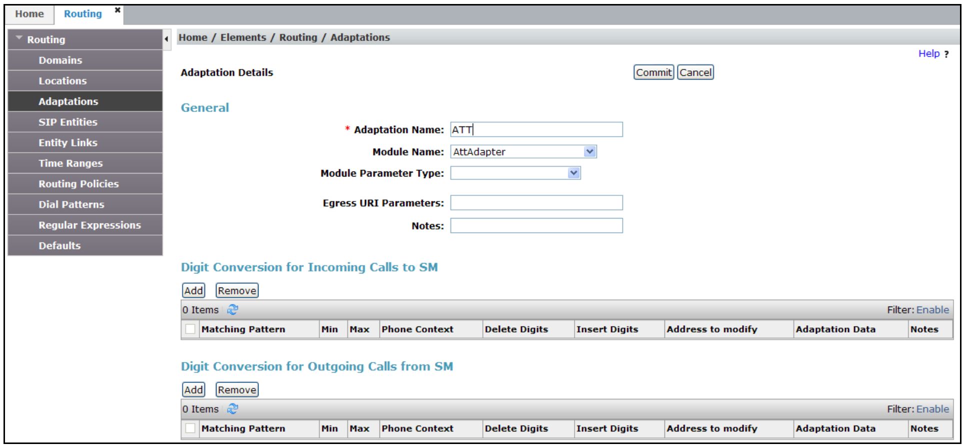
Note – Alternatively, History-Info headers may be removed by Communication Manager (see **Section 5.8**), or by the Avaya SBCE (see **Section 9.4.3**).

Step 1 - Click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).
Step 2 - In the **Adaptation Details** page, enter:

1. A descriptive **Name**, (e.g., **ATT**).
2. Select **AttAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **AttAdapter**).

Step 3 - Click on **Commit**.

Note – As shown in the screen below, no Incoming or Outgoing Digit Conversion was required in the reference configuration.



4.3.3. Adaptation for Direct Calls to Avaya Aura® Messaging

PSTN may dial directly to Avaya Aura® Messaging to retrieve message, using the designated IPFR-EF DID number **7325553170** (see **Section 4.8.3**). These DNIS digits must be converted to the Avaya Aura® Messaging pilot extension, **36000**.

Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

Step 2 - In the **Adaptation Details** page, enter:

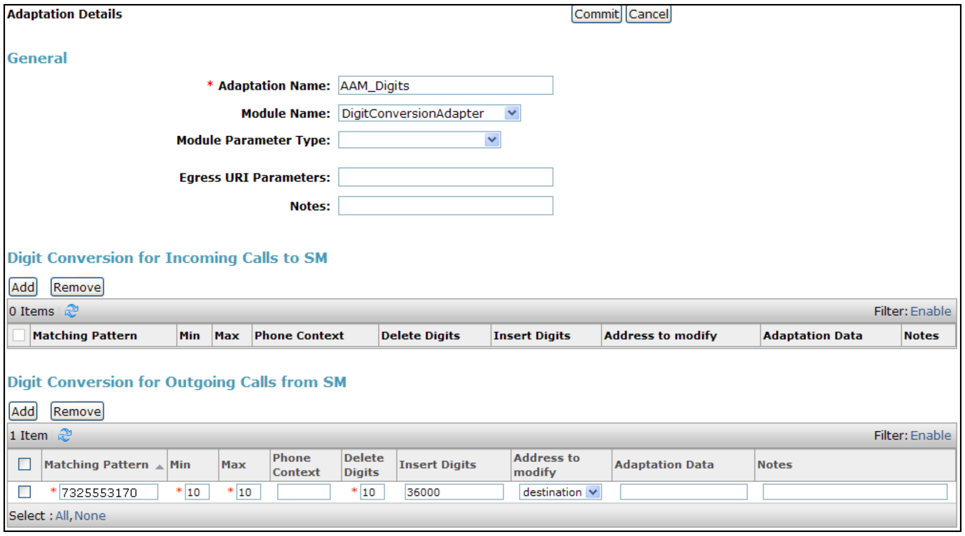
- A descriptive **Name**, (e.g., **AAM_Digits**).
- Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select <click to add module> and enter **DigitConversionAdapter**).

Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* digits from AT&T that need to be replaced with the Avaya Aura® Messaging pilot number before being sent to Avaya Aura® Messaging. Click on **Add**, and enter the following:

- Enter **7325553170** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column.
- Enter **36000** in the **Insert Digits** column.
- Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
- Enter any desired notes.

Step 4 - Click on **Commit**.

Note – As shown in the screen below, no Digit Conversion for Incoming Calls to SM were required in the reference configuration.



4.4. SIP Entities

In this section, SIP Entities are administered for the following SIP network elements:

- Session Manager (**Section 4.4.1**).
- Experience Portal (**Section 4.4.2**). This entity, and its associated Entity Link (using TCP with port 5060), is for calls from AT&T via the Avaya SBCE.
- Communication Manager for AT&T "public" trunk (**Section 4.4.3**) – This entity, and its associated Entity Link (using TCP with port 5062), is for calls from AT&T via the Avaya SBCE. Note that this connection will be associated with the NCR *enabled* trunk on Communication Manager.
- Communication Manager "local" trunk (**Section 4.4.4**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily for traffic between Avaya SIP telephones and Communication Manager.
- Avaya SBCE platform (**Section 4.4.5**) - This entity, and its associated Entity Link (using TCP and port 5060), is for calls from AT&T.
- Avaya Aura® Messaging (**Section 4.4.6**).

4.4.1. Avaya Aura® Session Manager SIP Entity

Step 1 - In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

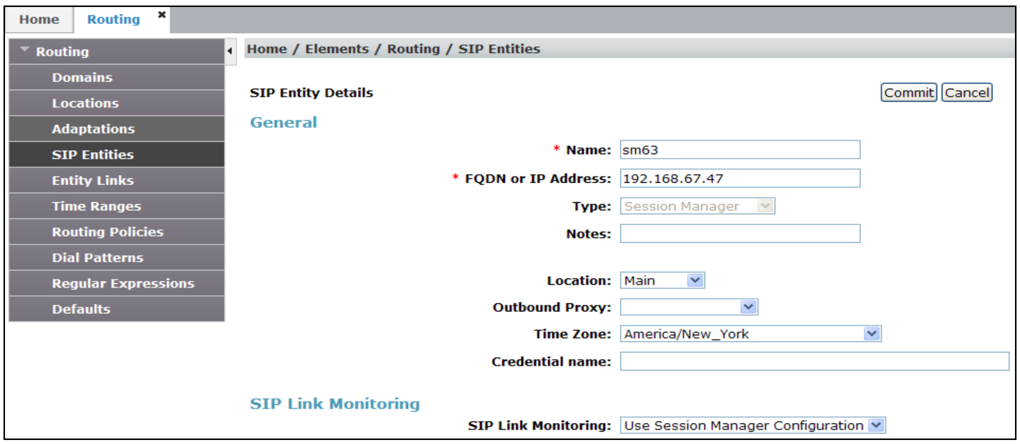
Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name (e.g., **sm63**).
- **FQDN or IP Address –** Enter the IP address of the Main Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **192.168.67.47**).
- **Type –** Verify **Session Manager** is selected.
- **Location** – Select location **Main** (**Section 4.2.1)**.

- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.

Step 3 - In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:

- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.



Step 4 – Scrolling down to the **Port** section of the **SIP Entity Details** page, click on **Add** and provision entries as follow:

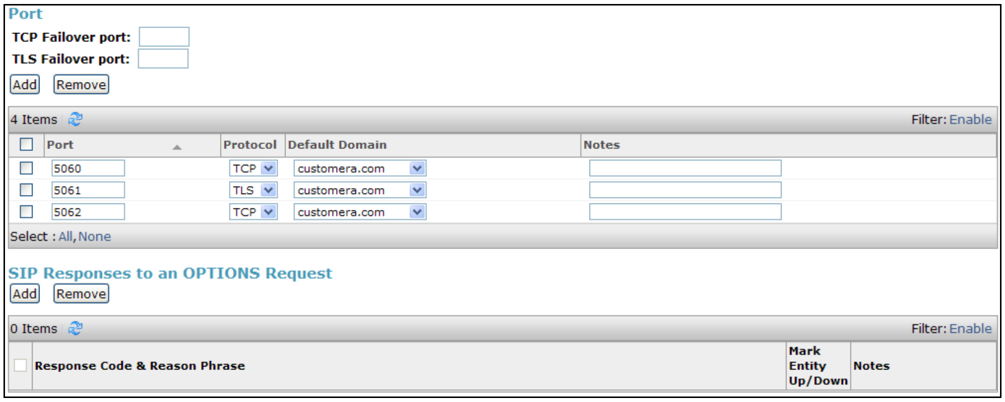
- **Port –** Enter **5060**.
- **Protocol** – Select **TCP**
- **Default Domain –** Select a SIP domain administered in **Section 4.1** (e.g., **customera.com**)

Step 5 - Repeat **Step 4** to provision entries for:

- **5062** for **Port** and **TCP** for **Protocol**.
- **5061** for **Port** and **TLS** for **Protocol**.

Step 6 – Enter any notes as desired and leave all other fields on the page blank/default.
Step 7 - Click on **Commit**.

Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 4.5**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.



4.4.2. Avaya Experience Portal SIP Entity

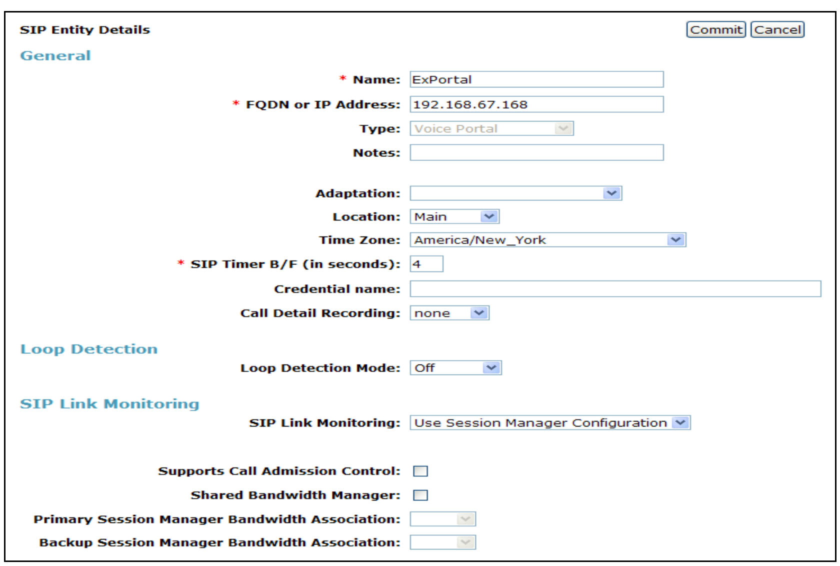
Step 1- In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name (e.g. **ExPortal**).
- **FQDN or IP Address –** Enter the IP address of the Experience Portal application (e.g. **192.168.67.168**, see **Section 3.1**).
- **Type –** Select **Voice Portal**
- **Location** – Select location **Main** (**Section 4.2.1**).
- **Time Zone** – Select the time zone in which Experience Portal resides.
- Note that this Entity has no Adaptation defined.

Step 3 - In the **SIP Monitoring** section of the **SIP Entity Details** page configure as follows:

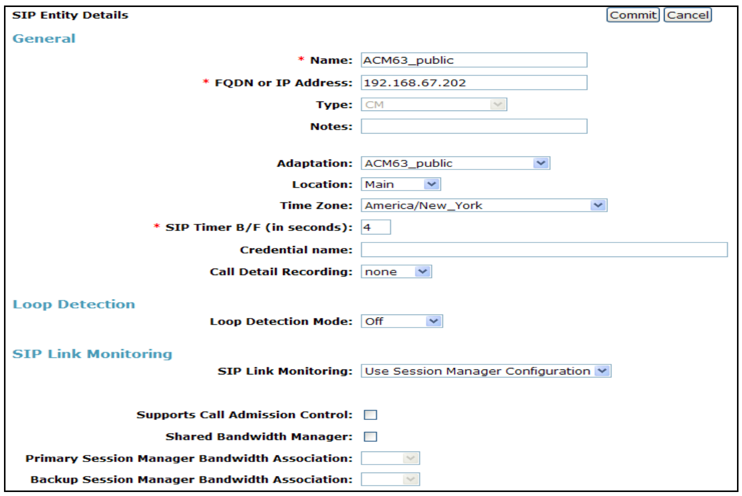
- Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.



4.4.3. Avaya Aura® Communication Manager SIP Entity – Public Trunk

Repeat the steps in **Section 4.4.2**, with the following changes :

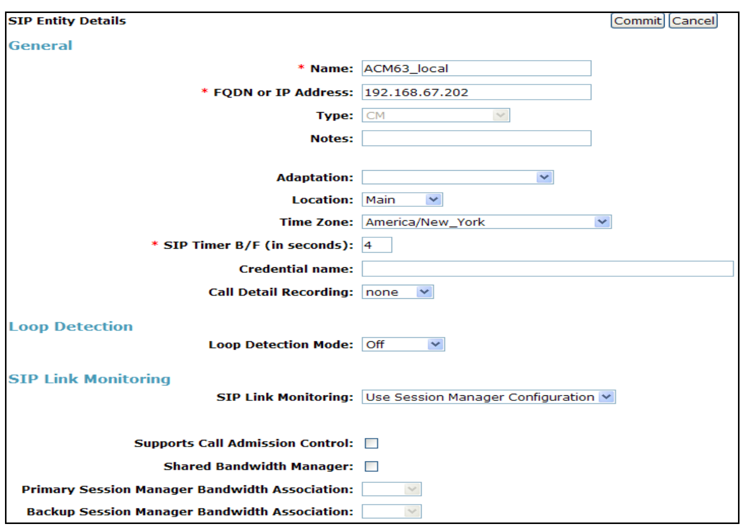
- **Name** – Enter a descriptive name (e.g., **ACM63_public**).
- **FQDN or IP Address** – Enter the IP address of the Main Communication Manager Processor Ethernet (procr) described in **Section 5.5** (e.g. **192.168.67.202**, see **Section 3.1**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **ACM63_public** administered in **Section 4.3.1**.



4.4.4. Avaya Aura® Communication Manager SIP Entity – Local Trunk

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 4.4.2** with the following changes:

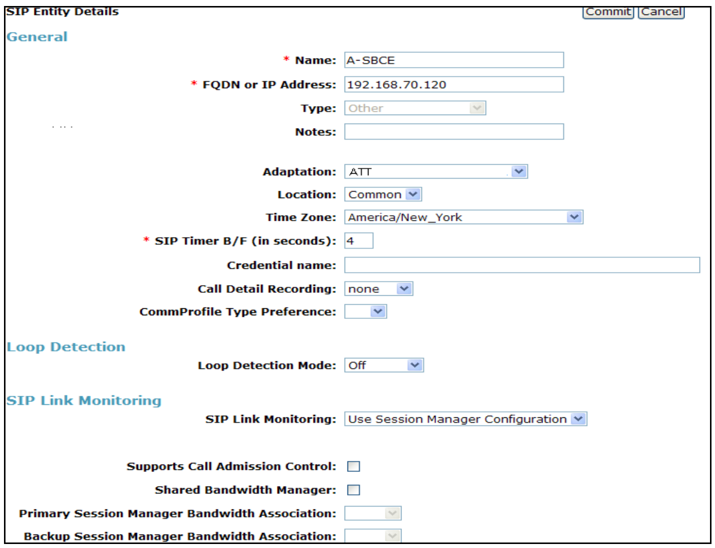
- **Name** – Enter a descriptive name (e.g., A**CM63_local**).
- Note that this Entity has no Adaptation defined.



4.4.5. Avaya Session Border Controller for Enterprise SIP Entity

To configure the Avaya SBCE SIP Entity, repeat the steps in **Section 4.4.4** with the following changes:

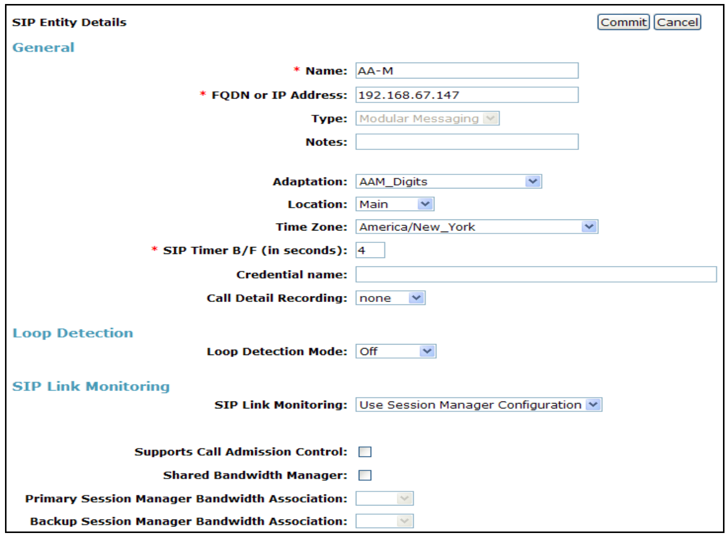
- **Name –** Enter a descriptive name (e.g., **A-SBCE**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **192.168.70.120**, see **Section 9.5.1**).
- **Type –** Verify **Other** is selected.
- **Adaptations –** Select Adaptation **ATT** (**Section 4.3.2**).
- **Location** – Select location **Common** (**Section 4.2.2)**.



4.4.6. Avaya Aura® Messaging SIP Entity

To configure the Avaya Aura® Messaging Entity, repeat the steps in **Section 4.4.2** with the following changes:

- **Name –** Enter a descriptive name (e.g., **AA-M**).
- **FQDN or IP Address –** Enter the IP address of Avaya Aura® Messaging (e.g., **192.168.67.147**, see **Section 3.1**)
- **Type –** Select **Modular Messaging**.
- **Adaptations –** Select Adaptation **AA-M_Digits** (**Section 4.3.3**).
- **Location** – Select location **Main** (**Section 4.2.1)**.



4.5. Entity Links

Note – See the note in **Section 3** regarding transport protocols used in the reference configuration.

In this section, Entity Links are administered for the following connections:

- Session Manager to Experience Portal trunk (**Section 4.5.1**).
- Session Manager to the Communication Manager Public trunk (**Section 4.5.2**).
- Session Manager to the Communication Manager Local trunk (**Section 4.5.3**).
- Session Manager to the Avaya SBCE (**Section 4.5.4**).
- Session Manager to Avaya Aura® Messaging (**Section 4.5.5**).

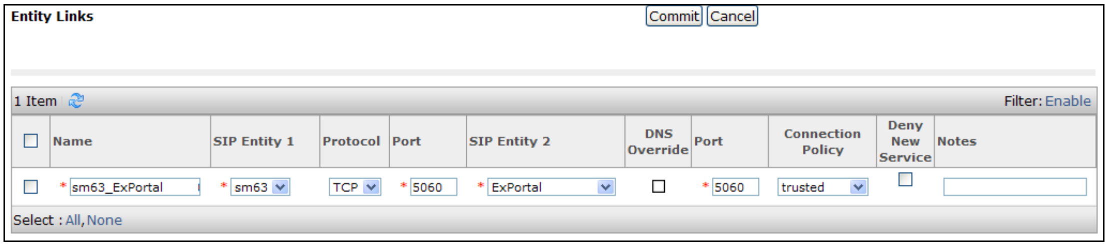
Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 4.4**.

4.5.1. Avaya Aura® Session Manager Entity Link to Avaya Experience Portal

Step 1 - In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).
Step 2 - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Experience Portal (e.g., **sm63_ExPortal**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 4.4.1** for Session Manager (e.g., **sm63**).
- **SIP Entity 1 Port** – Enter **5060**.
- **Protocol** – Select **TCP**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 4.4.2** for the Experience Portal entity (e.g., **ExPortal**).
- **SIP Entity 2 Port** - Enter **5060**.
- **Connection Policy** – Select **Trusted**.

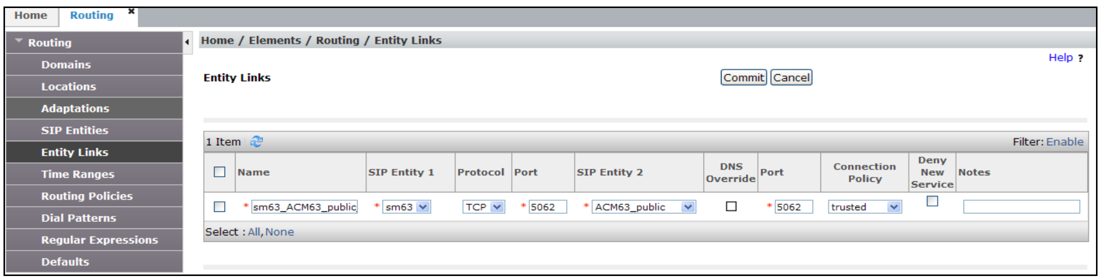
Step 3 - Click on **Commit**.



4.5.2. Avaya Aura® Session Manager Entity Link to Avaya Aura® Communication Manager – Public Trunk

Repeat the steps in **Section 4.5.1** with the following changes:

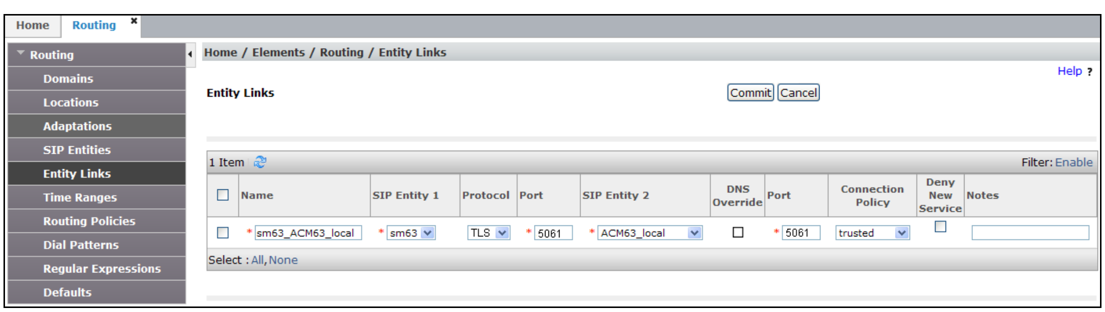
- **Name** – Enter a descriptive name for this link to the Communication Manager "public" trunk (e.g., **sm63_ACM63_public**).
- **SIP Entity 1 Port** and **SIP Entity 2 Port** – Enter **5062**
- **SIP Entity 2** – Select the SIP Entity administered in **Section 4.4.3** for the Communication Manager public entity (e.g., **ACM63_public**).



4.5.3. Avaya Aura® Session Manager Entity Link to Avaya Aura® Communication Manager – Local Trunk

To configure this Entity Link, repeat the steps in **Section 4.5.1**, with the following changes:

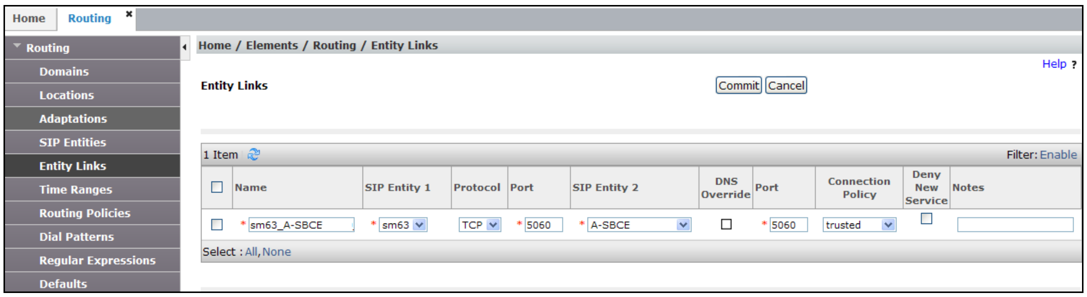
- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **sm63_ACM63_local**).
- **SIP Entity 1 Port** and **SIP Entity 2 Port** – Enter **5061**.
- **Protocol** – Select **TLS** (see **Section 3**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 4.4.4** for the Communication Manager local entity (e.g., **ACM63_local**).



4.5.4. Avaya Aura® Session Manager Entity Link for the AT&T IP Flexible Reach-Enhanced Features Service via the Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 4.5.1**, with the following changes:

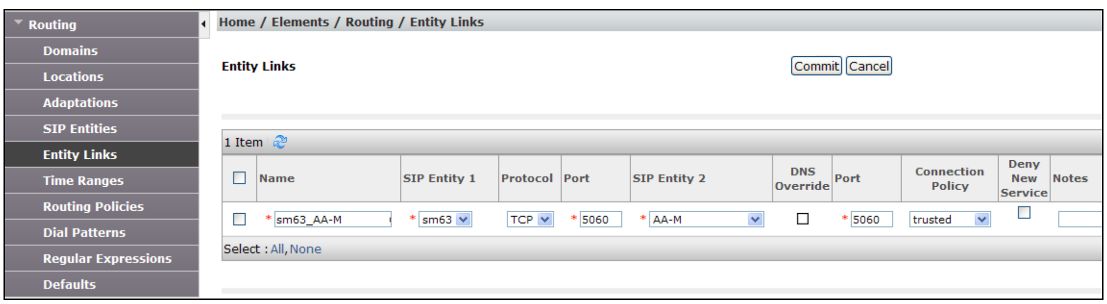
- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sm63_A-SBCE**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 4.4.5** for the Avaya SBCE (e.g., **A-SBCE**).



4.5.5. Avaya Aura® Session Manager Entity Link for Avaya Aura® Messaging

To configure this Entity Link, repeat the steps in **Section 4.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sm63_AA-M**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 4.4.6** for the Communication Manager public entity (e.g., **AA-M**).



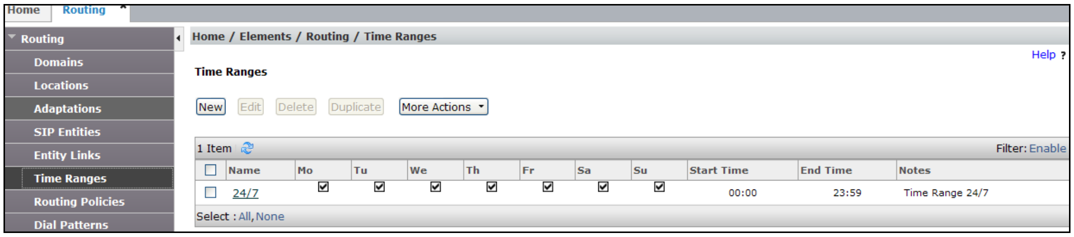
4.6. Time Ranges

Step 1 - In the left pane under **Routing**, click on **Time Ranges**. In the **Time Ranges** page click on **New** (not shown).

Step 2 - Continuing in the **Time Ranges** page, enter a descriptive **Name**, check the checkbox(s) for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

Step 3 - Click on **Commit**.

Step 4 - Repeat **Steps 1 – 3** to provision additional time ranges.



4.7. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Experience Portal from AT&T (**Section 4.7.1**).
- Inbound calls to the Communication Manager "public" trunk. The majority of these calls are generated by the Avaya SBCE, after receiving SIP Refer messages from Experience Portal (**Section 4.7.2**).
- Inbound calls to the Communication Manager "local" trunk. The majority of these calls are to/from Communication Manager SIP endpoints (**Section 4.7.3**).
- Inbound calls to Avaya Aura® Messaging (**Section 4.7.4**).
- Outbound calls from Experience Portal/Proactive Outreach Manager to AT&T (**Section 4.7.5**).

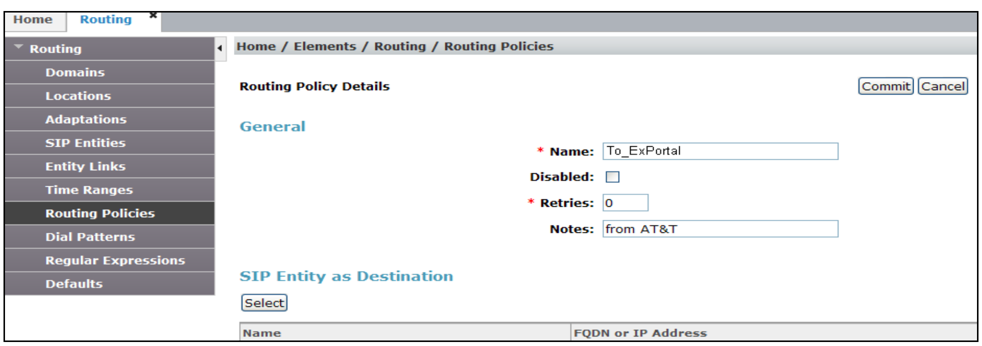
4.7.1. Routing Policy for AT&T Routing to Avaya Experience Portal

This Routing Policy is used for inbound calls from AT&T.

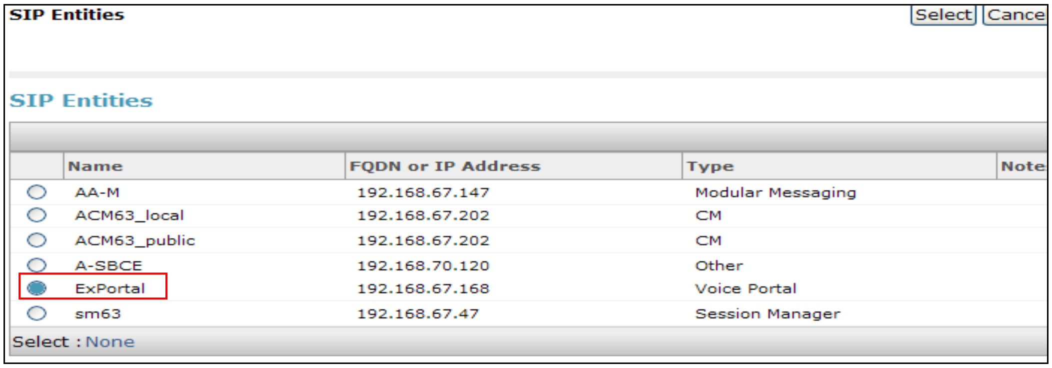
Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Experience Portal (e.g., **To_ExPortal**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Step 3 - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.



Step 4 - In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.4.2** for the Experience Portal SIP Entity (**ExPortal**), and click on **Select**.



Step 5 - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on **Add**.

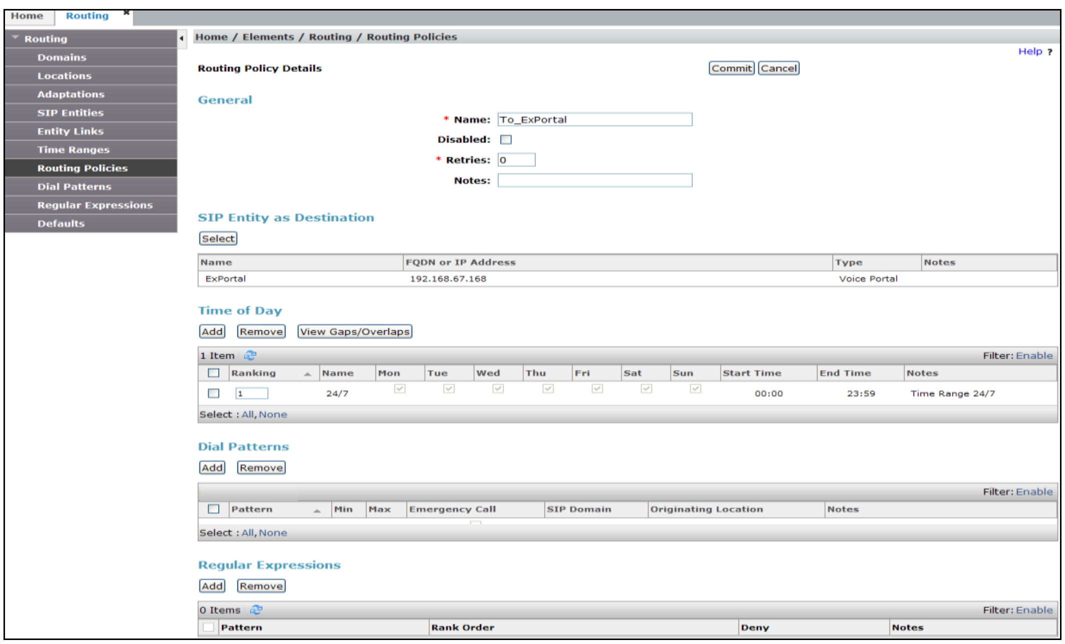
Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 4.6**, and click on **Select**.

Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, if multiple Time Ranges were selected, user may enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on **Commit**.

Step 8 - No **Regular Expressions** were used in the reference configuration.

Step 9 - Click on **Commit**.

Note that once the **Dial Patterns** are defined (**Section 4.8**) they will appear in the **Dial Pattern** section of this form.

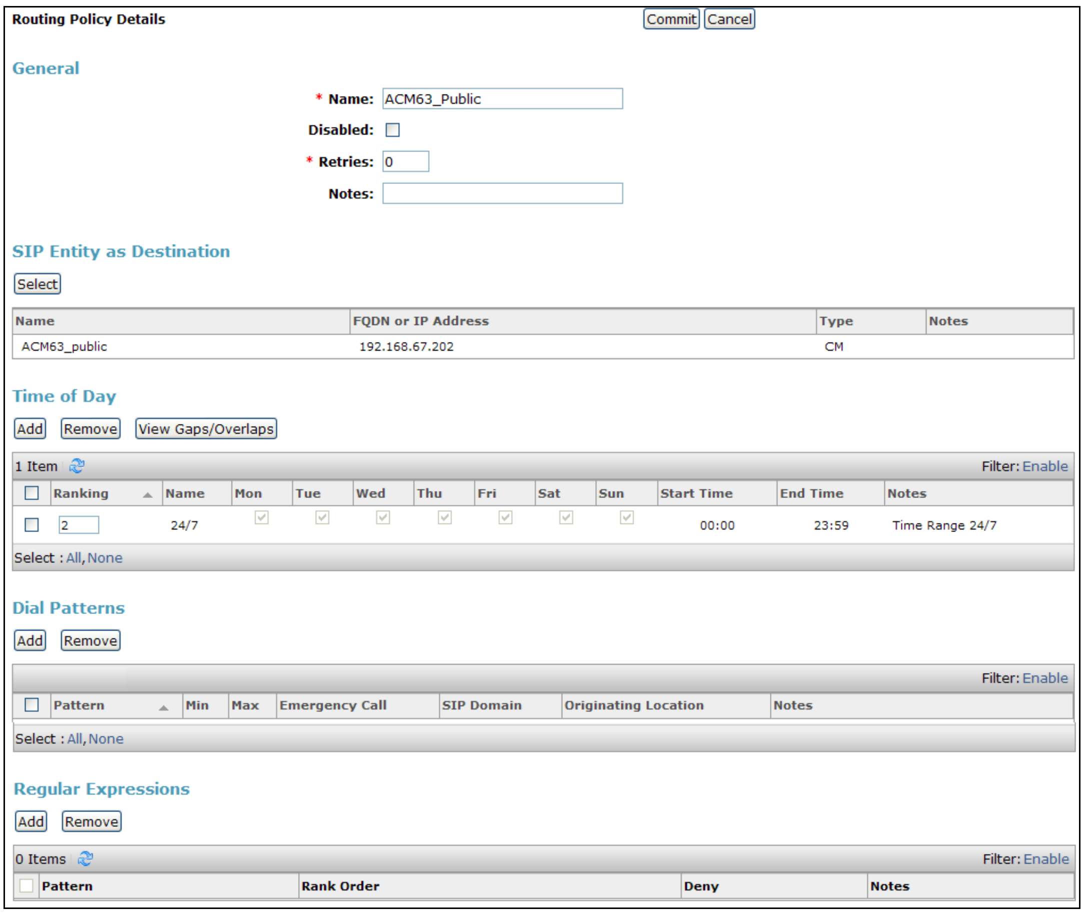


4.7.2. Routing Policy to Avaya Aura® Communication Manager Public Trunk

This Routing Policy is used to direct calls from Experience Portal to Communication Manager "public" trunk (via the Avaya SBCE). The majority of these calls are generated by the Avaya SBCE, after receiving SIP Refer messages from Experience Portal. Repeat the steps in **Section 4.7.1** with the following changes:

- Enter a descriptive **Name** (e.g. **ACM63_Public**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.4.3** for the Communication Manager "public" trunk (e.g. **ACM63_Public**).
- In the **Time of Day** section, change the ranking number to **1**.

Note that once the **Dial Patterns** are defined (**Section 4.8**), they will appear in the **Dial Pattern** section.

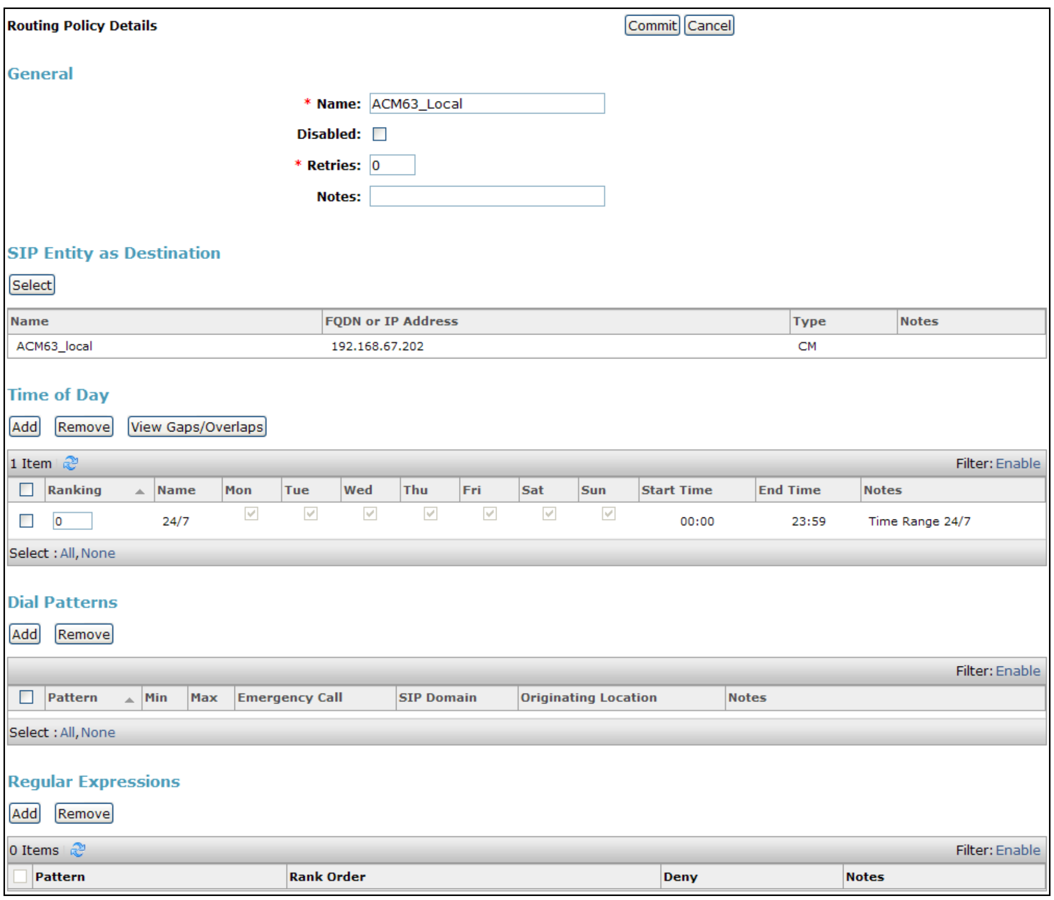


4.7.3. Routing Policy to Avaya Aura® Communication Manager Local Trunk

This Routing Policy is used primarily to direct calls to the Communication Manager "private" trunk. The majority of these calls are to/from Avaya SIP endpoints. Repeat the steps in **Section 4.7.1** with the following changes:

- Enter a descriptive **Name** (e.g. **ACM63_local**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.4.4** for the Communication Manager "local" trunk (e.g. **ACM63_local**).
- In the **Time of Day** section, change the ranking number to **1**.

Note that once the **Dial Patterns** are defined (**Section 4.8**), they will appear in the **Dial Pattern** section.

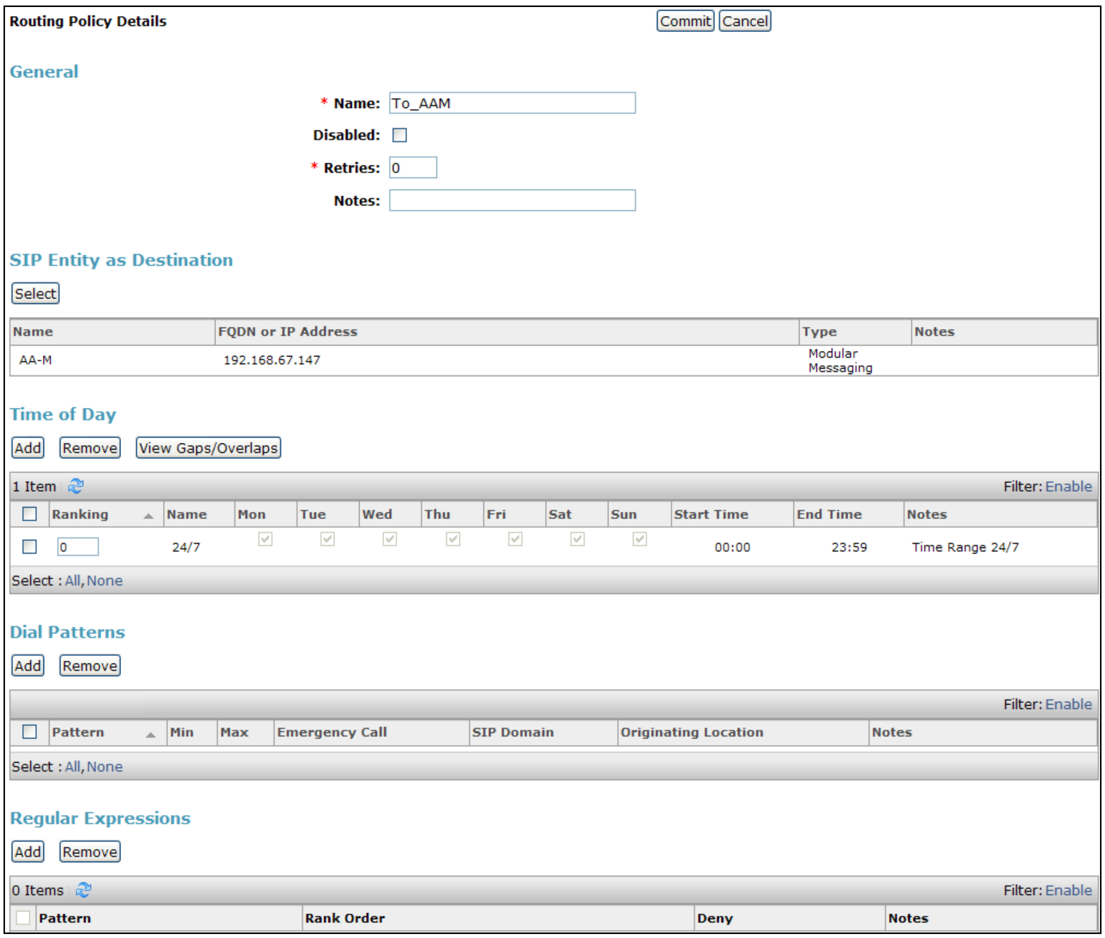


4.7.4. Routing Policy to Avaya Aura® Messaging

This Routing Policy is used for PSTN direct calls to Avaya Aura® Messaging Repeat the steps in **Section 4.7.1** with the following changes:

- Enter a descriptive **Name** (e.g. **To_AAM**) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.4.6** for Avaya Aura® Messaging (e.g. **AA-M**).
- In the **Time of Day** section, change the ranking number to **1**.

Note that once the **Dial Patterns** are defined (**Section 4.8**), they will appear in the **Dial Pattern** section.

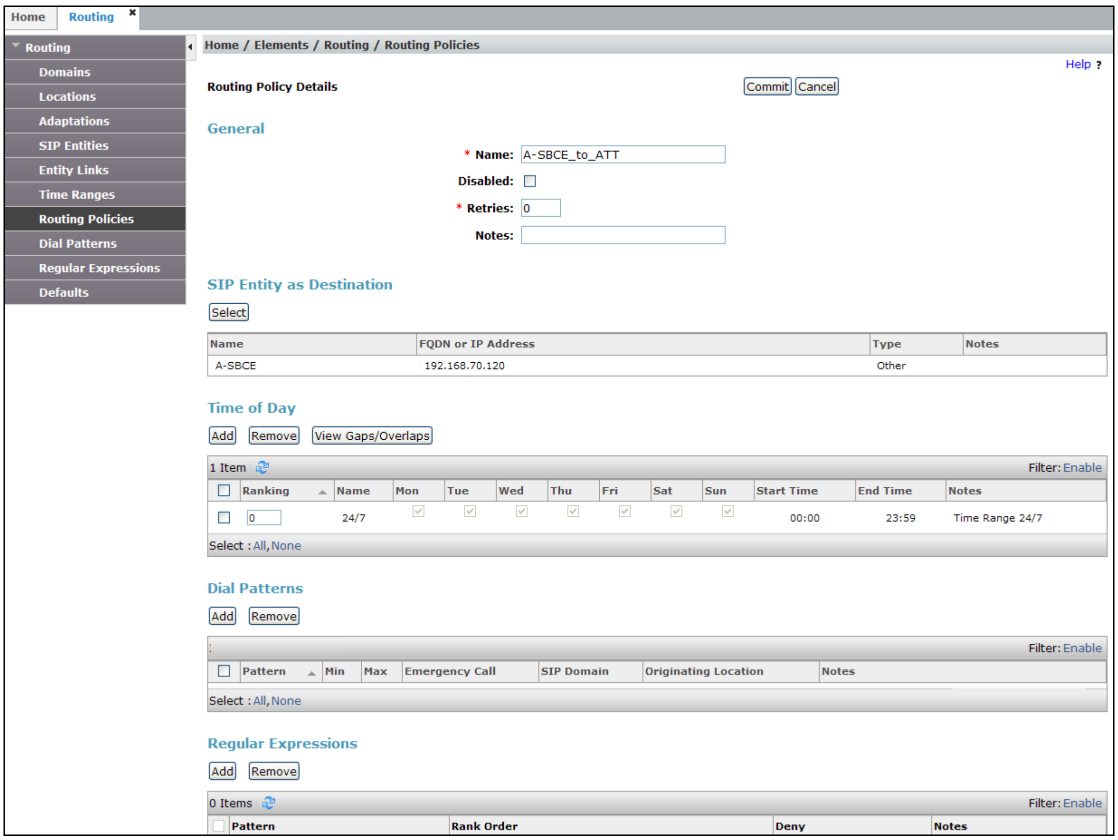


4.7.5. Routing Policy for Experience Portal/Proactive Outreach Manager to AT&T

This Routing Policy is used for Experience Portal/Proactive Outreach Manager outbound calls to AT&T. Repeat the steps in **Section 4.7.1** with the following changes:

- Enter a descriptive **Name** (e.g. **A-SBCE_to_ATT**) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 4.4.5** for the Avaya SBCE (e.g. **A-SBCE**).
- In the **Time of Day** section, change the ranking number to **1**.

Note that once the **Dial Patterns** are defined (**Section 4.8**), they will appear in the **Dial Pattern** section.



4.8. Dial Patterns

In this section, Dial Patterns are administered matching the following calls:

- Inbound PSTN calls to Experience Portal (**Section 4.8.1**).
- Calls from Experience Portal to Communication Manager Agent skills/extensions (**Section 4.8.2**). Note that these calls are generated by the Avaya SBCE, after receiving SIP Refer messages from Experience Portal.
- Inbound PSTN calls direct to Avaya Aura® Messaging for message retrieval (**Section 4.8.3**).

- Access to the Communication Manager local SIP trunk for SIP phone extensions, as well as for station MWI (**Section 4.8.4**).
- Outbound calls from Experience Portal/Proactive Outreach Manager to AT&T (**Section 4.8.5**).

4.8.1. Matching Inbound PSTN Calls to Avaya Experience Portal

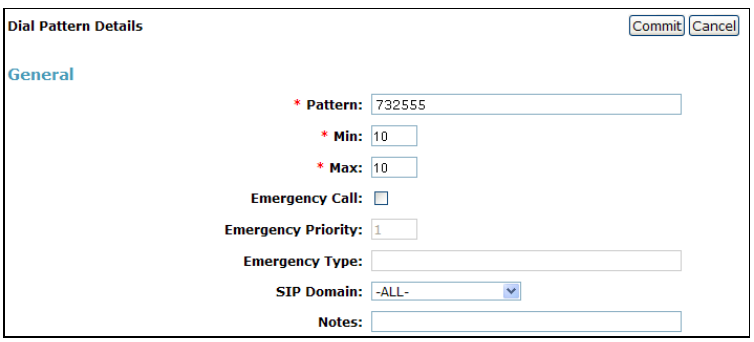
In the reference configuration, inbound calls from AT&T used 10 digits in the SIP Request URI. These digit strings began with **732555**.

> **Note** – Be sure to match on the DNIS digit string specified in the AT&T Request URI, not the DID digit string that is dialed. They may be different.

Step 1 - In the left pane under **Routing**, click on **Dial Patterns**. In the **Dial Patterns** page click on **New** (not shown).

Step 2 - In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – To match the digit patterns sent by AT&T, enter **732555**. Experience portal will map these digit strings to the appropriate applications (see **Section 6.5**).
- **Min** - Enter **10**
- **Max** – Enter **10**.
- **SIP Domain** – Select **-ALL-**, to select all of the administered SIP Domains.

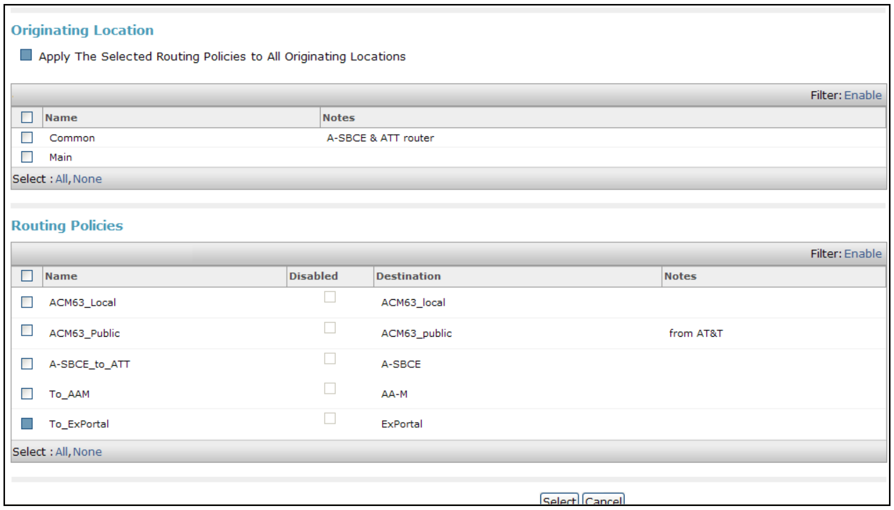


Step 3 – Scrolling down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on **Add**.

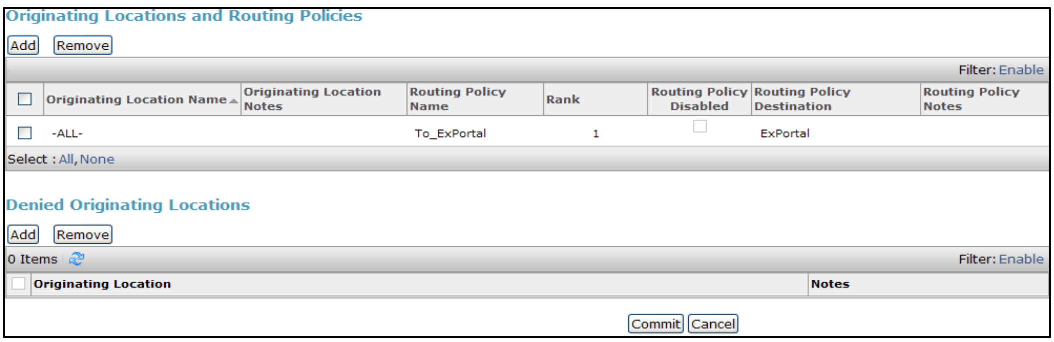
Step 4 - In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to all Locations).

Step 5 - In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to Experience Portal in **Section 4.7.1** (e.g., **To_ExPortal**).

Step 6 – Click on **Select**.



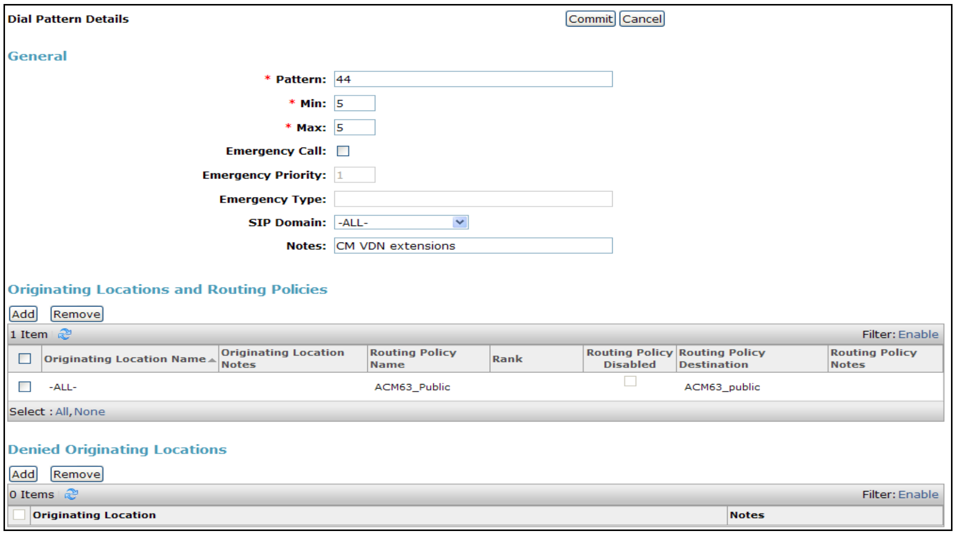
Step 7 - Returning to the Dial Pattern Details page click on **Commit**.



4.8.2. Matching Calls From Experience Portal to Avaya Aura® Communication Manager

Customer interactions with Experience Portal can result in subsequent connections to Communication Manager Agents, (these calls are generated by the Avaya SBCE, to Communication Manager, after the Avaya SBCE receives SIP Refer messages from Experience Portal). In the reference configuration, Communication Manager is provisioned with 5 digit Voice Directory Numbers (VDNs), using the format 44xxx. These VDNs provide connections to the Agents (see **Section 5.14**). To define the VDN patterns, follow the steps shown in **Section 4.8.1**, with the following changes:

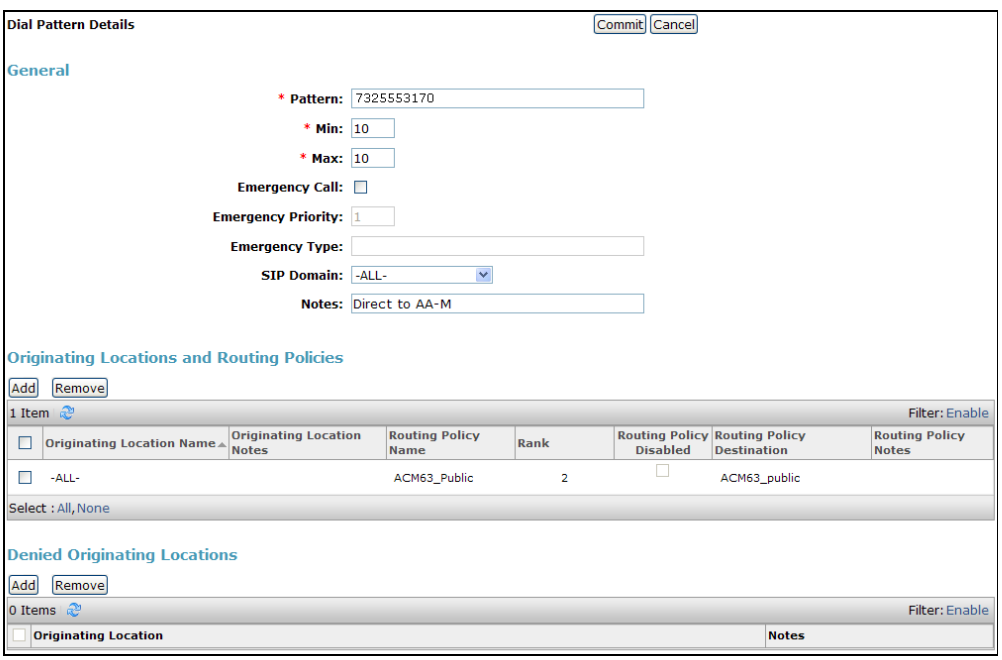
- **Pattern** –Enter **44**.
- **Min** and **Max** – Enter **5**.
- **Originating Locations** – Select **All.**
- **Routing Policy** – Select the policy for the Communication Manager public trunk defined in **Section 4.7.2** (e.g., **ACM63_Public**).
- Click on **Commit.**



4.8.3. Matching PSTN Inbound Calls to Avaya Aura® Messaging

PSTN callers may dial directly to Avaya Aura® Messaging to retrieve messages. a designated AT&T IPFR-EF DNIS number **7325553170**, follow the steps in **Section 4.8.1**, with the following changes:

- **Pattern** –Enter **7325553170**.
- **Min** and **Max –** Enter **10**.
- **Routing Policy Name** – Select **ACM63_Public**.

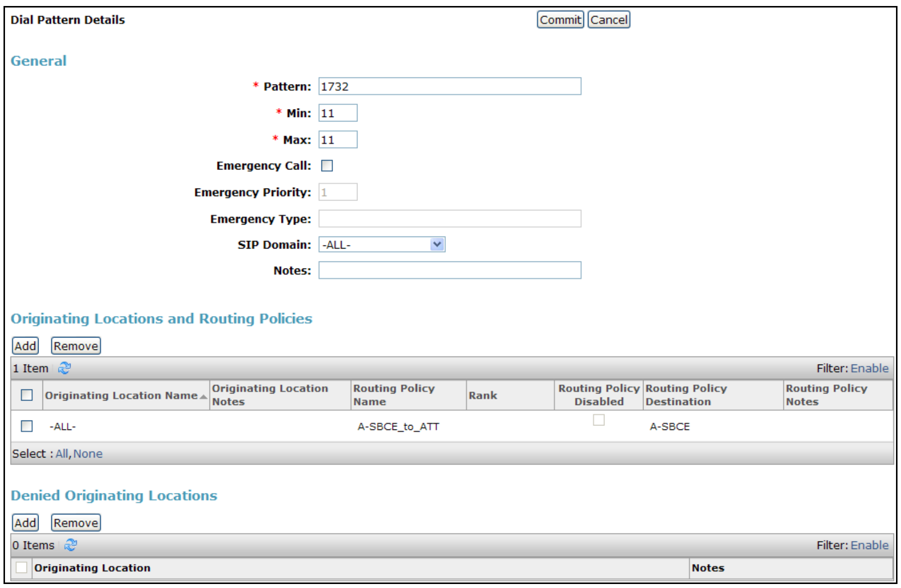


Note – The digit string **7325553170** is converted to the Avaya Aura® Messaging Pilot extension **36000** as described in **Section 4.3.3**.

4.8.4. Matching Experience Portal/Proactive Outreach Manager calls to AT&T.

Proactive Outreach Manager will place calls out to PSTN via the Avaya SBCE. Follow the steps shown in **Section 4.8.1**, with the following changes:

- **Pattern** – Enter **1732**.
- **Min and Max** – Enter **11**.
- **Routing Policy Name** – Select **A-SBCE_to_ATT**.



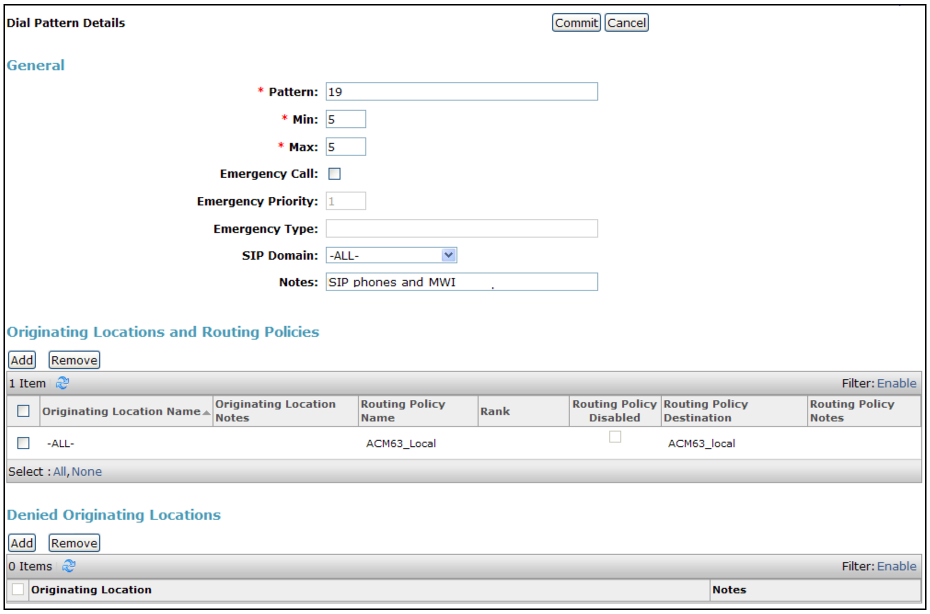
4.8.5. Matching Avaya Aura® Communication Manager SIP Endpoint Extensions and Message Wait Indicator (MWI)

As described in **Section 4.4**, Communication Manager SIP endpoints use the "local" SIP trunk for call processing. In the reference configuration, Communication Manager SIP endpoints used the extension pattern **19xxx**.

Note – This pattern will also process Message Wait Indicator (MWI) signaling from Avaya Aura® Messaging for Communication Manager.

Follow the steps shown in **Section 4.8.1**, with the following changes:

- **Pattern** – Enter **19**.
- **Min and Max** – Enter **5**.
- **Routing Policy Name** – Select **ACM63_local**.



5. Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult documents **[7 & 8]** for further details.

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these application notes. Other parameter values may or may not match based on local configurations.

5.1. System-Parameters Customer-Options

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes.

NOTE - For any required features that cannot be enabled in the steps that follow, contact an authorized Avaya account representative to obtain the necessary licenses.

Step 1 - Enter the **display system-parameters customer-options** command. On **Page 2** of the form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

```
display system-parameters customer-options                    Page   2 of  11
                                OPTIONAL FEATURES
IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 4
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                   Maximum Video Capable IP Softphones: 18000 5
                       Maximum Administered SIP Trunks: 24000 30
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
        (NOTE: You must logoff & login to effect the permission changes.)
```

Step 2 - On **Page 3** of the form, verify that the **ARS** feature is enabled.

```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES
    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y              Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                    DCS (Basic)? y
          ASAI Link Core Capabilities? n              DCS Call Coverage? y
          ASAI Link Plus Capabilities? n             DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                        DS1 MSP? y
                                 ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

Step 3 - On **Page 4** of the form, verify that the **IP Stations?**, **IP Trunks?**, and **ISDN/SIP Network Call Redirection?** fields are 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? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                           ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                  ISDN-PRI? y
              ESS Administration? y                Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                      Malicious Call Trace? y
     External Device Alarm Admin? y                  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? y                  Multifrequency Signaling? y
      Global Call Classification? y          Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y       Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y                Multimedia IP SIP Trunking? y
                      IP Trunks? y

           IP Attendant Consoles? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. System-Parameters Features

Step 1 - Enter the **display system-parameters features** command. On **Page 1** of the form, verify that the **Trunk-to-Trunk Transfer** is set to **all**.

```
change system-parameters features                             Page   1 of  20
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
              Music (or Silence) on Transferred Trunk Calls? no
              DID/Tie/ISDN/SIP Intercept Treatment: attendant
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n
             Abbreviated Dial Programming by Assigned Lists? n
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

5.3. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. The following dial plan was used in the reference configuration.

Step 1 - Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings used in the reference configuration:

- 3-digit facilities access codes (indicated with a **Call Type** of **fac**) beginning with ***** and **#** for Feature Access Code (FAC) access.
- 5-digit extensions with a **Call Type** of **ext** beginning with:
  - The digit **1** for Communication Manager station extensions.
  - The digit **3** for the Avaya Aura® Messaging Pilot Extension (36000).
  - The digit **4** for Communication Manager Agent or VDN extensions.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code **6xx** for SIP Trunk Access Codes (TAC). See the trunk forms in **Section 5.8**.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**), e.g., access code **8** for Automatic Alternate Routing dialing, see **Section 5.11**.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**), e.g., access code **9** for outbound Automatic Route Selection dialing, see **Section 5.10**.

```
change dialplan analysis                                         Page   1 of  12
                            DIAL PLAN ANALYSIS TABLE

                                   Location: all           Percent Full: 2
    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   1            5   ext
   3            5   ext
   4            5   ext
   6            3   dac
   8            1   fac
   9            1   fac
   *            3   fac
   #            3   fac
```

5.4. IP Node Names

Node names define IP addresses to various Avaya components in the enterprise. Note that the Processor Ethernet (procr) node is automatically added during the installation process.

Step 1 - Enter the **change node-names ip** command, and add the following:

- Avaya SBCE private network interface (e.g., **A-SBCE** and **192.168.70.120**).
- Session Manager SIP signaling interface (e.g., **SM63** and **192.168.67.47**).
- Note that the Communication Manager procr name and IP address are entered during installation.

```
change node-names ip                                              Page   1 of 2
                                  IP NODE NAMES
    Name              IP Address
A-SBCE              192.168.70.120
SM63                192.168.67.47
default             0.0.0.0
procr               192.168.67.202
procr6              ::
```

5.5. IP Interface for procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters defined during installation. The following screen shows the parameters used in the reference configuration.

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** fields are set to **y**.
- In the reference configuration the procr is assigned to **Network Region: 1**.
- The default values are used for the remaining parameters.

```
display ip-interface procr                                        Page   1 of   2
                                  IP INTERFACES
                  Type: PROCR
                                                          Target socket load: 1700
      Enable Interface? y                               Allow H.323 Endpoints? y
                                                         Allow H.248 Gateways? y
        Network Region: 1                                 Gatekeeper Priority: 5
                                 IPV4 PARAMETERS
             Node Name: procr                     IP Address: 192.168.67.202
           Subnet Mask: /24
```

5.6. IP Network Regions

Network Regions are used to group various Communication Manager resources such as codecs, UDP port ranges, and inter-region communication. In the reference configuration, three network regions are used, one for the CPE (region 1), and one for the AT&T SIP trunk access (region 2).

5.6.1. IP Network Region 1 – CPE Region

Step 1 – Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region **1**). This IP network region will be used to represent the local CPE. Populate the form with the following values:

- Enter a descriptive name (e.g., **Main**).
- Enter the enterprise domain (e.g., **customera.com**) in the **Authoritative Domain** field (see **Section 4.1**).
- Enter **1** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.

- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min**: – Set to **16384** (**AT&T requirement**).
- **UDP Port Max**: – Set to **32767** (**AT&T requirement**).

```
change ip-network-region 1                                          Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: customera.com
    Name: Main                    Stub Network Region: n
MEDIA PARAMETERS                  Intra-region IP-IP Direct Audio: yes
      Codec Set: 1                Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                       IP Audio Hairpinning? n
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Step 2 - On **page 2** of the form:

- Verify that RTCP Reporting Enabled is set to **y**.

```
change ip-network-region 1                                       Page   2 of  20
                               IP NETWORK REGION
 RTCP Reporting Enabled? y
 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? y
```

Step 3 - On **page 4** of the form:

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **2** in the **dst rgn** column, enter **2** for the codec set (this means region 1 is permitted to talk to region 2 and it will use codec set 2 to do so). The **direct WAN** and **Units** columns will self populate with **y** and **No Limit** respectively.
- Let all other values default for this form.

```
change ip-network-region 1                                      Page   4 of  20
Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    1                                                                all
 2    2      y    NoLimit                                            n       t
```

5.6.2. IP Network Region 2 – AT&T Trunk Region

Repeat the steps in **Section 5.6.1** with the following changes:

Step 1 – On **Page 1** of the form (not shown)**:**

- Enter a descriptive name (e.g., **AT&T**).
- Enter **2** for the **Codec Set** parameter.

Step 2 – On **Page 4** of the form:

- Set codec set **2** for **dst rgn 1**.
- Note that **dst rgn 2** is pre-populated with codec set **2** (from page 1 provisioning).

```
change ip-network-region 2                                      Page   4 of  20
 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    c
 rgn  set   WAN  Units    Total Norm  Prio Shr Regions          CAC  R  L    e
 1    2      y    NoLimit                                            n       t
 2    2                                                                all
```

5.7. IP Codec Parameters

5.7.1. Codecs for IP Network Region 1

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls (e.g., **1**).

Step 2 - On **Page 1** of the **ip-codec-set** form, using the following order, set **G.711MU**, **G.729A**, and **G.729B** in the codec list, and set packet interval size to **30**ms.

Note – Both the G.729A and G.729B codec are included here, and in **Section 5.7.2**, to preclude mismatch issues should the use of silence suppression change during the duration of a call.

```
change ip-codec-set 1              IP Codec Set                 Page   1 of   2
    Codec Set: 1
    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n         3        30
 2: G.729A             n         3        30
 3: G.729B             n         3        30
```

Step 3 - On **Page 2** of the ip-codec-set form, set **FAX Mode** to **t.38-standard**.

```
change ip-codec-set 1                IP Codec Set                     Page   2 of   2
                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:  2048:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:  2048:Kbits
                        Mode                 Redundancy
    FAX                 t.38-standard         0
    Modem               off                   0
    TDD/TTY             off                   0
    Clear-channel       n                     0
```

5.7.2. Codecs for IP Network Region 2

Step 1 – Repeat the steps in **Section 5.7.1** for **Page 1** of the ip-codec-set form, however set the codec order as **G.729B, G.729A, and G.711mu**.

```
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.729B             n          3        30
 2: G.729A             n          3        30
 3: G.711MU            n          3        30
```

5.8. SIP Trunks

Two SIP trunks are defined on Communication Manager in the reference configuration. SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group.

- AT&T access – SIP Trunk 2
  - Note that this trunk will use TCP port 5062.
- Avaya SIP telephone access – SIP Trunk 1
  - Note that this trunk will use TCP port 5061

Note –See the note in **Section 3** regarding the use of transport protocols in the CPE.

5.8.1. SIP Trunk for Calls To/From AT&T

This section describes the steps for administering the SIP trunk to Session Manager used for IPFR-EF calls. This trunk corresponds to the **ACM63_Public** SIP Entity defined in **Section 4.4.3**.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **2**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp** (see the note at the beginning of this section).
- Verify that **IMS Enabled?** is set to **n**.

- Verify that **Peer Detection Enabled?** is set to **y**. The systems will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.4** (e.g., **SM63**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5062**.
- **Far-end Network Region** – Set the IP network region to **2**, as set in **Section 5.6.2**.
- **Far-end Domain** – Enter **customera.com**. This is the domain provisioned for Session Manager in **Section 4.1**.
- **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 directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Enable Layer 3 Test** – Set to **y**. This directs Communication Manager to send SIP OPTIONS messages to Session Manager to check link status.
- Use the default parameters on **page 2** of the form (not shown).

```
add signaling-group 2                                           Page   1 of   1
                                SIGNALING GROUP
 Group Number: 1              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
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
   Near-end Node Name: procr                  Far-end Node Name: SM63
 Near-end Listen Port: 5062                 Far-end Listen Port: 5062
                                          Far-end Network Region: 1
Far-end Domain: customera.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
```

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **2**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **ATT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **602**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Step 1** (e.g., **2**).

- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **20**).

```
add trunk-group 2                    TRUNK GROUP                    Page   1 of  21
Group Number: 2                    Group Type: sip            CDR Reports: y
  Group Name: ATT                     COR: 1        TN: 1        TAC: 602
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: public-ntwrk           Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 2
                                                     Number of Members: 20
```

Step 3 - On **Page 2** of the **Trunk Group** form:

- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900**. This entry will actually cause a value of 1800 to be generated in the SIP Session-Expires header pertaining to active call session refresh.

```
add trunk-group 2                                                Page   2 of  21
Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                            Redirect On OPTIM Failure: 6000
            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
 Disconnect Supervision - In? y  Out? y
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

Step 4 - On **Page 3** of the **Trunk Group** form:

- Set N**umbering Format:** to **private**.

Note – Typically a trunk defined as **public-ntwrk** (see **Step 2** above), will use a public numbering format. However, when a public numbering format is selected, Communication Manager will insert a plus sign (+) prefix. When a private numbering format is specified, Communication Manager does not insert the plus prefix. The IPFR-EF service does not require number formats with plus, so private numbering was used for the public trunk.

```
add trunk-group 2                                                Page   3 of  21
                                TRUNK FEATURES
          ACA Assignment? n            Measured: none      Maintenance Tests? y
          Numbering Format: private
                                                  UUI Treatment: service-provider
                                                   Replace Restricted Numbers? y
                                                  Replace Unavailable Numbers? y
                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
```

Step 5 - On **Page 4** of the **Trunk Group** form:

- Verify **Network Call Redirection** and **Send Diversion Header** are set to **y**.
- Set **Telephone Event Payload Type** to **100**, recommended by the IPFR-EF service.

Note –By default, History-Info header is enabled by Communication Manager. As described in **Section 4.3.2**, History Info header is removed by Session Manager. Alternatively, History Info may be disabled here.

```
add trunk-group 2             PROTOCOL VARIATIONS                Page   4 of  21
                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? y
                                   Support Request History? y
                              Telephone Event Payload Type: 100
                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
```

5.8.2. Local SIP Trunk (Avaya SIP Telephone and Avaya Aura® Messaging Access)

This trunk corresponds to the **ACM63_Local** SIP Entity defined in **Section 4.4.4**.
Step 1 – Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **1**), and repeat the steps in **Section 5.8.1** with the following changes:

- **Transport Method** – Set to **tls** (see the note at the beginning of this section).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061**
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 5.6.1**.

```
add signaling-group 1          SIGNALING GROUP                    Page   1 of   1
Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tls
        Q-SIP? n
     IP Video? n          Priority Video? y        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
   Near-end Node Name: procr                 Far-end Node Name: SM63
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1
Far-end Domain: customera.com      Far-end Secondary Node Name:
                                         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
```

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **1**). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 5.8.1** with the following changes:

- **Group Name** – Enter a descriptive name (e.g., **Local**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **601**).
- **Service Type** – Set to **tie**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **1**).

```
add trunk-group 1                                                Page   1 of  21
                                TRUNK GROUP
Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: Local                       COR: 1        TN: 1        TAC: 601
   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: 20
```

Step 3 - On **Page 2** of the **Trunk Group** form:

- Same as **Section 5.8.1**.

Step 4 - On **Page 3** of the **Trunk Group** form:

- Same as **Section 5.8.1**.

Step 5 - On **Page 4** of the **Trunk Group** form:

- Verify **Network Call Redirection** and **Diversion header** are set to **n** (default).
- Use default values for all other settings.

```
add trunk-group 1                                                Page   4 of  21
                              PROTOCOL VARIATIONS
                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? n
                                  Network Call Redirection? n
                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 100
                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

5.9. Private Numbering

In the reference configuration, the private-numbering form is used to:

a) Convert Communication Manager local extensions to IPFR-EF DNIS numbers, (previously identified by AT&T), for inclusion in any SIP headers directed to the IPTF service via the public trunk defined in **Section 5.8.1**.
b) Define local extension ranges to facilitate call coverage to Avaya Aura® Messaging via the local trunk defined in **Section 5.8.2**.

Step 1 - Using the **change private-numbering 0** command, enter the following for the Avaya Aura® Messaging pilot number (for the local trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension assigned to the Avaya Aura® Messaging coverage hunt group defined in **Section 5.14.1** (e.g., **36000**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

Step 2 – Add all Communication Manager local extension patterns (for the local trunk).

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension patterns defined in the Dial Plan in **Section 5.3** (e.g., **1**, **3**, and **4**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

Step 3 – Add a Communication Manager station extension and its corresponding IPTF DNIS number (for the public trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager station extension (e.g., **19001**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **2**).
- **CPN Prefix** – Enter the corresponding IPFR-EF DNIS number (e.g., **7325553160**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 4 – Add a Communication Manager skill VDN extension and its corresponding IPTF DNIS number (for the public trunk):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager station extension (e.g., **44001**).
- **Trk Grp(s)** – Enter the number of the Public trunk group (e.g., **2**).
- **CPN Prefix** – Enter the corresponding IPFR-EF DNIS number (e.g., **7325553180**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 5 – Repeat **Steps 3** and **4** for all IPTF DNIS numbers and their corresponding Communication Manager VDN, station, skill hunt group, or Agent extensions as required.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT
         Ext Ext            Trk         Private           Total
         Len Code           Grp(s)      Prefix            Len
         0   attd                       0                 1
         5   1              1                             5
         5   3              1                             5
         5   4              1                             5
         5   19001          2           7325553160        10
         5   36000          1                             5
         5   44001          2           7325553180        10
```

5.10. Automatic Route Selection (ARS) Dialing

The ARS table is selected based on the caller dialing the ARS access code (e.g., **9**) as defined in **Section 5.3**. The access code is removed and the ARS table matches the remaining outbound dialed digits and sends them to the designated route-pattern (see **Section 5.12**).

Step 1 – For outbound dialing to AT&T enter the following:

- In the **Dialed String** column enter a matching dial pattern (e.g. **1732**). Note that the best match will route first, that is 1732555xxxx will be selected before 17xxxxxxxxx.
- In the **Min** and **Max** columns enter the corresponding matching digit lengths, (e.g. **11** and **11**).
- In the Route Pattern column select a route-pattern to be used for these calls (e.g.**2**).
- In the **Call Type** column enter **hnpa**.

In the example below outbound calls to 1732xxxxxxx and 1800xxxxxxx will be sent to route-pattern 2. In addition, IPFR-EF Call Forward feature access codes (e.g., *7Xyyyzzzxxxx & *9Xyyyzzzxxxx) are defined as well.

```
change ars analysis 1732      ARS DIGIT ANALYSIS TABLE         Page   1 of   2
                                   Location: all            Percent Full: 1
          Dialed            Total     Route     Call   Node  ANI
          String           Min  Max  Pattern    Type   Num   Reqd
    1732                   11   11     2        hnpa         n
    1800                   11   11     2        hnpa         n
    *7                     14   14     2        hnpa         n
    *9                     14   14     2        hnpa         n
```

5.11. Automatic Alternate Routing (AAR) Dialing

AAR is used to direct coverage calls for Avaya Aura® Messaging (**36000**) to the route pattern defined in **Section 5.12**, and to direct calls to Communication Manager SIP telephones (extension pattern **1902x** was used in the reference configuration to identify SIP telephones).

Step 1 – Enter the following:

- **Dialed String**
  - Avaya Aura® Messaging Pilot Number, enter **36000**.
  - In the reference configuration, SIP telephone extension pattern is **1902** (to match 1902x).
- **Min** & **Max** – Enter **5**.

- **Route Pattern** – Enter **1**.
- **Call Type** – Enter **aar**.

Step 2– Repeat **Step 1** for all required local routing.

```
change aar analysis 0          AAR DIGIT ANALYSIS TABLE         Page   1 of   2

                                    Location: all            Percent Full: 1
          Dialed             Total     Route     Call    Node  ANI
          String            Min  Max   Pattern   Type    Num   Reqd
    1902                    5    5      1        aar           n
    36000                   5    5      1        aar           n
```

5.12. Route Patterns

Route Patterns are used to direct calls to the Public SIP trunk (e.g., AT&T access) and to the Local SIP trunk for access to SIP phones and Avaya Aura® Messaging.

5.12.1. Route Pattern for Calls to AT&T

This form defines the local SIP trunk, based on the route-pattern selected by the ARS table in **Section 5.10**. In the reference configuration, route pattern 2 is used.

Step 1 – Enter the **change route-pattern 2** command and enter the following:

- In the **Grp No** column enter **2** for SIP trunk 2 (Public trunk).
- In the **FRL** column enter **0** (zero).
- In the **Numbering Format** column, across from line **1:** enter **unk-unk** (corresponding to the **private** numbering specified in **Section 5.8.1**).

```
change route-pattern 2                                            Page   1 of   3
                          Pattern Number: 2   Pattern Name: ATT Trunk
                             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: 2    0                                                                 n
user
 2:                                                                        n
user
 3:                                                                        n
user
 4:                                                                        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                               unk-unk   next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
```

5.12.2. Route Pattern for Calls to Avaya SIP Telephones

This form specifies the local SIP trunk (e.g., **1**), based on the route-pattern selected by the AAR table in **Section 5.11** (e.g., calls to the Avaya Aura® Messaging pilot number **36000**, or SIP phone extensions **1902x**).

Step 1 – Enter the **change route-pattern 1** command and enter the following:

- In the **Grp No** column enter **1** for SIP trunk 1 (local trunk).
- In the **FRL** column enter **0** (zero).
- In the Numbering Format column, across from line **1:** enter **unk-unk**.

```
change route-pattern 1                                          Page   1 of   3
                   Pattern Number: 1   Pattern Name: Local Trunk
                             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
     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                                unk-unk   next
 2: y y y y y n  n            rest                                          none
 3: y y y y y n  n            rest                                          none
 4: y y y y y n  n            rest                                          none
 5: y y y y y n  n            rest                                          none
```

5.13. Avaya G430 Media Gateway Provisioning

In the reference configuration, a G430 Media Gateways is used. The G430 provides local DSP resources, announcements, Music On Hold, etc. While Media Gateway provisioning is beyond the scope of this document, the configuration used in the reference configuration is included for completeness. See **[9]** for more information on G430 Media Gateway provisioning.

```
display media-gateway 1                                         Page   1 of   2
                                  Type: g430

                    Name: g430
               Serial No: *******             Enable CF? n
            Encrypt Link? n                   Location: 1
          Network Region: 1                   Site Data:
           Recovery Rule: none
              Registered?  y
   FW Version/HW Vintage: 34 .5  .1  /1
        MGP IPV4 Address: 192.168.67.50
   Controller IP Address: 192.168.67.202
```

```
display media-gateway 1                                          Page   2 of   2
                               Type: g430

Slot   Module Type            Name                     DSP Type  FW/HW version
 V1:   MM711                  ANA MM                   MP20      112  0
 V2:   MM712                  DCP MM
 V3:
 V5:                                                   Expansion Type HW version
 V6:
 V7:
 V8:                                                 Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```

5.14. Provisioning for Coverage to Avaya Aura® Messaging

To provide coverage to Avaya Aura® Messaging for Communication Manager extensions, a hunt group is defined using the Avaya Aura® Messaging pilot number (e.g., **36000**), as well as a coverage path that is defined to the various stations.

5.14.1. Hunt Group for Station Coverage to Avaya Aura® Messaging

Step 1 – Enter the command **add hunt-group x**, where **x** is an available hunt group (e.g., **1**), and on **Page 1** of the form enter the following:

- **Group Name** – Enter a descriptive name (e.g., **AAM**).
- **Group Extension** – Enter an available extension (e.g., **36000**). Note that the hunt group extension need *not* be the same as the Avaya Aura® Messaging pilot number.
- **ISDN/SIP Caller Display** – Enter **mbr-name**.
- Let all other fields default.

```
add hunt-group 1                                              Page   1 of  60
                                  HUNT GROUP
            Group Number: 1                                   ACD? n
              Group Name: AAM                               Queue? n
         Group Extension: 36000                            Vector? n
              Group Type: ucd-mia                   Coverage Path:
                      TN: 1          Night Service Destination:
                     COR: 1                   MM Early Answer? n
           Security Code:                Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name
```

Step 2 – On **Page 2** of the form enter the following:

- **Message Center –** Enter **sip-adjunct**.
- **Voice Mail Number** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Voice Mail Handle** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Routing Digits** – Enter the AAR access code defined in **Section 5.3** (e.g., **8**).

```
change hunt-group 1                                          Page   2 of  60

                                  HUNT GROUP

Message Center: sip-adjunct        Routing Digits
     Voice Mail Number        Voice Mail Handle     (e.g., AAR/ARS Access Code)
          36000                     36000                       8
```

5.14.2. Coverage Path for Station Coverage to Avaya Aura® Messaging

After the coverage hunt group is provisioned, it is associated with a coverage path.

Step 1 – Enter the command **add coverage path x**, where **x** is an available coverage path (e.g., **1**), and on **Page 1** of the form enter the following:

- **Point1** – Specify the hunt group defined in the previous section (e.g., **h1**).
- **Rng** – Enter the number of rings before the stations go to coverage (e.g., **4**).
- Let all other fields default.

```
add coverage path 1                                       Page   1 of   1

                                 COVERAGE PATH

     Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage
COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
       Don't Answer?             y               y        Number of Rings: 4
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n
COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h1             Rng: 4  Point2:
  Point3:                        Point4:
```

5.14.3. Apply Station/Agent Coverage Path

The Coverage Path to Avaya Aura® Messaging s defined on the station form or on the Agent form. In addition, the Class of Restriction (COR) is applied to the Agent.

Step 1 – Enter the command **change station xxxxx**, where **xxxxx** is a previously defined station (e.g., **19001**), and on **Page 1** of the form enter the following:

- **Coverage path** – Specify the coverage path defined in **Section 5.14.2** (e.g., **1**).

```
change station 19001                                            Page   1 of   5

                                   STATION

Extension: 19001                         Lock Messages? n               BCC: 0
     Type: 9630                          Security Code:                  TN: 1
     Port: S00000                      Coverage Path 1: 1               COR: 1
     Name: 9630 H323                   Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 19001
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n
                                                         IP Video? N
                          Short/Prefixed Registration Allowed: default
                                              Customizable Labels? y
```

Step 2 – Using the command **change Agent xxxxx**, where **xxxxx** is a previously defined Agent (e.g., **47002**), repeat **Step 1** to define a coverage path for an Agent (e.g., coverage path **1**).

5.15. Call Center Provisioning

The administration of Communication Manager Call Center elements – Agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult **[10]** for further details, if necessary. The samples that follow are provided for reference purposes only.

```
display Agent-loginID 47002        AGENT LOGINID                  Page   2 of   3
      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: 2       1
```

```
display hunt-group 2              HUNT GROUP                        Page   1 of   4
            Group Number: 2                                 ACD? y
              Group Name: Skill2                          Queue? y
         Group Extension: 43002                          Vector? y
              Group Type: ead-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 :
```

```
display vdn 44002                                               Page   1 of   3
                             VECTOR DIRECTORY NUMBER

                             Extension: 44002
                                 Name*: Skill2
                           Destination: Vector Number        2
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

```
display vector 2                                                Page   1 of   6
                                CALL VECTOR

    Number: 2               Name: Skill2
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    2   secs hearing ringback
02 announcement 42002
03 queue-to     skill 2    pri m
04 wait-time    10  secs hearing music
05 announcement 42005
06 goto step    3             if unconditionally
07 stop
```

5.16. Save Translations

After the Communication Manager provisioning is completed, changes must be saved.
Step 1 – Enter the command **save translation.**

```
save translation
                               SAVE TRANSLATION
           Command Completion Status                                Error Code
           Success                                                  0
```

6. Avaya Experience Portal

These Application Notes assume that Experience Portal, and Nuance have been installed, and basic administration has already been performed. In addition it is assumed that all necessary licensing of these platforms has been performed as well. The installation and licensing of these platforms is beyond the scope of this document. The following configuration steps illustrate only the settings used for the test reference configuration. Please see [**1 - 3**] for more information.

6.1. Background

As described in **Section 3**, Experience Portal consists of one or more Media Processing Platform (MPP) servers and an Experience Portal Manager (EPM) server. A "single server" configuration was used in the reference configuration. This consisted of a single MPP and EPM, running on a VMware environment, including a co resident Apache Tomcat Application Server for hosting the Voice XML (VXML) and/or Call Control XML (CCXML) application scripts for inbound call. In addition, Proactive Outreach Manager (POM) was installed to provide outbound dialing capabilities for Experience Portal (see **Section 7**).

Nuance Recognizer, Vocalizer, and Speech Server were installed on a Windows 2008 server also running in the VMWare environment. These provided Automated Speech Recognition (ASR) and Text to Speech (TTS) capabilities for Experience Portal.

Note – Avaya Experience Portal utilizes application scripts to define interactive capabilities (e.g., menus, call routing, etc), between Experience Portal, the service provider, and the rest of the CPE. Customers may develop their own applications to meet their specific needs, or consult Avaya Professional Services and/or authorized Avaya Business Partners. The programming and testing of such applications are beyond the scope of this document. Basic Experience Portal functionality, used in the SIP trunk testing described in this document, was provided by sample test scripts included as part of the Experience Portal installation (e.g., *intro.vxml* and *root.ccxml*).

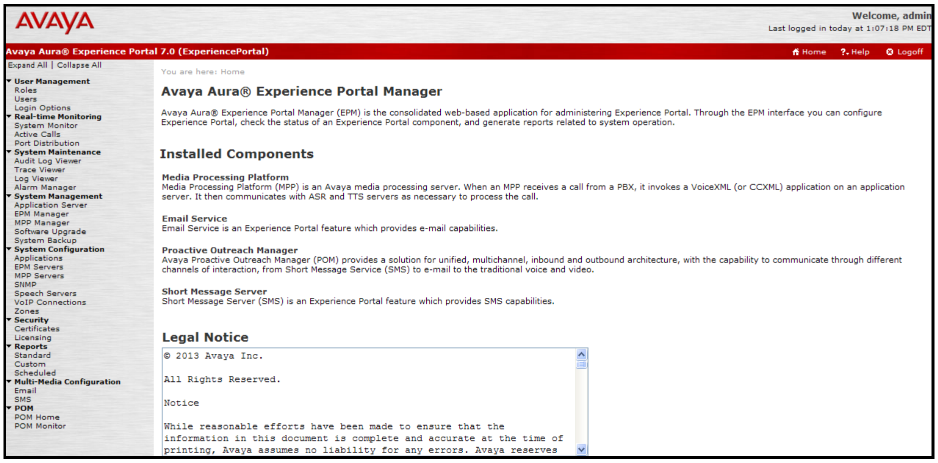
6.2. Experience Portal and Nuance Licenses Status

6.2.1. Experience Portal License Status

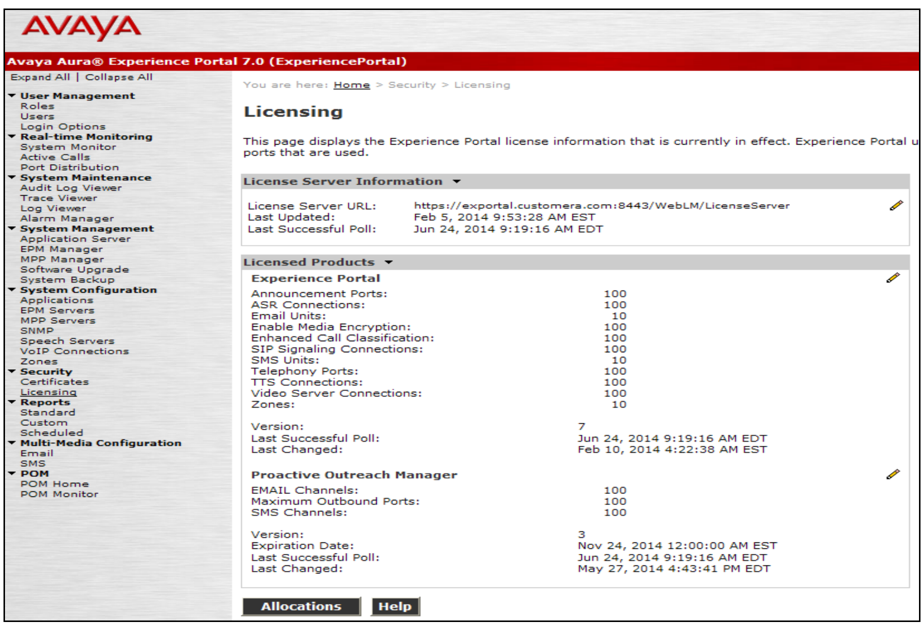
The following section displays the status of the Experience Portal and Proactive Outreach Manager licenses.

Step 1 - Launch a web browser, and enter the URL:
http://<IP address of the Avaya Experience Portal server>/
Then log in with the appropriate credentials and the following screen is displayed.

Note – All page navigation described in the following sections will utilize the menu shown on the left pane of the screenshot below.

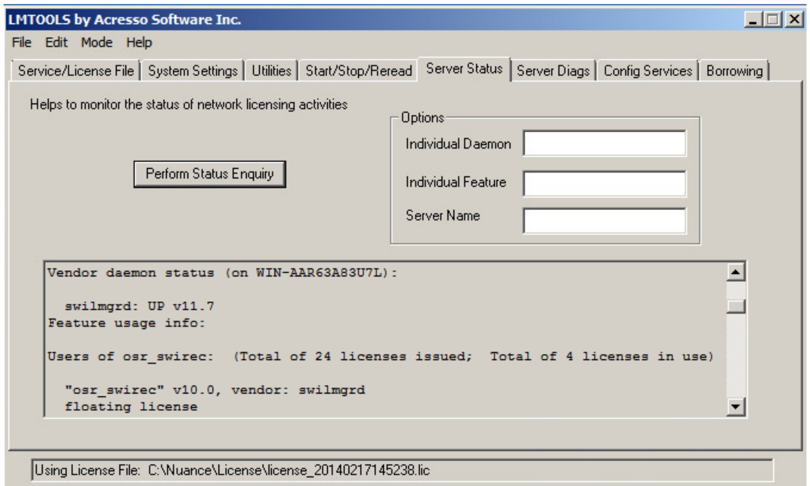


Step 2 - In the left pane, navigate to **Security→Licensing**. On the **Licensing** page, verify that Experience Portal and Proactive Outreach Manager are properly licensed. If required licenses are not enabled, contact an authorized Avaya account representative to obtain the licenses.



6.2.2. Nuance License Status

Step 1 – Log into the Windows server running Nuance, and navigate to **Start → Licensing Tools**, and the **LMTools** window will open. Select on the **Server Status** tab and click on **Perform Status Enquiry**. The display window will populate. Scroll through the display windows for the Nuance license information.

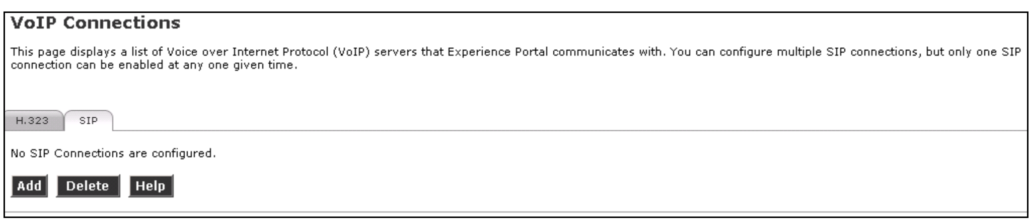


6.3. VoIP Connection

This section defines a SIP trunk between Experience Portal and Session Manager (see **Section 4.5.1**).

Step 1 - Following the steps shown in **Section 6.2, Step 1**, log into Experience Portal. In the left pane, navigate to **System Configuration→VoIP Connections**. On the **VoIP Connections** page, select the **SIP** tab and click **Add** to add a SIP trunk.

Note – Only ***one*** SIP trunk can be active at any given time on Experience Portal.

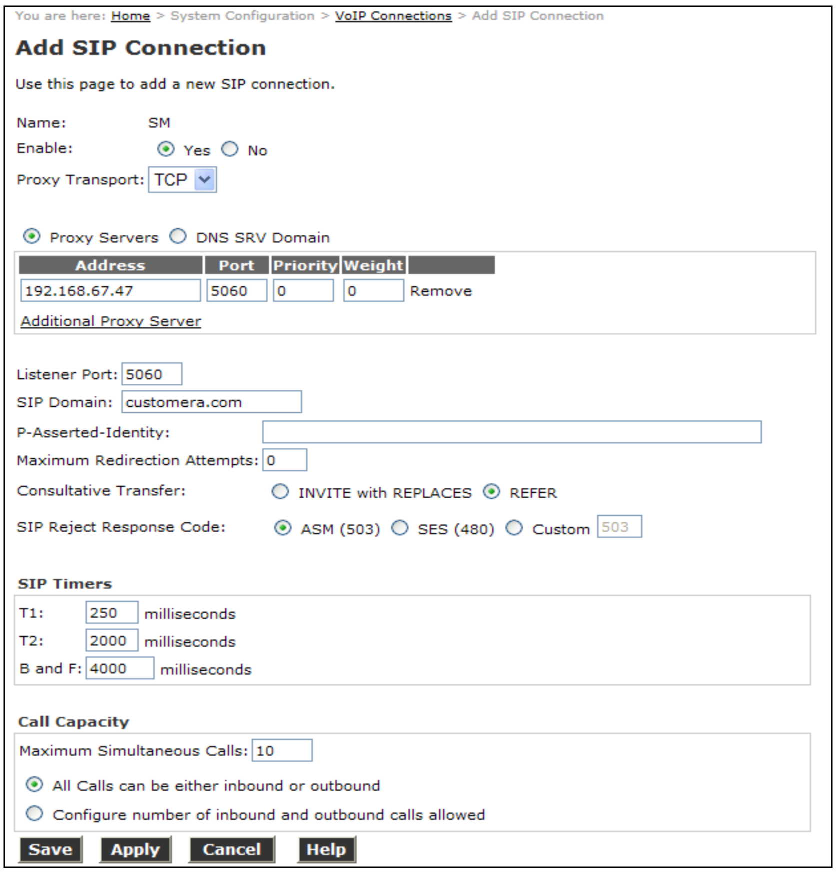


Step 2 - Configure a SIP connection as follows:

- **Name** – Set to a descriptive name (e.g., **SM**).
- **Enable** – Set to **Yes**.
- **Proxy Server Transport** – Set to **TCP**.
- Select **Proxy Servers**, and enter:
  - **Proxy Server Address** = **192.168.67.47** (the IP address of the Session Manager signaling interface defined in **Section 4.4.1**).
  - **Port** = **5060**

- **Priority** = **0** (default)
- **Weight** = **0** (default)

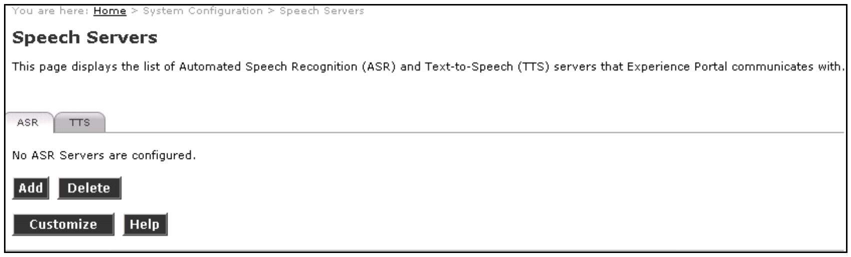
- **Listener Port** – Set to **5060**.
- **SIP Domain** – Set to **customera.com** (see **Section 4.1)**.
- **Consultative Transfer** – Select **REFER**.
- **Maximum Simultaneous Calls** – Set to a number in accordance with licensed capacity. In the reference configuration a value of **10** was used.
- Select **All Calls can be either inbound or outbound**.
- Use default values for all other fields.
- Click **Save**.



6.4. Speech Servers

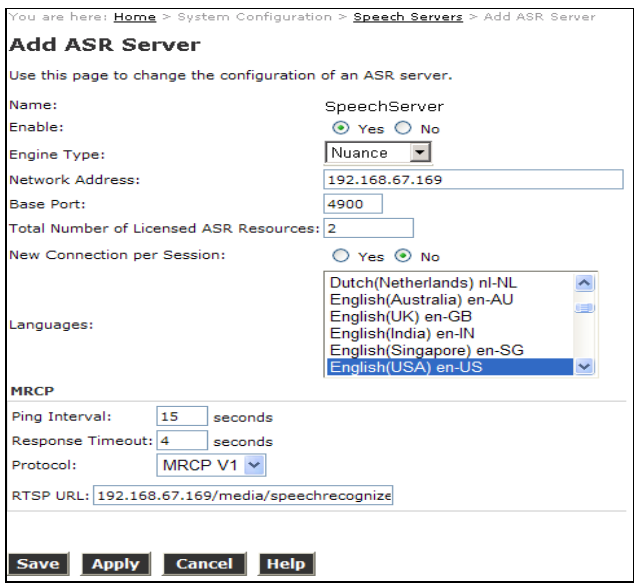
The installation and administration of the Nuance ASR and TSR Speech Servers are beyond the scope of this document. Some of the values shown below were defined during the Speech Server installations. Note that in the reference configuration the ASR and TTS servers use the IP address of the Windows server where they are installed.

Step 1 - To configure Experience Portal for communication with Speech Server, navigate to **System Configuration→Speech Servers** in the left pane menu, and the following screen is displayed. Select the **ASR** tab and click **Add** to add an ASR server.



Step 2 - On the **Add ASR Server** page, configure as follows:

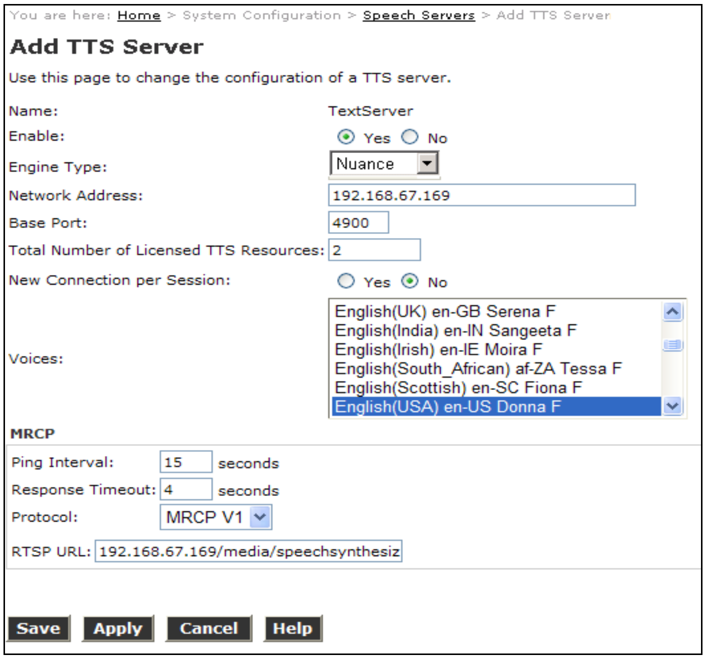
- **Name** – Set to any descriptive name (e.g., **SpeechServer**).
- **Enable** – Select **Yes**.
- **Engine Type** – Select **Nuance**.
- **Nework Address** – Set to the IP address of the ASR Server (e.g., **192.168.67.169**).
- **Languages** – Select the appropriate value (e.g., **English (USA) en-US**).
- The **RTSP URL** field contains the string ***<Network Address>/media/speechrecognizer***.
    - Replace ***<Network Address>*** with the ASR Server IP address (e.g., **192.168.67.169**).
- Use default values for all other fields and click **Save**.



Step 3 - Click **TTS** and **Add** on the screen shown in **Step 1**. On the **Add TTS Server** page, configure as follows:

- **Name** – Set to any descriptive name (e.g., **TextServer**).
- **Enable** – Select **Yes**.
- **Engine Type** – Select **Nuance**.
- **Nework Address** – Set to the IP address of the TTS Server (e.g., **192.168.67.169**).
- **Languages** – Select the appropriate value (e.g., **English(USA) en-US Donna F**).
- The **RTSP URL** field contains the string ***<Network Address>/media/speechsynthesizer***. Replace ***<Network Address>*** with the TTS Server IP address (e.g., **192.168.67.169**).

- Use default values for all other fields.
- Click **Save**.



6.5. Application References

This section describes the steps for administering a reference to the VXML and/or CCXML applications residing on the application server. As described previously, basic Experience Portal functionality, used in the SIP trunk testing described in this document, was provided by sample test scripts included as part of the Experience Portal installation (e.g., *intro.vxml* and *root.ccxml*). In addition, inbound AT&T IPFR-EF service DNIS digits are defined.

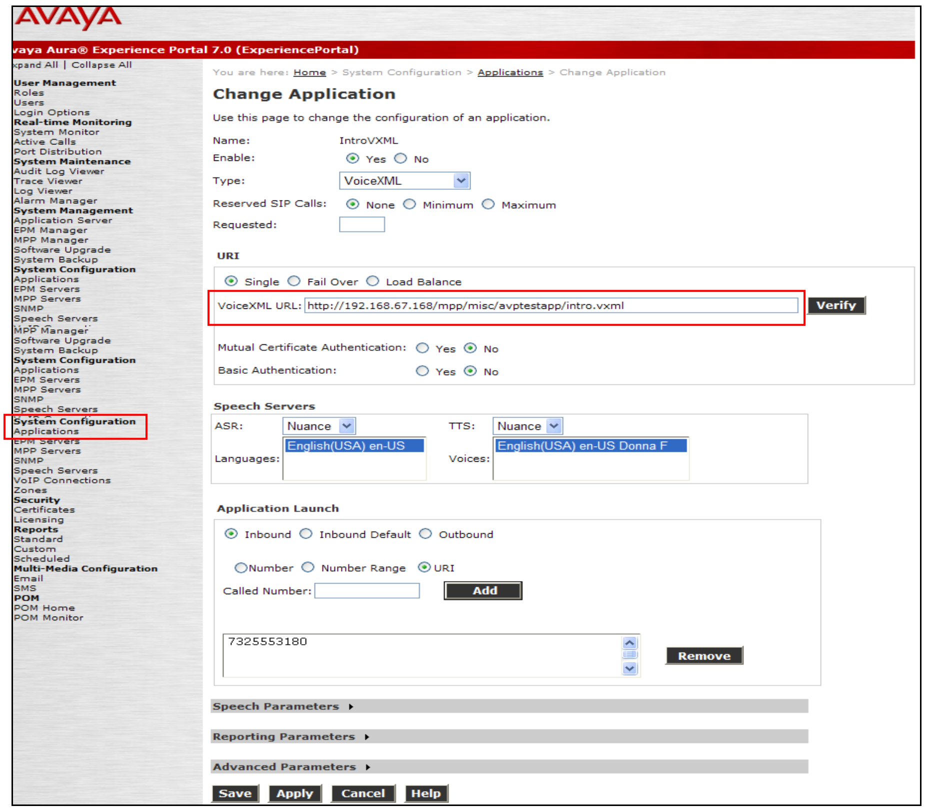
Step 1 - In the left pane, navigate to **System Configuration→Applications**. On the **Applications** page (not shown), click **Add** to add a VoiceXML application and configure as follows:

- **Name** – Set to a descriptive name (e.g., **IntroVXML**).
- **Enable** – Set to **Yes**. This field determines which application(s) will be executed based on their defined criteria.
- **Type** – Set **to VoiceXML**.
- **URI** –
  - Set to **Single**
  - **VoiceXML URL** – Set to the application URL on the Tomcat server. (e.g., **http://**<*Tomcat server IP address*>**/mpp/misc/avptestapp/intro.vxml**
- **Speech Servers - ASR:** and **TTS:** – Set to **Nuance**.
- **Languages** - In the reference configuration, these were set to **English (USA) en-US** and **Voices** set to **English(USA) en-US Donna F**. Note that these values are per the speech server settings in **Section 6.4**.

Step 2 - Inbound AT&T IPFR-EF service DNIS numbers, processed by this application, are defined in the following steps. Select the **Number** or **URI** radio button. When the **Number** option is selected Experience Portal will match on the contents of the inbound Invite *To* header. If the URI option is selected, Experience Portal will match on the contents of the inbound Invite *R-URI* header. In the reference configuration, the **URI** option was chosen.

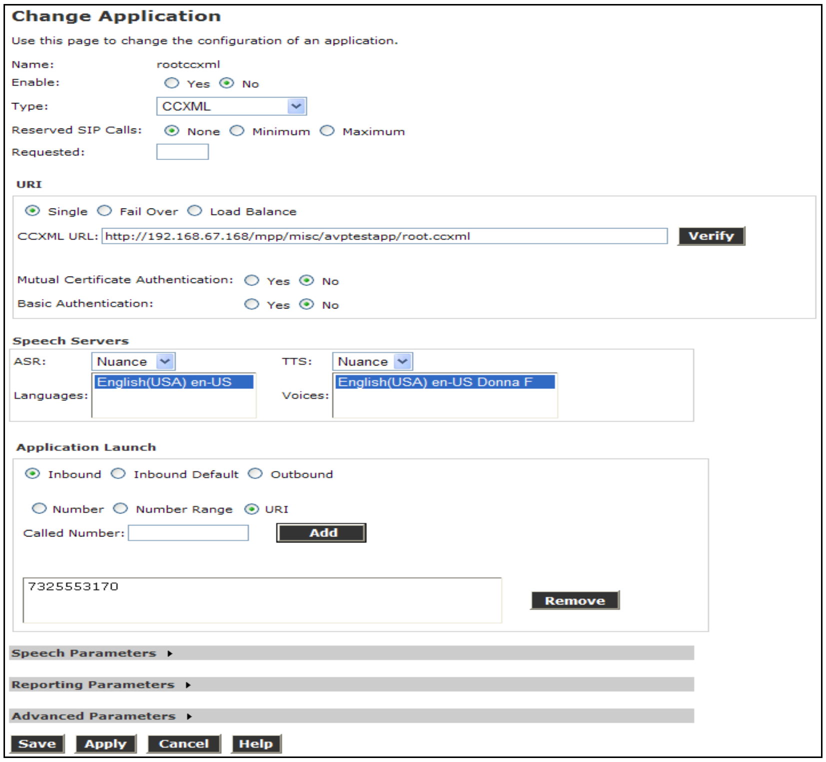
- **Application Launch –** Set to **Inbound**.
- **Called URI –** Set to an inbound AT&T IPFR-EF service DNIS specified in the **Request-URI** header of the inbound SIP INVITE message (e.g.,**7325553180**), then click on **Add**. The entered number will then appear in the box below the field. Use the **Remove** button to delete an entry.

Step 3 - Use the default values for all other fields. Click on **Save**.



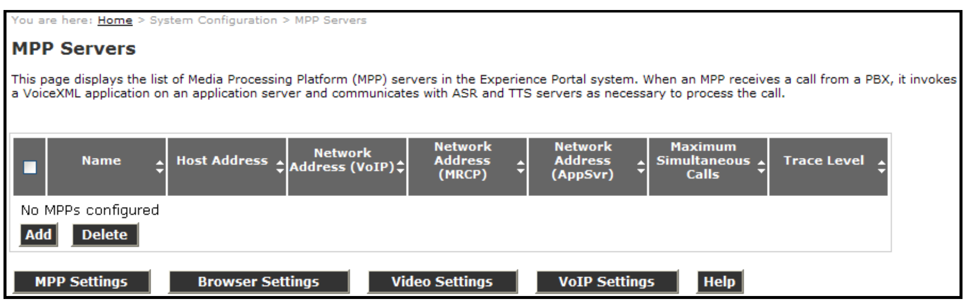
Step 4 - Repeat **Steps 1 - 3** to define additional applications. The sample CCXML application *root.ccxml*, was used in the reference configuration and is defined below:

- **Type** – Set **to CCXML**.
- **URI** – Set to **Single**
- **CCXML URL** – Set to the application URL of the Tomcat server. (e.g., **http://<***Tomcat server IP address***>/mpp/misc/avptestapp/ root.ccxml**.
- **Called URI –** In this example AT&T IPFR-EF service DNIS number **7325553170** is used.

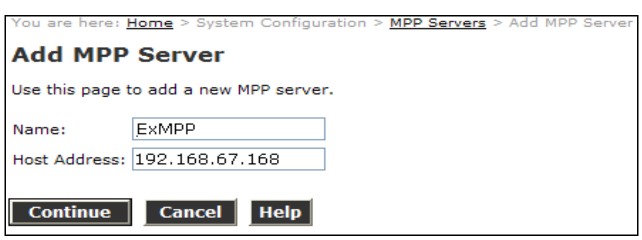


6.6. Add an MPP Server

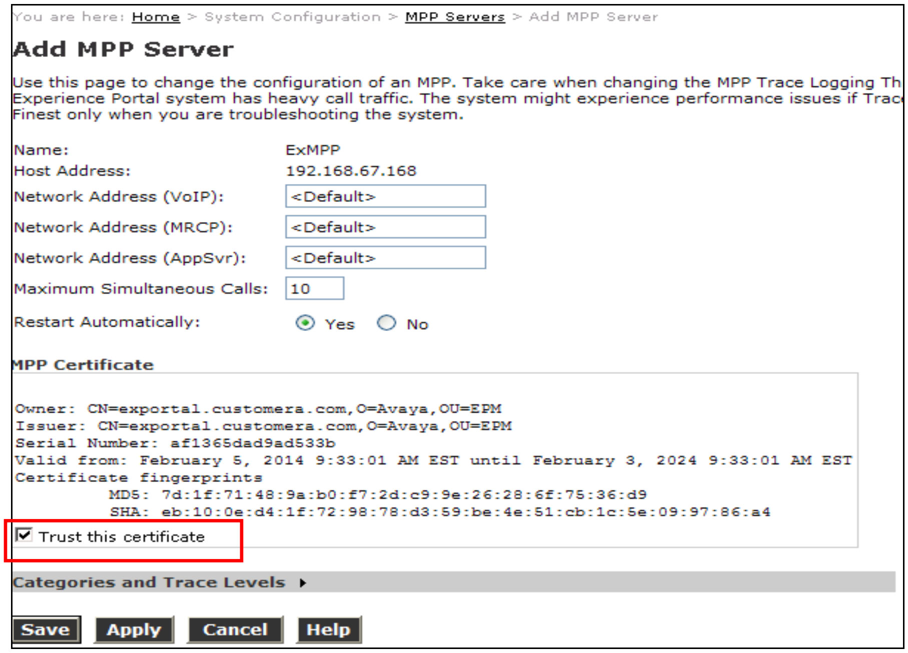
Step 1 - In the left pane, navigate to **System Configuration→MPP Servers** and the following screen is displayed. Click **Add**.



Step 2 - Enter any descriptive name in the **Name** field (e.g., **ExMPP**) and the IP address of the MPP server in the **Host Address** field.



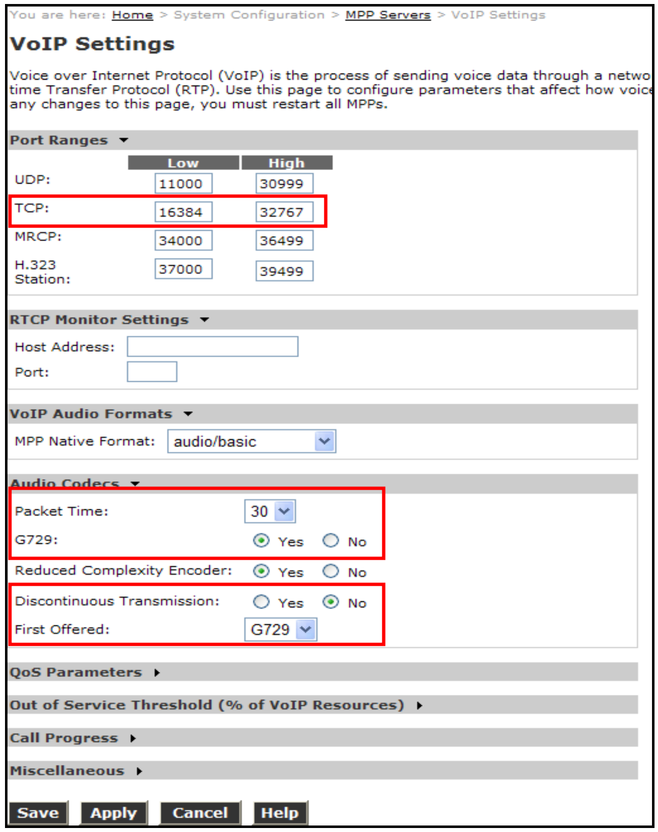
Step 3 - Click **Continue** and the certificate page will open. Use the self-populating/default values, and check the **Trust this certificate** box. Click **Save**.



Step 4 - Click **VoIP Settings** tab on the screen displayed in **Step 1**, and the following screen is displayed.

- In the Port Ranges section, verify that **TCP** ports are in the range of **16384** and **32767** as required by the AT&T IPFR-EF service.
- In the Audio Codecs section set:
  - Set **Packet Time** to **30**. (See **Section 2.2, Item 5**).
  - Verify the **G729** is set to **Yes**.
  - Set **Discontinuous Transmission** to **No** (G.729A) or **Yes** (G.729B) as required.
  - Set **First Offered** to **G729**.
- Use default values for all other fields.

Step 5 - Click on **Save**.

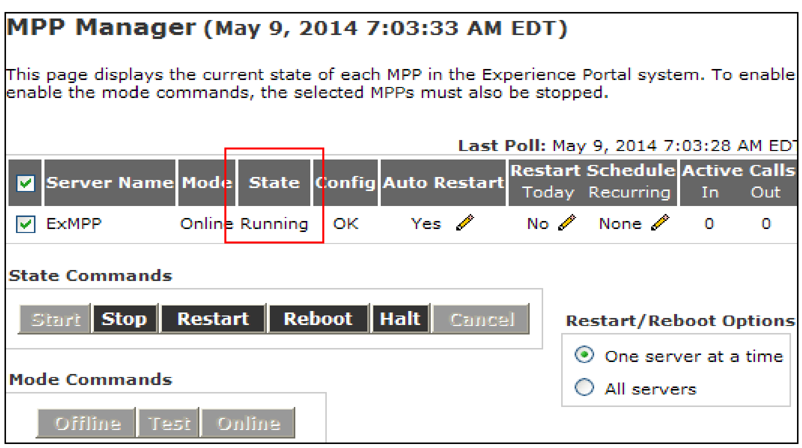


6.7. Restarting the MPP Manager

After adding/configuring the MPP, the MPP must be restarted to have the changes take effect.

Step 1 - In the left pane, navigate to **System Maintenance→MPP Manager** and select the **ExMPP** instance created in **Section 6.6**. This will enable the **State Command** buttons.

Step 2 - Click **Restart**. Note that the **State** column shows when the MPP is running after the restart.



7. Proactive Outreach Manager

Avaya Proactive Outreach Manager (POM) is a managed application of Avaya Aura® Experience Portal, providing a solution for unified, outbound calling capabilities. In the reference configuration, Avaya Proactive Outreach Manager is used to generate outbound calls to PSTN, via the IPFR_EF service.

Note - These Application Notes assume that Avaya Proactive Outreach Manager has been installed, and basic administration has already been performed. In addition it is assumed that all necessary licensing has been performed as well. The installation and licensing of Avaya Proactive Outreach Manager is beyond the scope of this document. The following configuration steps illustrate only the settings used for the test reference configuration. Please see [**4**] for more information.

7.1. Defining a Proactive Outreach Manager Campaign

POM Campaigns define the conditions under which POM will generate outbound calls.

Note - The following campaign is designed for generating a basic outbound call, and should not be considered prescriptive. The design and programming of campaigns is beyond the scope of these application notes.

7.1.1. Creating a Contact List

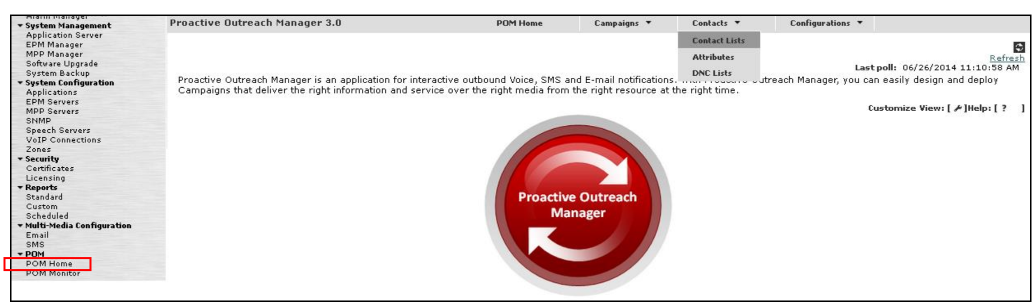
Before creating the campaign, a contact list must be created that the campaign will use for the outbound calls.

Step 1 – Open a text application such as Windows Notepad and enter the following information in the format shown below. Note that the fields are separated by a comma.

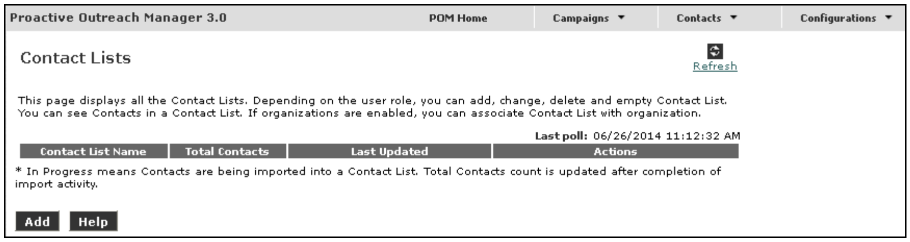
- Contact **ID** = an identifier for the contact (e.g., 123).
- **phonenumber1** = the contact's phone number (e.g., 7325551234).

```
Id,phonenumber1
123,7325551234
```

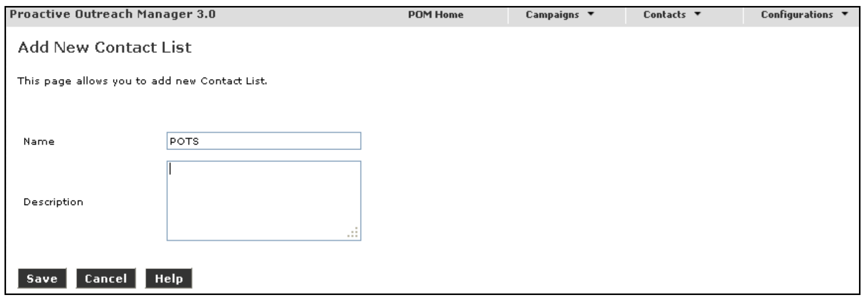
Step 2 – Save the file using a ***.csv*** extension (e.g., **POTS.csv**)
Step 3 – Following the steps in **Section 6.2.1**, connect to the Experience Portal GUI and click on **POM Home** in the left hand menu. The POM configuration page will open.
Step 4 –Click on **Contacts → Contacts Lists**.



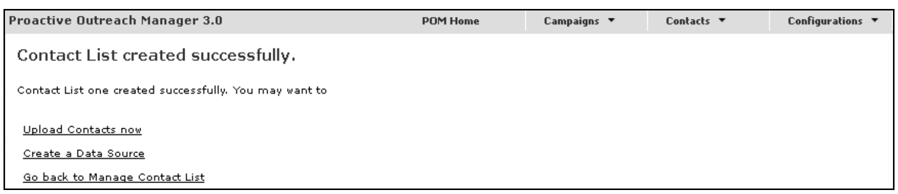
Step 5 – The Contact List page will open. Click on **Add**.



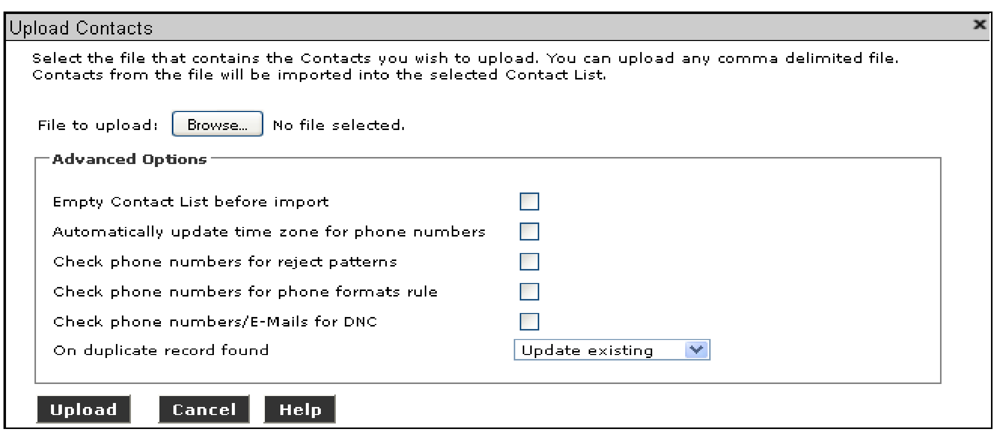
Step 6 – Enter a descriptive name (e.g., **POTS**) and click on **Save**.



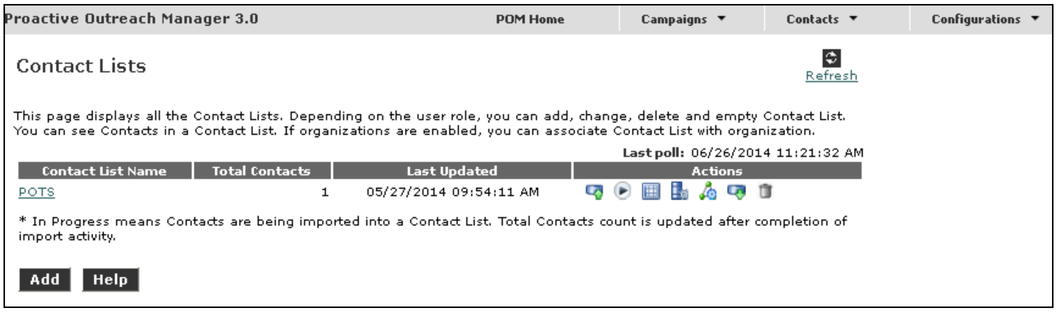
Step 7 – The following menu will open. Select **Upload Contacts now**.



Step 8 – The **Upload Contacts** form will open. Select **Browse** and point to the POTS.csv file saved in **Step 2**. Then click on **Upload**.

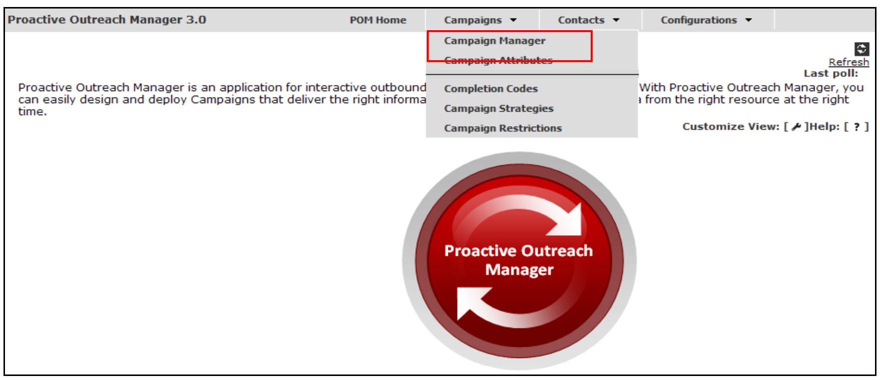


Step 9 – Once the contact file has uploaded, the system will display the completed contact.



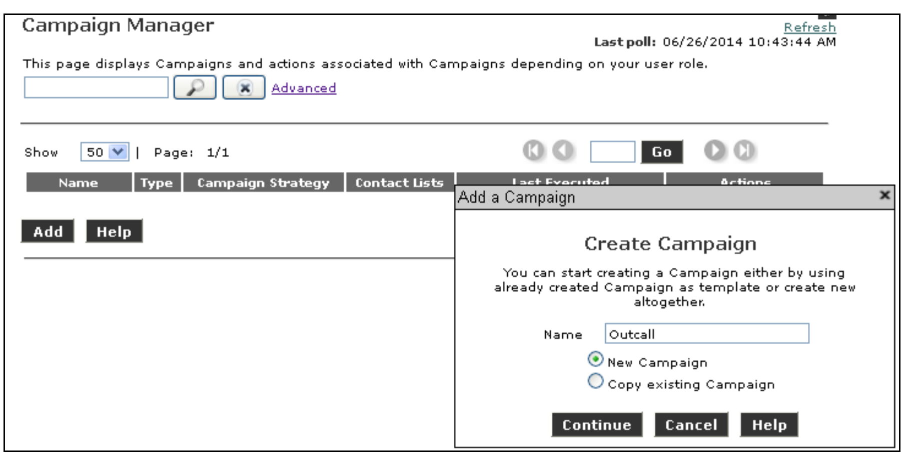
7.1.2. Creating a Campaign

Step 1 – As shown in **Section 7.1.1**, **Step 3**, click on **POM Home**, and the POM main page will open. Click on **Campaigns → Campaign Manager**.



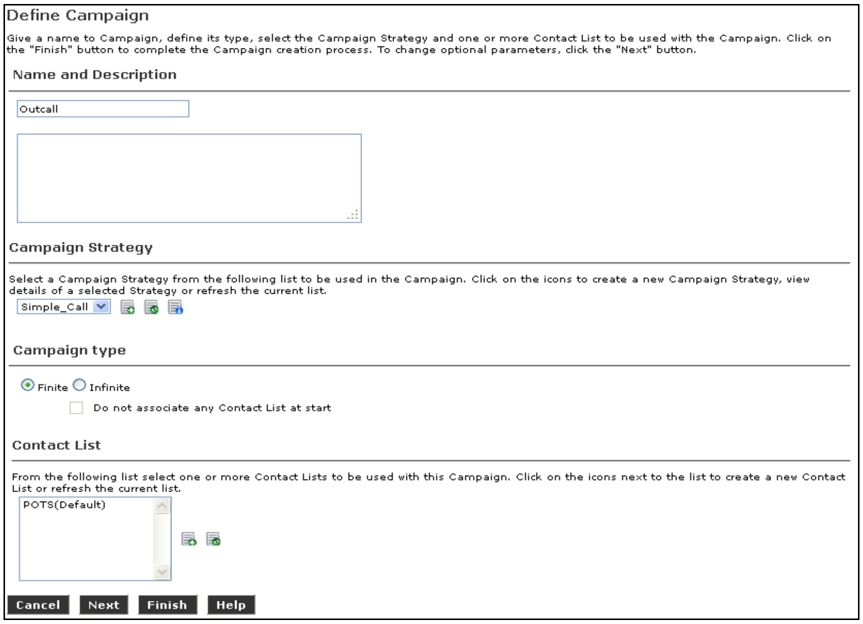
Step 2 – Click on **Add**. In the **Create Campaign** form enter:

- **Name** = Enter a name for the campaign.
- Select **New Campaign**.
- Click on **Continue**.



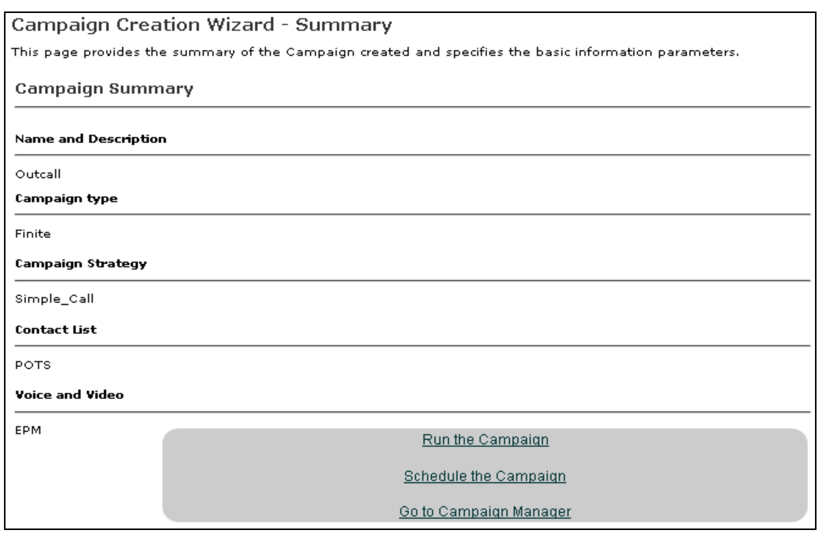
Step 3 – The **Define Campaign** window will open.

- In the name field enter a descriptive campaign name (e.g., **Outcall**).
- In the **Campaign Strategy** section, select **Simple_Call** from the drop-down menu.
- For **Campaign Type**, select **Finite**.
- For **Contact List** select the Contact defined in **Section 7.1.1** (e.g., **POTS**).
- Click on **Finish.**



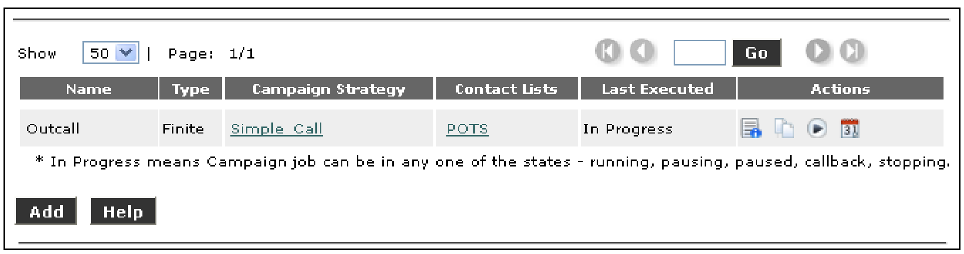
Step 4 – The system displays the **Summary** screen, with the following choices:

- Select **Run the Campaign**, to execute the campaign now.
- Select **Schedule the Campaign** to bring up the Campaign scheduler.
- Select **Go to Campaign Manager** to return to the Campaign Manager main screen.



Step 5 – If **Go to Campaign Manager** is selected, then the system returns to the Campaign Manager screen, displaying the new campaign. The campaign may be executed here by clicking on the  (Run Now) **Action** button.

The **Last Executed** column will display "**In Progress**" as the outbound call is sent.



8. Avaya Aura® Messaging

In this reference configuration, Avaya Aura® Messaging is used to verify basic call coverage/message retrieval functionality, as well as Message Waiting Indicator (MWI).

The administration for Avaya Aura® Messaging is beyond the scope of these Application Notes. Consult **[13]** for further details.

9. Configure Avaya Session Border Controller for Enterprise

Note: Only the Avaya SBCE provisioning required for the reference configuration is described in these Application Notes. The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to **[11 & 12]** for additional information.

9.1. Initial Installation/Provisioning

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE <u>must</u> be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in its own subnet (Common site, 192.168.70.x), with access to the Main site (192.168.67.x) subnet. The connection to AT&T uses the Avaya SBCE public interface B1 (IP address 10.10.10.12[6]).

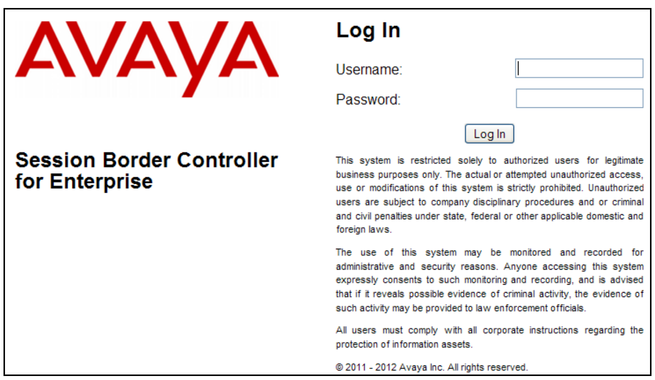
9.2. Log into the Avaya SBCE

The follow provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

Step 1 - Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).

Step 2 - Enter the **Username** and click Continue (not shown).

Step 3 – Enter the **Password** and click **Log In**.

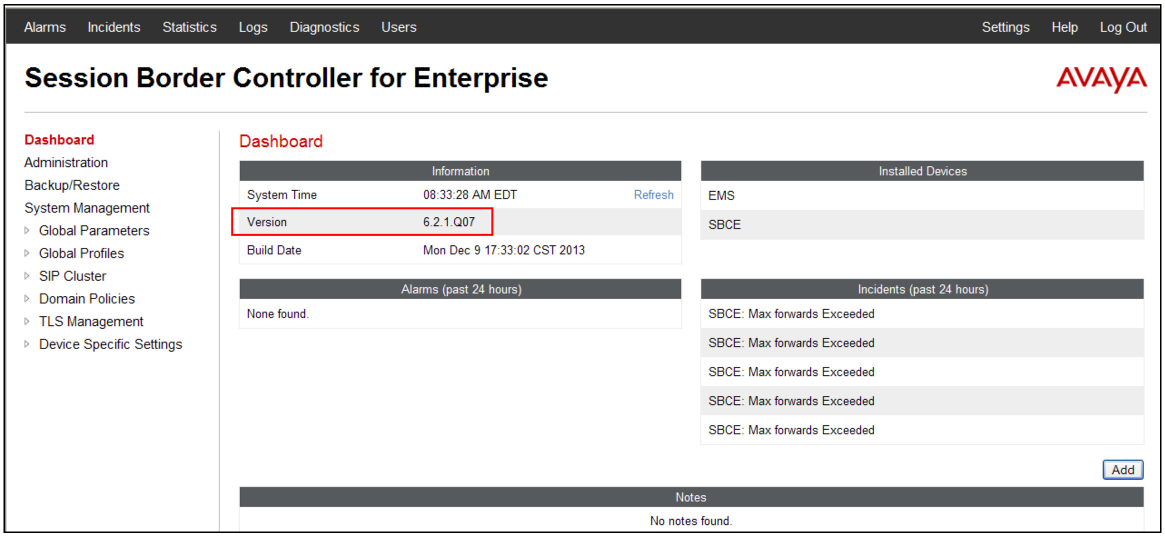


Step 4 - The main menu window will open. Note that the installed software version is displayed[7].

Note – All page navigation described in the following sections will utilize the menu shown on the left pane of the screenshot below.

[6] See **Section 3**.

[7] Note that loads Q07 and Q16 were used during testing.



9.3. Global Profiles

Global Profiles allow for configuration of parameters across the Avaya SBCE appliances.

9.3.1. Server Interworking – Avaya

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing.

One of the capabilities important to the Experience Portal environment is the Avaya SBCE **Refer Handling** option. As described in **Section 3.2**, Experience Portal inbound call processing may include call redirection to Communication Manager Agents, or other CPE destinations. This redirection is accomplished by having Experience Portal send SIP Refer messaging to the Avaya SBCE. Enabling the **Refer Handling** option causes the Avaya SBCE to intercept and process the Refers, and generate new SIP Invite messages back to the CPE (e.g., Communication Manager, see **Section 2.2**, **Item 4a** and **Section 3.2.2**).

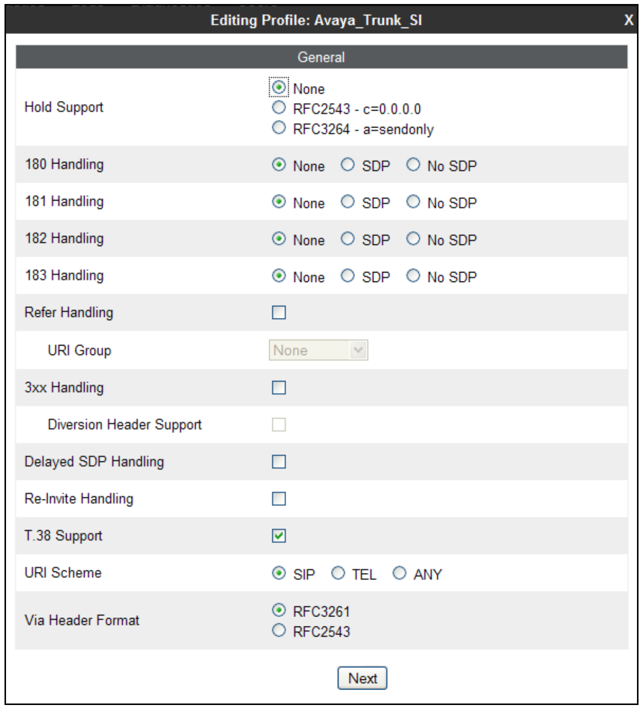
Note – For call redirection scenarios requiring Refer processing by the AT&T IPFR-EF service, (see **Section 2.2**, **Item 4b** and **Section 3.2.3**), the **Refer Handling** option must be disabled.

Step 1 - Select **Global Profiles → Server Interworking** from the left-hand menu (not shown).
Step 2 - Select the default **avaya-ru** profile and click **Clone** button (not shown). The **Profile** name window will open (not shown).
Step 3 - Enter a profile name: (e.g., **Avaya_Trunk_SI**), and click **Next**.
Step 4 - The **General** screen will open.

- Verify that **Hold Support** is **None** (default).
- Verify that **Refer Handling** is _not_ selected (default), and **URI Group** is set to **None** (default).

Note – See the comments at the beginning of this section regarding this option.

- Select **T38 Support**.
- All other options can be left with default values
- Click **Next**



Step 5 - On the **Privacy/DTMF** screen (not shown), select **Next** to accept default values.
Step 6 - On the **SIP Timers/Transport Timers** screen (not shown), select **Next** to accept default values.
Step 7 - On the **Advanced** screen(not shown), accept the default values, and click **Finish**.

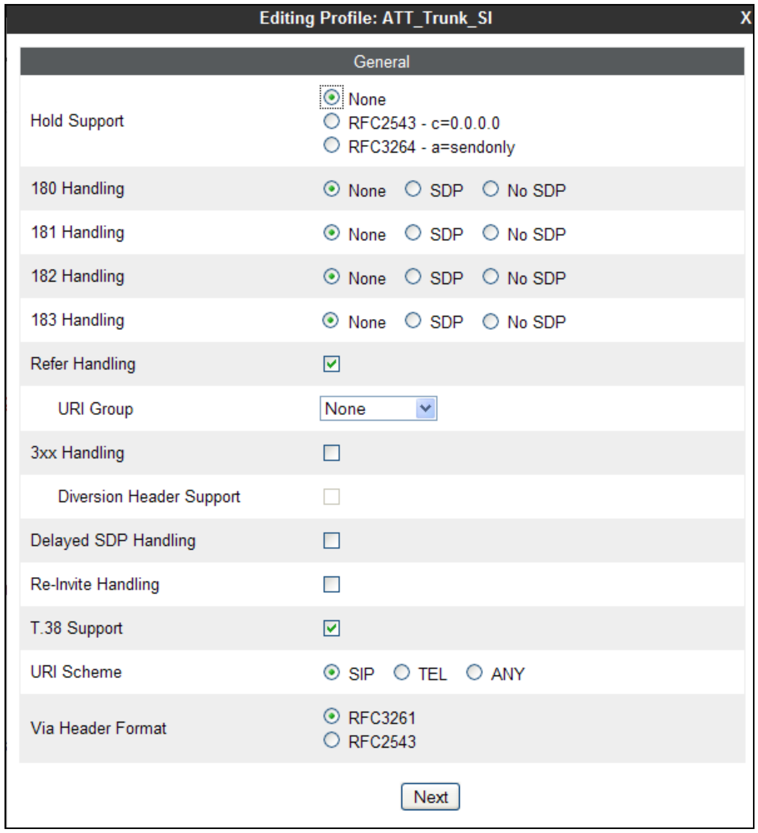
9.3.2. Server Interworking – AT&T

Add an Interworking Profile for the connection to AT&T via the public network.
Step 1 - Select **Global Profiles → Server Interworking** from the menu on the left-hand side (not shown).
Step 2 - Select **Add Profile**.
Step 3 - On the **General** Tab (not shown):

- Enter a profile name**:** (e.g., **ATT_Trunk_SI**).
- Enable **Refer Handling**, and verify that **URI Group** is set to **None** (default).

Note – See the comments at the beginning of **Section 9.3.1** regarding this option.

- Check **T38 Support.**
- All other options can be left as default.
- Click **Next.**



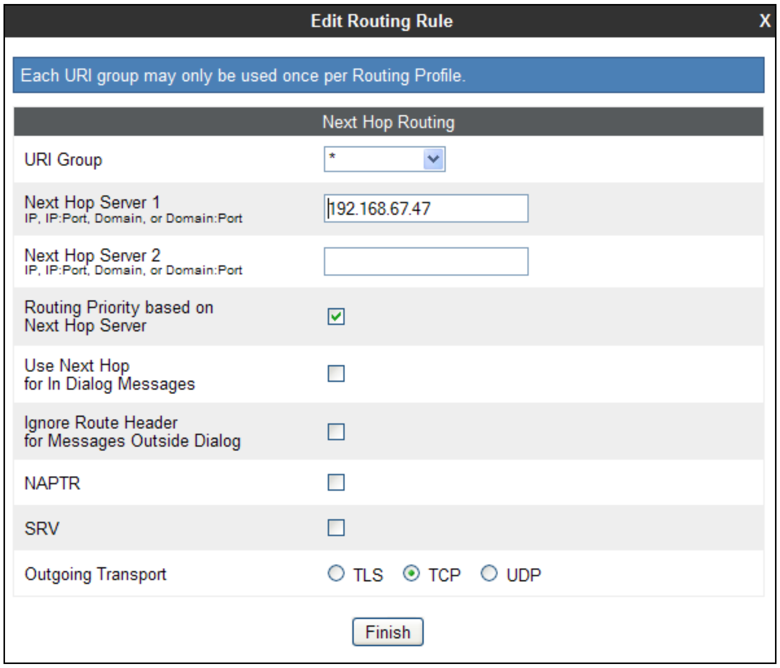
Step 4 - At the **Privacy** screen (not shown), select **Next** to accept default values.
Step 5 - At the **Interworking Profile** screen (not shown), select **Next** to accept default values.
Step 6 - On the last screen, **Advanced** options, (not shown), accept the default values, and click **Finish**.

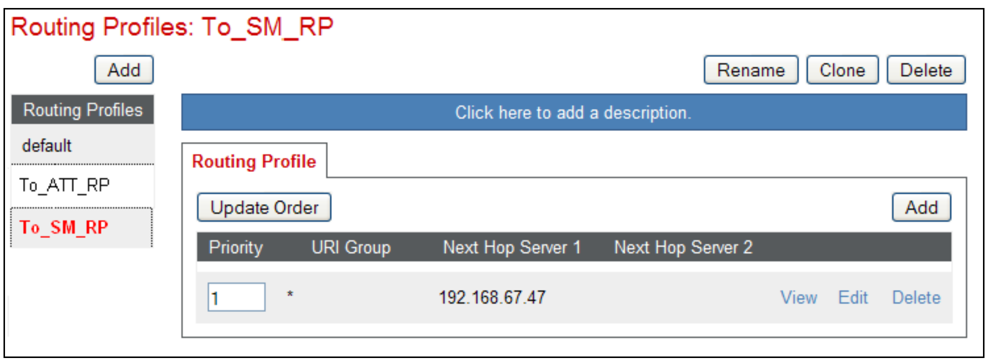
9.3.3. Routing – To Session Manager

The following routing profile provides routing to Session Manager.
Step 1 - Select **Global Profiles → Routing** from the menu on the left-hand side (not shown).
Step 2 - Select **Add Profile** (not shown).
Step 3 - Enter **Profile Name**: (e.g., **To_SM _RP)**.
Step 4 - Click **Next** and enter the following for regular inbound calls:

- In the **URI Group** field specify *
- **Next Hop Server 1**: **192.168.67.47** (Session Manager)
- Verify **Routing Priority Based on Next Hop Server** is selected (default).
- **Outgoing Transport**: **TCP**
- Accept remaining default values

Step 5 - Click **Finish**.





9.3.4. Routing – To AT&T

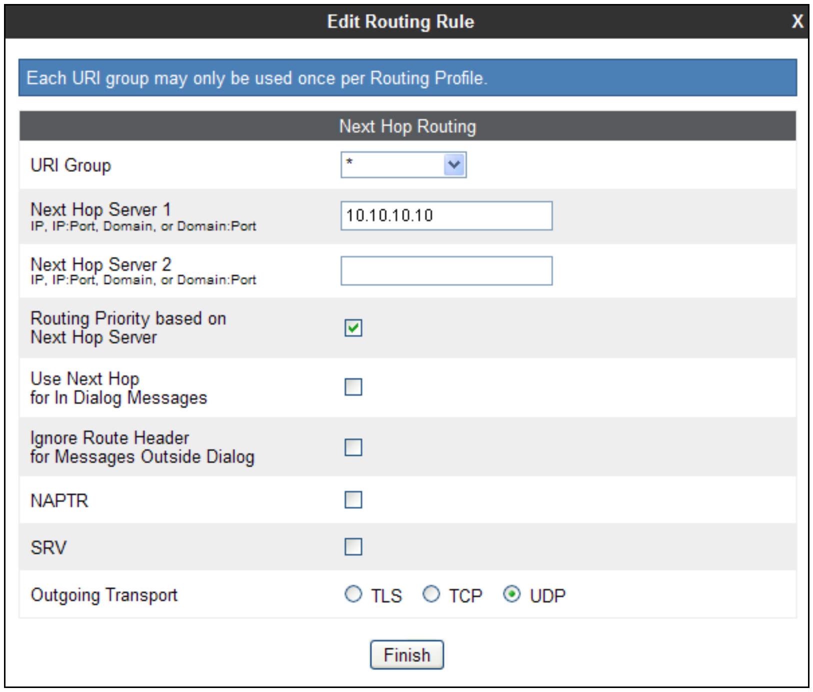
Repeat the steps in **Section 9.3.3**, with the following changes, to add a Routing Profile for the connection to AT&T.

Step 1 - Enter Profile Name: (e.g., **To_ATT_RP)**.

Step 2 - Click **Next**, then enter the following:

- **Next Hop Server 1: 10.10.10.10** (Primary AT&T Border Element IP address)
- Verify **Routing Priority Based on Next Hop Server** is selected (default).
- **Outgoing Transport**: **UDP**

Step 3 - Click **Finish**.



9.3.5. Server Configuration – Session Manager

Step 1 - Select **Global Profiles → Server Configuration** from the menu on the left-hand side (not shown).

Step 2 - Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **SM_Trunk_SC**) and click **Next**.

Step 3 - The **Add Server Configuration Profile - General** window will open (not shown).

- Select **Server Type**: **Call Server**
- **IP Address**: **192.168.67.47**
- **Supported Transports**: Check **TCP and TLS** (see the note in **Section 3**).
- **TCP Port**: **5060**
- **TLS Port: 5061**
- Select **Next**

Step 4 - The **Add Server Configuration Profile - Authentication** window will open (not shown).

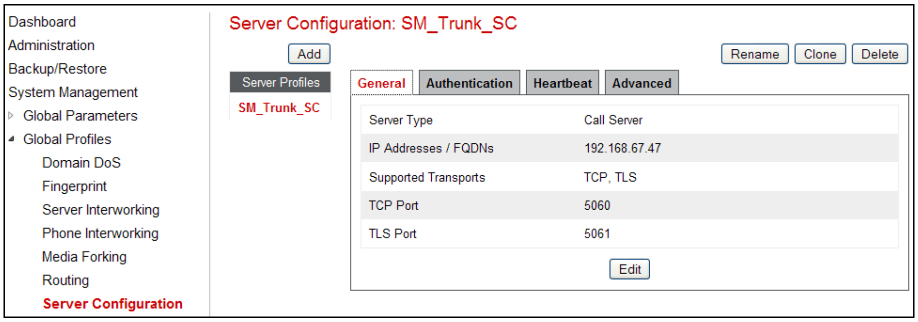
- Select **Next** to accept default values.

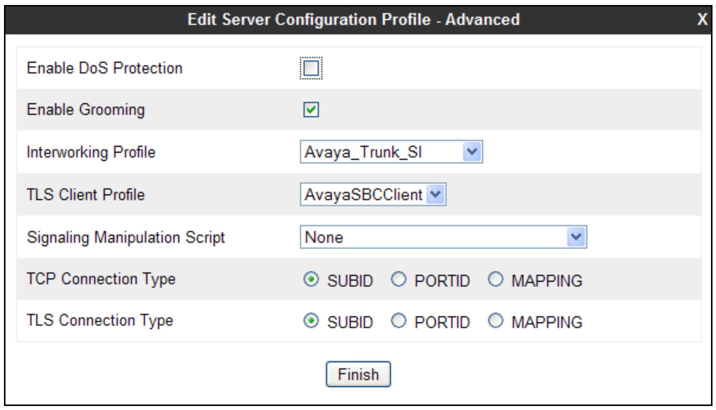
Step 5 - The **Add Server Configuration Profile - Heartbeat** window will open (not shown).

- Select **Next** to accept default values.

Step 6 - The **Add Server Configuration Profile - Advanced** window will open.

- Select **Avaya_Trunk_SI** (created in **Section 9.3.1**), for **Interworking Profile**.
- Select **AvayaSBCClient** for **TLS Client Profile**.
- **Verify the Signaling Manipulation Script field is set to None (default).**
- Select **Finish**.





9.3.6. Server Configuration – AT&T

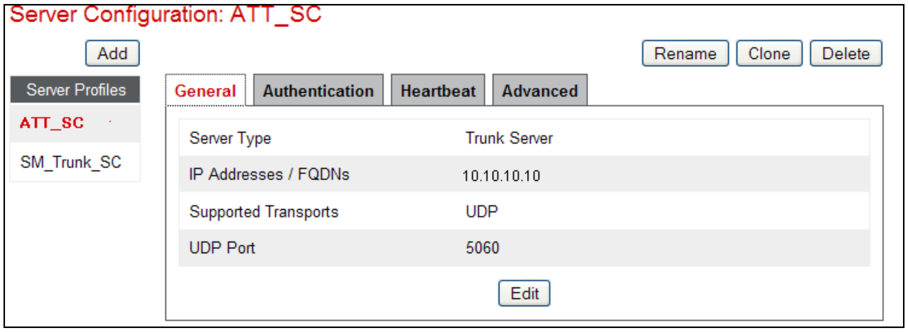
Note – The AT&T IPFR-EF service may provide a Primary and Secondary Border Element. This section describes the connection to a single Border Element. See **Addendum 1** for information on configuring Primary & Secondary IPFR-EF Border Elements.

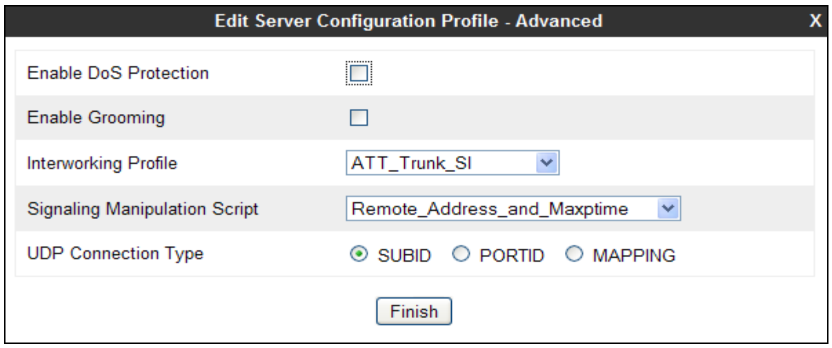
Repeat the steps in **Section 9.3.5**, with the following changes.
Step 1 - Enter a Profile Name (e.g., **ATT_SC**) and select **Next**.
Step 2 - The **Add Server Configuration Profile - General** window will open (not shown).

- Select Server Type**: Trunk Server**
- **IP Address: 10.10.10.10** (AT&T Border Element IP address)
- **Supported Transports**: Check **UDP**
- **UDP Port: 5060**
- Select **Next**.

Step 3 - The **Add Server Configuration Profile - Advanced** window will open.

- Select **ATT_Trunk_SI** (created in **Section 9.3.2**), for **Interworking Profile**.
- In the **Signaling Manipulation Script** field select **Remote_Address_and_Maxptime** (see **Section 2.2**, **Items 3** & **6**, and **Section 9.3.9**).
- Select **Finish**.





9.3.7. Topology Hiding – Avaya Side

The **Topology Hiding** hides the topology of the enterprise network from external networks.
Step 1 - Select **Global Profiles → Topology Hiding** from the menu on the left-hand side (not shown).
Step 2 - Click **default** profile and select **Clone Profile** (not shown).
Step 3 - Enter Profile Name: (e.g., **Avaya_TH**)
Step 4 - For the Header **To**,

- In the **Criteria** column select **IP/Domain**
- In the **Replace Action** column select **Overwrite**
- In the **Overwrite Value** column enter **customera.com**

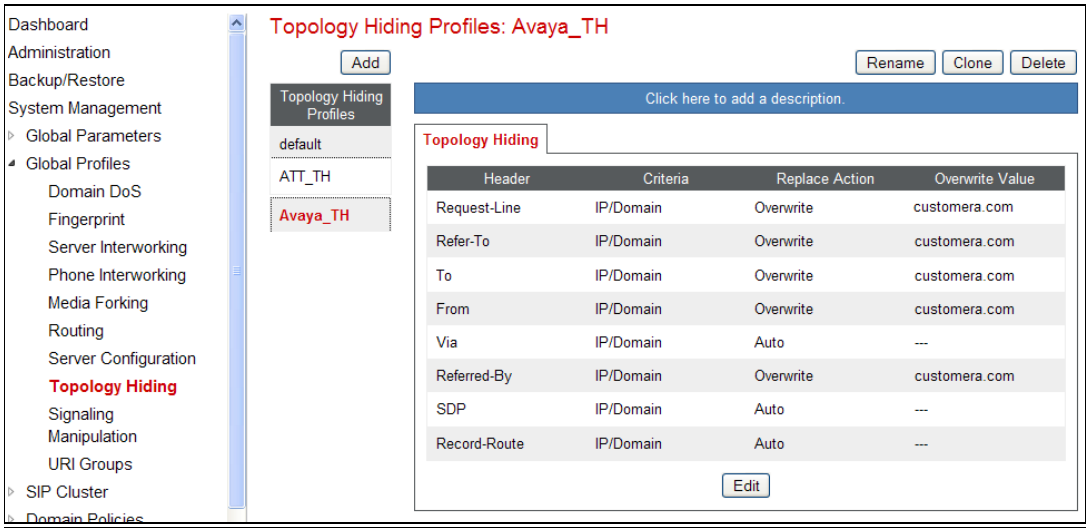
Step 5 - For the Header **Request Line**,

- In the **Criteria** column select **IP/Domain**
- In the **Replace Action** column select **Overwrite**
- In the **Overwrite Value** column enter **customera.com**

Step 6 - For the Header **From**,

- In the **Criteria** column select **IP/Domain**
- In the **Replace Action** column select **Overwrite**
- In the **Overwrite Value** column enter **customera.com**

Step 7 - Use default values for rest of the fields.
Step 8 - Click **Finish**.

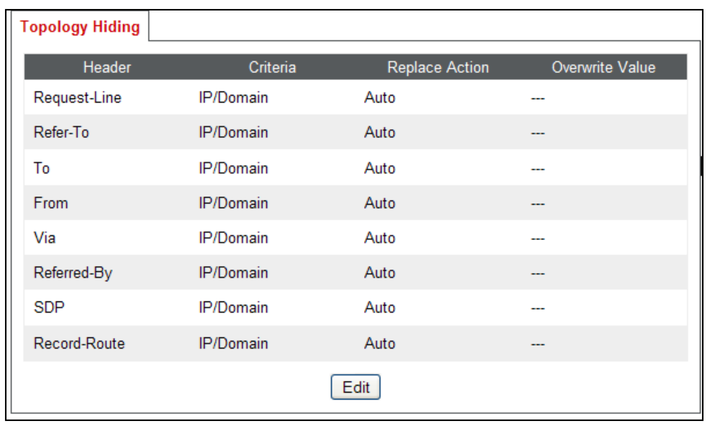


Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	customera.com
Refer-To	IP/Domain	Overwrite	customera.com
To	IP/Domain	Overwrite	customera.com
From	IP/Domain	Overwrite	customera.com
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Overwrite	customera.com
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

9.3.8. Topology Hiding – AT&T Side

Step 1 - Repeat the steps in **Section 9.3.7,** with the following changes:

- Enter Profile Name: (e.g., **ATT_TH**).
- Leave all values at default.



Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

9.3.9. Signaling Manipulations

The Avaya SBCE can manipulate inbound and outbound SIP headers. In the reference configuration the following signaling manipulation scripts are used:

- To add the Diversion header for Experience Portal (see **Section 2.2**, **Item 7**).
- To remove the *SendOnly* parameter sent by Communication Manager in a ReInvite (to signal a Hold state), causing the IPFR_EF service to respond with SendRecv in their 200OK response (see **Section 2.2**, **Item 6a**).

Note – This issue was fixed by the IPFR-EH network on 7/13/14 (see **Section 2.2**, **Item 6b**). Therefore, this signaling manipulation is no longer required, however it is included below for informational purposes.

- To remove *Remote-Address* headers sent by the Avaya SBCE, (see **Section 2.2**, **Item 2**).
- To add the *ptime=30* parameter to the *maxptime=30* parameter sent by AT&T (see **Section 2.2**, **Item 5**).

Note – The use of Signaling Manipulation scripts demands higher processing requirements. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 9.4.3**) does not meet the desired result. Refer to **[12]** for information on the Avaya SBCE scripting language.

9.3.9.1 Add Diversion Header

This script is applied to the **SM_Trunk_SC** Server Configuration in **Section 9.3.5**.
Step 1 - Select **Global Profiles → Signaling Manipulation** from the left hand menu (not shown).
Step 2 - Click **Add Script** (not shown) and the script editor window will open.
Step 3 - Enter a script name in the **Title** box (e.g., **CPE_EP_Diversion_Sendonly**). The following script is defined. Note that AT&T requires that an IPFR-EF DID number assigned to the CPE, is specified in the Diversion header. In this example **7325553170** is used:

- User field = An IPFR-EF telephone number assigned to the CPE, (e.g., **7325553170**).
- Host field = The public (B1) IP address of the Avaya SBCE, (e.g., **10.10.10.12**).

Title: CPE_EP_Diversion_Sendonly

```
//Add diversion header to EP redirect call. Add to CPE side.

within session "INVITE"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
   {

    if(exists(%HEADERS["Diversion"][1]))then
    {
      %var="Diversion exists";
    }
      else
    {
     %HEADERS["Diversion"][1] = "sip:7327373170@";
     append(%HEADERS["Diversion"][1], "10.10.10.12");
    }
  }
}

```

Step 4 – Leaving the editor window open, proceed to **Section 9.3.9.2**.

9.3.9.2 Remove the SendOnly Parameter

Note – This issue was fixed by the IPFR-EH network on 7/13/14 (see **Section 2.2**, **Item 6b**). Therefore, this signaling manipulation is no longer required, however it is included below for informational purposes.

This script is also applied to the **SM_Trunk_SC** Server Configuration in **Section 9.3.5**.
Step 1 – Continuing with the script editor from **Section 9.3.9.1** above, enter the additional script parameters highlighted below, then click on **Save**. The script editor will test for any errors, and the window will close.

Title CPE_EP_Diversion_Sendonly Save

```
//Add diversion header to EP redirect call. Add to CPE side.

within session "INVITE"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
   {

    if(exists(%HEADERS["Diversion"][1]))then
    {
      %var="Diversion exists";
    }
      else
    {
     %HEADERS["Diversion"][1] = "sip:7327373170@";
     append(%HEADERS["Diversion"][1], "10.10.10.12");
    }
  }
}


//Remove SendOnly due to AT&T Inactive response (E-IPFR). Apply to CPE side.

within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
        if(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]="") then
        {
            remove(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]);
        }
  }
}

within session "ALL"
{
  act on response where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
        if(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]="") then
        {
            remove(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]);
        }
  }
}
```

9.3.9.3 Remove Remote-Address header

Note – **Steps 1-3** are *not* required if Avaya SBCE load **Q16** is used.

This script is applied to the **ATT_SC** Server Configuration in **Section 9.3.6**.
Step 1 - Select **Global Profiles → Signaling Manipulation** from the left hand menu (not shown).
Step 2 - Click **Add Script** (not shown) and the script editor window will open.
Step 3 - Enter a script name in the **Title** box (e.g., **Remote_Address_and_Ptime**). The following script is defined:

Title ATT_Remote_Addr_EP_Ptime

```
// Remove Remote-Address header added by SBCE. Apply to AT&T side.

within session "ALL"
  {
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
      {
        remove(%HEADERS["Remote-Address"][1]);
      }
  }
```

Step 4 – Leaving the editor window open, proceed to **Section 9.3.9.4**.

9.3.9.4 Add Ptime=30 to Maxptime=30

Note – If the script specified in **Section 9.3.9.3** is not required, then only the script below is applied to the **ATT_SC** Server Configuration in **Section 9.3.6**.

Step 1 – Continuing with the script editor from **Section 9.3.9.3** above, enter the following, then click on **Save**. The script editor will test for any errors, and the window will close.

Title ATT_Remote_Addr_EP_Ptime Save

```
// Remove Remote-Address header added by SBCE. Apply to AT&T side.

within session "ALL"
  {
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
      {
        remove(%HEADERS["Remote-Address"][1]);
      }
  }


//Add ptime:30 to AT&T maxptime:30 in calls to EP

within session "ALL"
{

  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"

  {

      %SDP[1]["s"]["m"][1].ATTRIBUTES["ptime"][1]="30";

  }
}
```

9.4. Domain Policies

The Domain Policies feature allows users to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

9.4.1. Application Rules

Step 1 - Select **Domain Policies → Application Rules** from the menu on the left-hand side (not shown).

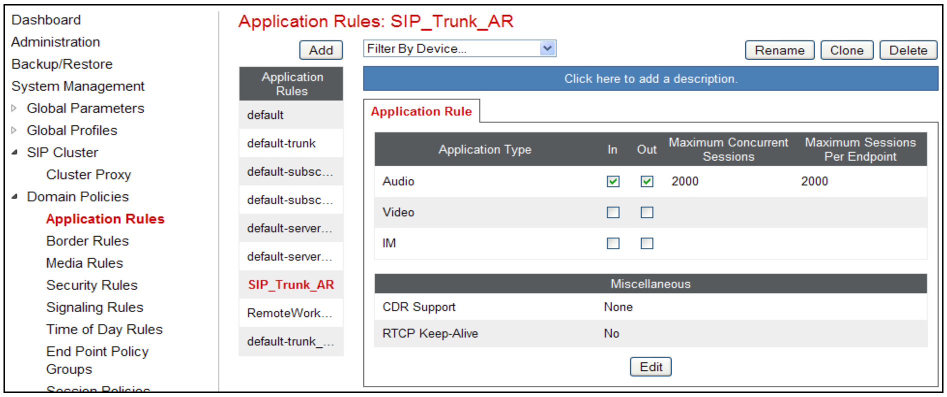
Step 2 - Select the **default** Rule (not shown).

Step 3 - Select the **Clone** button (not shown), and the **Clone Rule** window will open.

- In the **Clone Name** field enter **SIP_Trunk_AR**
- Click **Finish.**

Step 4 - Select the **SIP_Trunk_AR** rule just created (not shown).

- Click the **Edit** button. The **Editing Rule** screen will be displayed.
- In the **Voice** row:
  - Change the **Maximum Concurrent Sessions** to **2000**
  - Change the **Maximum Sessions per Endpoint** to **2000**
- Click on **Finish.**



9.4.2. Media Rules

The following Media Rule will be applied to both the Avaya and AT&T connections and therefore, only one rule is needed.

Step 1 - Select **Domain Policies → Media Rules** from the menu on the left-hand side menu (not shown).

Step 2 - The Media Rules window will open (not shown). From the Media Rules menu, select the **default-low-med** rule

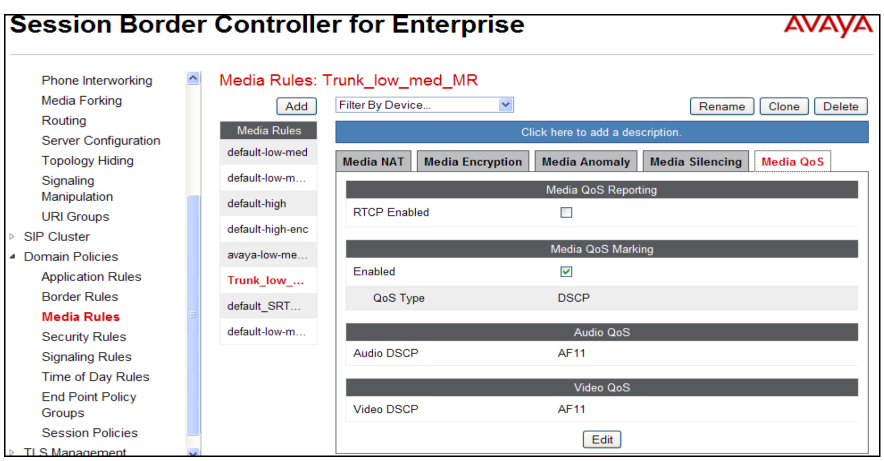
Step 3 - Select **Clone** button (not shown), and the **Clone Rule** window will open.

- In the **Clone Name** field enter **Trunk_low_med_MR**
- Click **Finish.** The newly created rule will be displayed.

Step 4 - Highlight the **Trunk-low-med_MR** rule just created (not shown):

- Select the **Media QOS** tab.
- Click the **Edit** button and the **Media QOS** window will open.
- Check the **Media QOS Marking** field is **Enabled.**
- Select the **DSCP** box.
- **Audio**: Select **AF11** from the drop-down.
- **Video**: Select **AF11** from the drop-down.

Step 5 - Click **Finish.** The completed **Media Rules** screen is shown below.



9.4.3. Signaling Rules

In the reference configuration, Signaling Rules are used to define QOS parameters, as well as to remove unwanted SIP headers (see **Section 2.2, Item 1**).

Note – SIP headers may also be blocked by the Signaling Manipulation function (see **Section 9.3.9**). However, Signaling Rules are a more efficient use of Avaya SBCE resources.

9.4.3.1 Avaya – Signaling QOS

Step 1 - Select **Domain Policies → Signaling Rules** from the menu on the left-hand side menu (not shown).

Step 2 - The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.

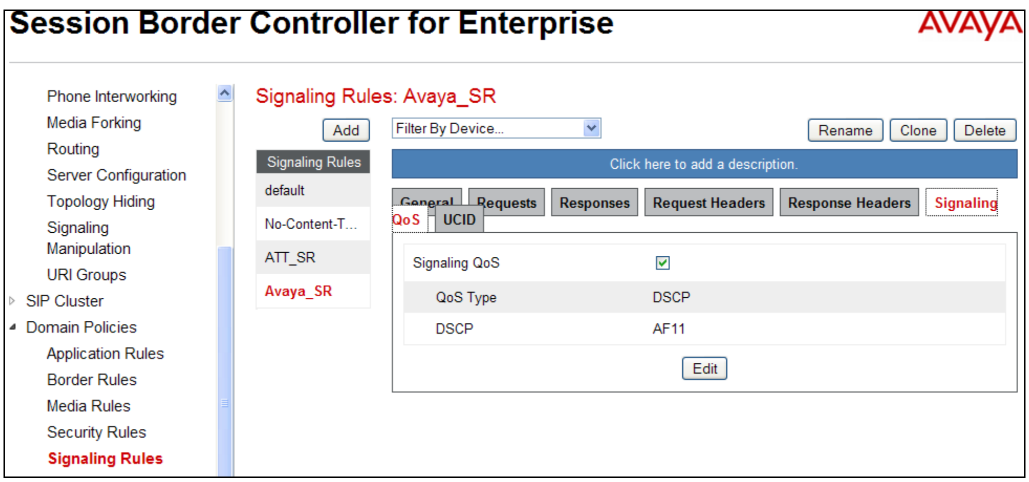
Step 3 - Select the **Clone** button and the **Clone Rule** window will open (not shown).

- In the **Rule Name** field enter **Avaya_SR**
- Click **Finish.** The newly created rule will be displayed.

Step 4 - Highlight the **Avaya_SR** rule created in step **4** and enter the following:

- Select the **Signaling QOS** tab.
- Click the **Edit** button and the **Signaling QOS** window will open.
- Verify that **Signaling QOS** is selected.
- Select **DCSP**.
- Select **Value** = **AF11**.

Step 5 - Click **Finish.** The completed **Signaling Rules** screen is shown below.



9.4.3.2 AT&T – Signaling QOS Tab

Step 1 - Repeat the steps in **Section 9.4.3.1**, with the following changes:

- After cloning the **default** rule (not shown), name the rule**: ATT_SR**
- Specify the same parameters used in **Section 9.4.3.1**.

9.4.3.3 Avaya – Request Headers Tab – Removal of Unwanted SIP Headers

The following Signaling Rules remove SIP Request headers (e.g., Invites) sent by Communication Manager, (or other components of the CPE), that are either not supported or required by AT&T, or headers that may contain internal CPE information.

Note – In configurations that include Avaya Aura® Session Manager, History-Info headers are removed by Session Manager (see **Section 4.3**). Alternatively they may be removed by Communication Manager (see **Section 5.8**), or removed here.

Use the following steps to remove the **P-Location** header from Invites:

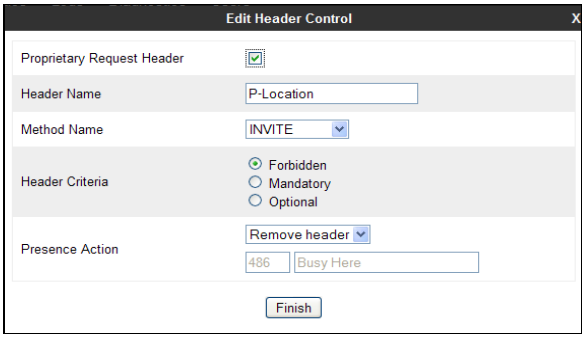
Step 1 - Select **Domain Policies** from the menu on the left-hand side menu (not shown).
Step 2 - Select **Signaling Rules** (not shown).
Step 3 - From the Signaling Rules menu, select the **default** rule.
Step 4 - Select **Clone Rule** button

- Enter a name**: Avaya_SR**
- Click **Finish**

Step 5 - Highlight and edit the **Avaya_SR** rule created in **Step 4** and enter the following:

- Select the **Add In Header Control** button (not shown). The Add Header Control window will open.
- Select the **Request Headers** tab (not shown).
- Click the **Edit** button and the **Edit Header Control** window will open.
- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **P-Location**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.

Step 6 - Click **Finish**



Step 7 - Repeat **Steps 5** through **6** to create a rule to remove the **P-Location** header from ACKs.

- Verify the **Proprietary Request Header** box is *checked*.
- From the **Header Name** menu select **Alert-Info**
- From the **Method Name** menu select **Ack**.

Step 8 - Repeat **Steps 5** through **6** to create a rule to remove the **Alert-Info** header.

- Verify the **Proprietary Request Header** box is *unchecked*.
- From the **Header Name** menu select **Alert-Info**

Step 9 - Repeat **Steps 5** through **6** to create a rule to remove the **Endpoint-View** header.

- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **Endpoint-View.**

Step 10 - Repeat **Steps 5** through **6** to create a rule to remove the **AV-Correlation-ID** header.

- Check the **Proprietary Request Header** box.
- In the **Header Name** field enter **AV-Correlation-ID**.

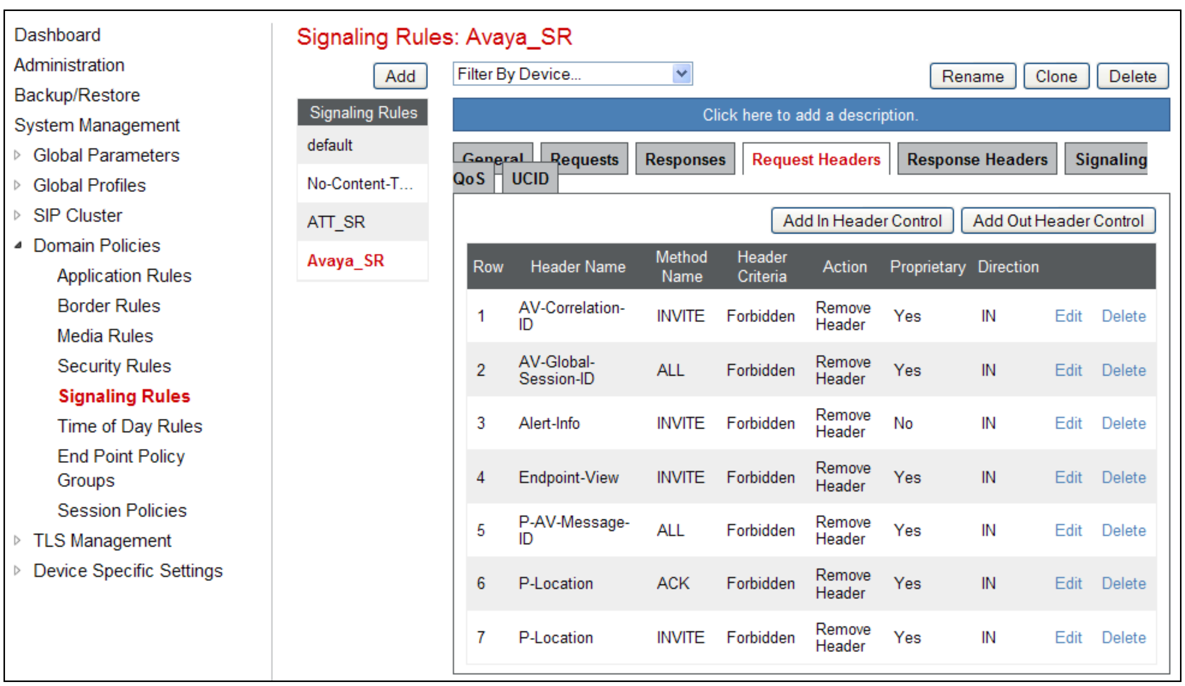
Step 11 - Repeat **Steps 5** through **6** to create a rule to remove the **AV-Global-Session-ID** header.

- Check the **Proprietary Request Header** box.
- In the **Header Name** field enter **AV-Global-Session-ID**
- From the **Method Name** menu select **ALL**.

Step 12 - Repeat **Steps 5** through **6** to create a rule to remove the P-**AV-Message-ID** header.

- In the **Header Name** field enter P-**AV-Message-ID**
- From the **Method Name** menu select **ALL**.

The completed **Request Headers** form is shown below. Note that the **Direction** column says **IN**.



9.4.3.4 Avaya – Response Headers Tab – Removal of Unwanted SIP Headers

The following Signaling Rules remove SIP Response headers (e.g., 1xx and/or 200ok) sent by Communication Manager, that are either not supported or required by AT&T, or are headers that may contain internal CPE information.

Step 1 - Highlight the **Avaya_SR** rule created in **Section 9.4.3.1**, and using the same procedures shown in **Section 9.4.3.3**, remove the **P-Location** header from **1xx** responses:

- Select the **Response Headers** tab (not shown).
- Check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **P-Location**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **Invite**.
- For **Header Criteria** select **Forbidden**.
- From the **Presence Action** menu select **Remove Header**.
- Click **Finish**

Step 2 - Repeat **Step 1** to create a rule to remove the **P-Location** header from **2xx** responses.

- From the **Response Code** menu select **2xx**.

Step 3 - Repeat **Step 1** to create a rule to remove the **Endpoint-View** header from **1xx** responses.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Response Code** menu select **1xx**.

Step 4 - Repeat **Step 3** to remove **Endpoint-View** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

Step 5 - Repeat **Step 1** to create a rule to remove the P-**AV-Message-ID** header from **1xx** responses.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **ALL**.

Step 6 - Repeat **Step 5** to remove P-**AV-Message-ID** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

Step 7 - Repeat **Step 1** to create a rule to remove the **AV-Global-Session-ID** header from **1xx** responses.

- In the **Header Name** field, enter **Endpoint-View**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **ALL**.

Step 8 - Repeat **Step 7** to remove **AV-Global-Session-ID** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

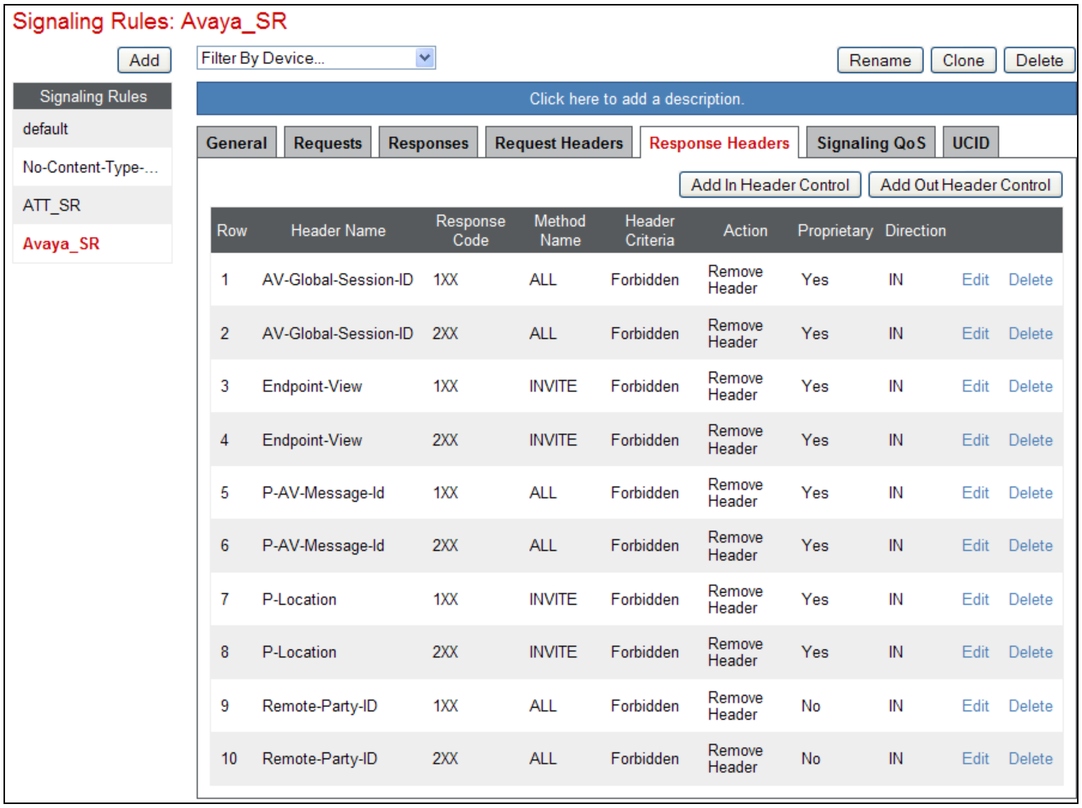
Step 9 - Repeat **Step 1** to remove **Remote-Party-ID** headers from **1xx** and **2xx** responses.

- *Do not* check the **Proprietary Request Header** box.
- In the **Header Name** field, enter **Remote-Party-ID**.
- From the **Response Code** menu select **1xx**.
- From the **Method Name** menu select **ALL**.

Step 10- Repeat **Step 9** to remove **Remote-Party-ID** headers from **2xx** responses.

- From the **Response Code** menu select **2xx**.

The completed **Response Headers** form is shown below. Note that the **Direction** column says **IN**.



Signaling Rules: Avaya_SR

Add | Filter By Device... | Rename | Clone | Delete

Signaling Rules: default, No-Content-Type-..., ATT_SR, Avaya_SR

Click here to add a description.

General | Requests | Responses | Request Headers | Response Headers | Signaling QoS | UCID

Add In Header Control | Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Endpoint-View	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Location	2XX	INVITE	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	Remote-Party-ID	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
10	Remote-Party-ID	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

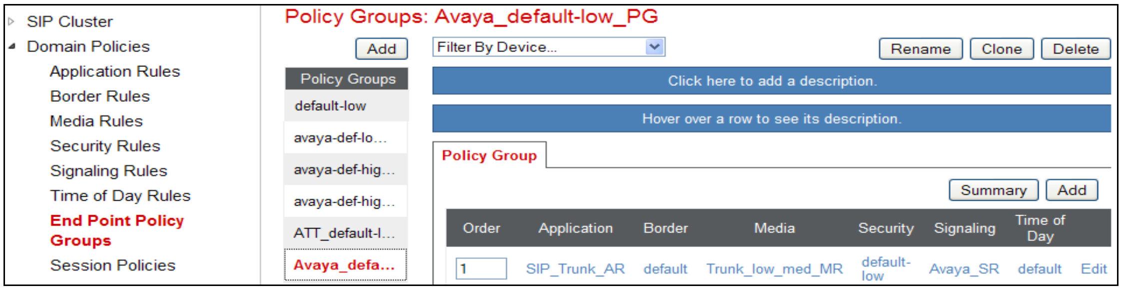
9.4.4. Endpoint Policy Groups – Avaya Connection

Step 1 - Select **Domain Policies → End Point Policy Groups** from the menu on the left-hand side (not shown).

Step 2 - Select **Add Group**, and enter the following:

- **Name**: **Avaya_default-low_PG**
- **Application Rule**: **SIP_Trunk_AR** (created in **Section 9.4.1**)
- **Border Rule**: **default**
- **Media Rule**: **Trunk_low_med_MR** (created in **Section 9.4.2**)
- **Security Rule**: **default-low**
- **Signaling Rule**: **Avaya_SR** (created in **Section 9.4.3**)
- **Time of Day**: **default**

Step 3 - Select **Finish** (not shown)

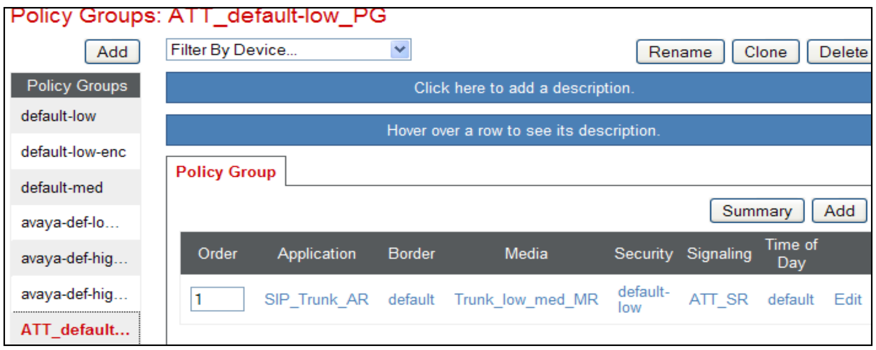


9.4.5. Endpoint Policy Groups – AT&T Connection

Step 1 - Repeat steps **1** through **4** from **Section 9.4.4** with the following changes:

- **Group Name**: **ATT_default-low_PG**
- **Signaling Rule**: **ATT_SR** (created in **Section 9.4.3)**

Step 2 - **Select Finish** (not shown)

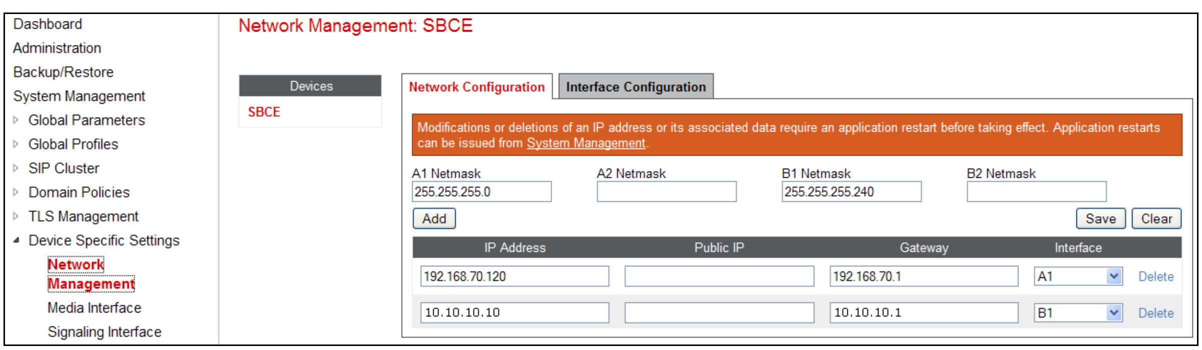


9.5. Device Specific Settings

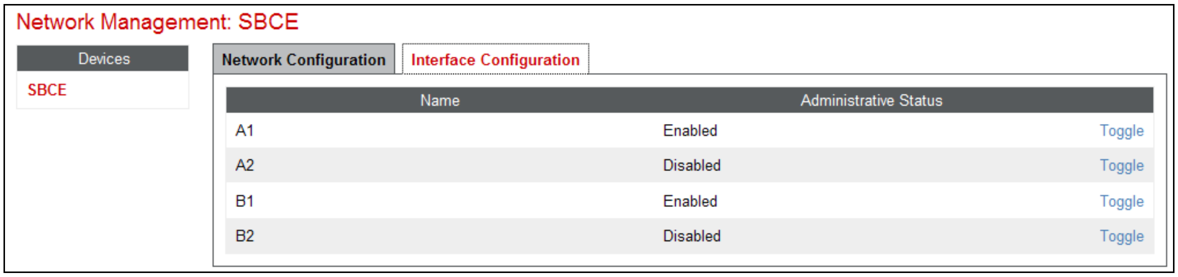
9.5.1. Network Management

Step 1 - Select **Device Specific Settings** from the menu on the left-hand side

Step 2 - Select **Network Management** and the **Network Configuration** tab. The network interfaces are defined during installation. However they may be modified, via this tab.



Step 3 - In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab (note that the A2 and B2 interfaces are not supported at this time).



9.5.2. Advanced Options

In **Section 9.5.3**, the media UDP port ranges required by AT&T are set (**16384 – 32767**). By default part of this range is already allocated by the Avaya SBCE for internal use (22000 - 31000). The following steps reallocate the port ranges used by the Avaya SBCE so the range required by AT&T can be used.

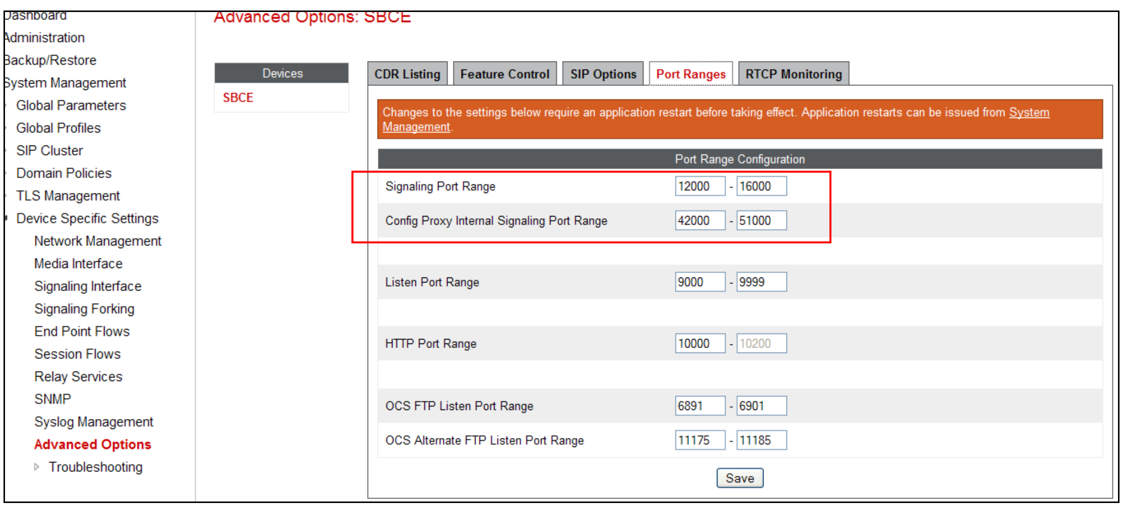
Step 1 - Select **Device Specific Settings → Advanced Options** from the menu on the left-hand side (not shown).

Step 2 - Select the **Port Ranges** tab.

Step 3 – In the **Signaling Port Range** row, change the range to **12000 – 16000**.

Step 4 - In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.

Step 5- Scroll to the bottom of the window and select **Save** (not shown).



9.5.3. Media Interfaces

The AT&T IPFR-EF service specifies that customers use RTP ports in the range of **16384 – 32767**. Both inside and outside ports have been changed to this range, but only the outside is required by the AT&T IPFR-EF service.

Step 1 - Select **Device Specific Settings → Media Interface** from the menu on the left-hand side (not shown).

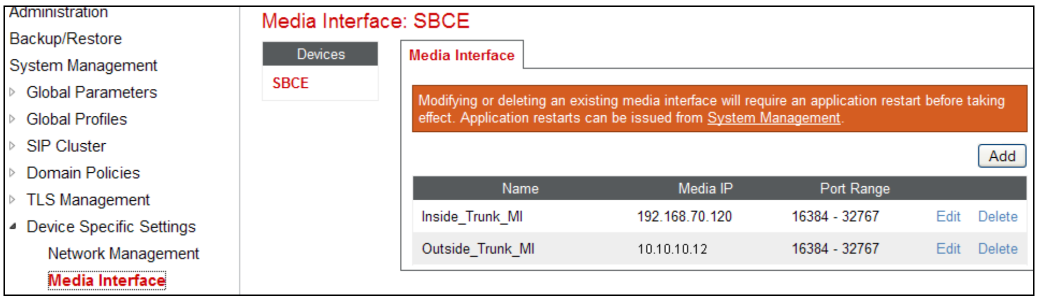
Step 2 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: **Inside_Trunk_MI**
- **IP Adrress**: **192.168.70.120** (Avaya SBCE A1 address)
- **Port Range**: **16384 - 32767**

Step 3 - Click **Finish** (not shown).
Step 4 - Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name**: **Outside_Trunk_MI**
- **IP Address**: **10.10.10.12** (Avaya SBCE B1 address)
- **Port Range**: **16384 - 32767**

Step 5 - Click **Finish** (not shown).



9.5.4. Signaling Interface

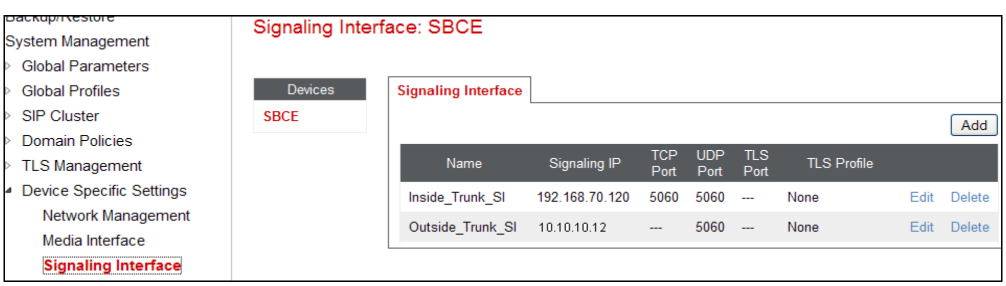
Step 1 - Select **Device Specific Settings → Signaling Interface** from the menu on the left-hand side (not shown).
Step 2 - Select **Add** (not shown) and enter the following:

- **Name**: **Inside_Trunk_SI**
- **IP Address**: **192.168.70.120** (Avaya SBCE A1 address)
- **TCP Port**: **5060**

Step 3 - Click **Finish** (not shown).
Step 4 - Select **Add** again, and enter the following:

- **Name**: **Outside_Trunk_SI**
- **IP Address**: **10.10.10.12** (Avaya SBCE B1 address)
- **UDP Port**: **5060**

Step 5 - Click **Finish** (not shown).



9.5.5. Endpoint Flows – Avaya

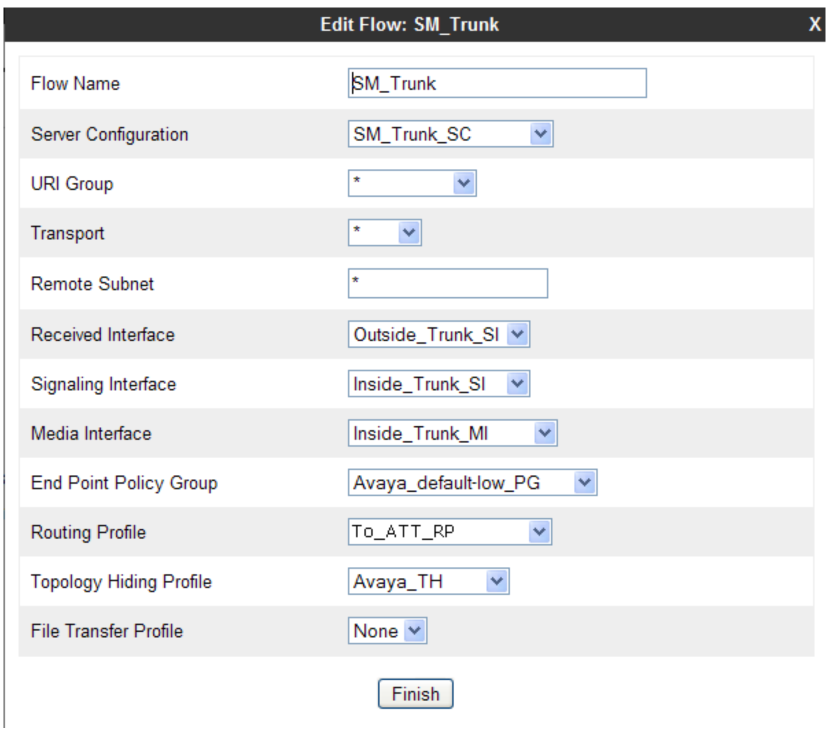
Step 1 - Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).

Step 2 - Select the **Server Flows** tab (not shown).

Step 3 - Select **Add**, (not shown) and enter the following:

- **Name**: **SM_Trunk**
- **Server Configuration**: **SM_Trunk_SC** (**Section 9.3.5**)
- **URI Group**: *
- **Transport**: *
- **Remote Subnet**: *
- **Received Interface**: **Outside_Trunk_SI (Section 9.5.4)**
- **Signaling Interface**: **Inside_Trunk_SI** (**Section 9.5.4**)
- **Media Interface**: **Inside_Trunk_MI** (**Section 9.5.3**)
- **End Point Policy Group**: **Avaya_default-low_PG** (**Section 9.4.4**)
- **Routing Profile**: **To_ATT _RP** (**Section 9.3.4**)
- **Topology Hiding Profile**: **Avaya_TH** (**Section 9.3.7**)
- **File Transfer Profile**: **None**

Step 4 - Click **Finish**.

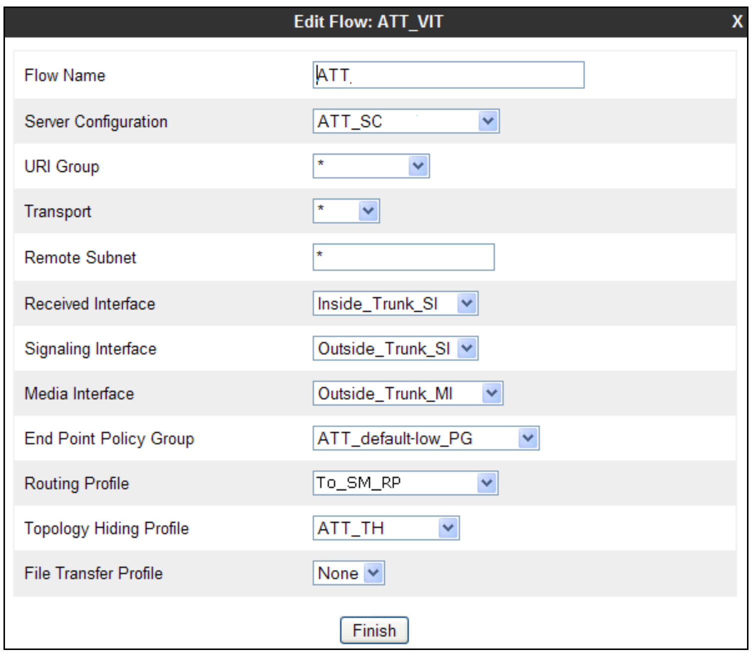


9.5.6. Endpoint Flows – AT&T

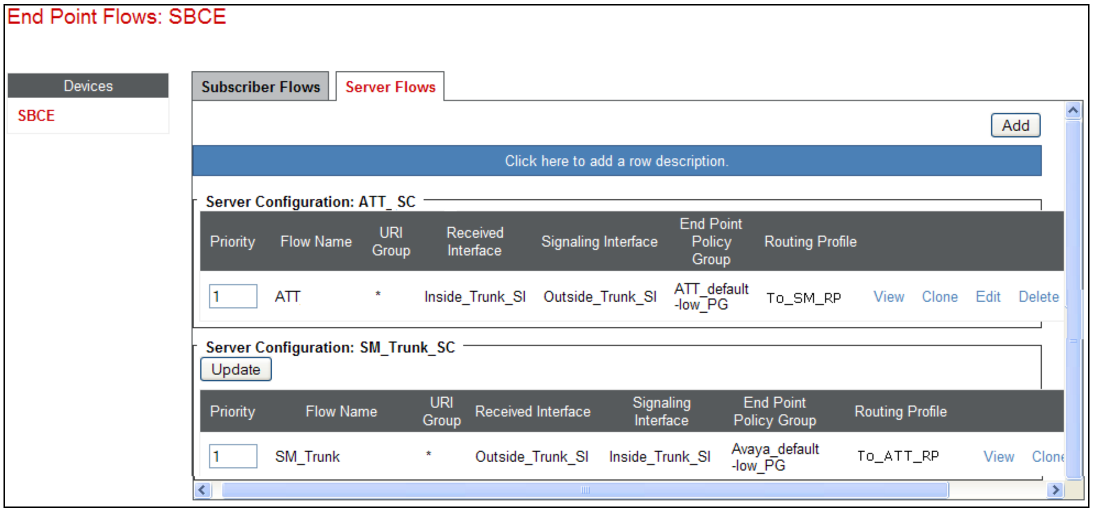
Step 1 - Repeat steps **1** through **4** from **Section 9.5.5**, with the following changes:

- **Name**: **ATT**
- **Server Configuration**: **ATT_ SC** (**Section 9.3.6**).
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Inside_Trunk_SI** (**Section 9.5.4**).
- **Signaling Interface**: **Outside_Trunk_SI (Section 9.5.4**).
- **Media Interface**: **Outside_Trunk_MI** (**Section 9.5.3**).
- **End Point Policy Group**: **ATT_default-low_PG** (**Section 9.4.5**).
- **Routing Profile**: **To_SM_RP (Section 9.3.3**).
- **Topology Hiding Profile**: **ATT_TH** (**Section 9.3.8**).
- **File Transfer Profile**: **None**

Step 2 - Click **Finish**.



The completed **End Point Flows** screen is shown below.



10. Verification Steps

The following steps may be used to verify the call flow via the reference configuration:

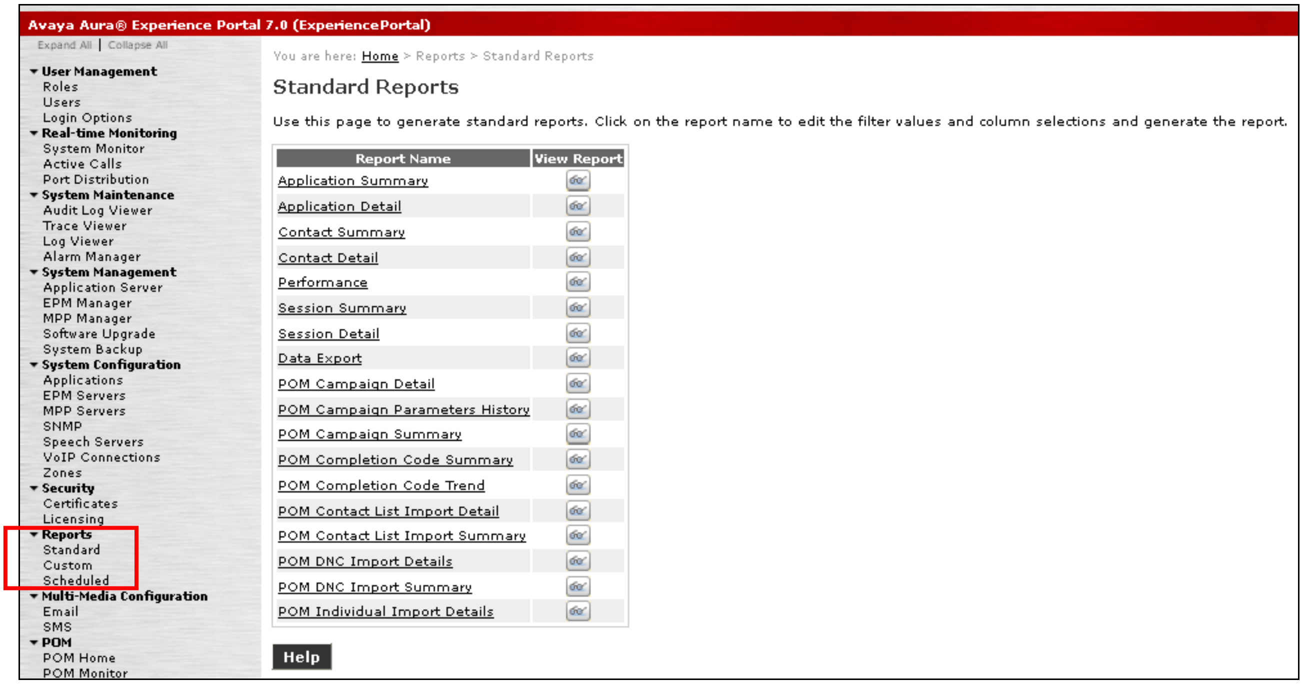
10.1. Telephony

1. Place an inbound call to Experience Portal application, verify the use of DTMF signaling and verify that two-way talkpath exists. Interact with the Experience Portal prompts and verify that the call remains stable for several minutes and disconnect properly.
2. Place an inbound call to Experience Portal application, verify the use of DTMF signaling and verify that the call is successfully transferred to a Communication Manager Agent and two-way talkpath exists between the caller and the Agent. Verify that the calls remain stable for several minutes and disconnect properly.
3. Verify that Refer call processing between Experience Portal and the Avaya SBCE, or Refer processing between Experience Portal and the IPFR-EF service, performs correctly[8].
4. Verify basic call functions such as hold, transfer, and conference.
5. Place an inbound call to an enterprise Agent station, but do not answer the call. Verify that the call covers to Avaya Aura® Messaging voicemail. Retrieve the message from Avaya Aura® Messaging either locally or from PSTN.

[8] See **Section 2.2, Item 4**

10.2. Experience Portal

Reports may be generated by Experience Portal to show status of Applications, Sessions, etc. In addition, status of Proactive Outreach Manager (POM) campaigns may be displayed as well.



10.3. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See **[7]** for more information.

SIP trunk activity may be monitored by selecting a Trunk Access Code (TAC) associated with a particular SIP trunk. In the reference configuration the SIP trunk used for AT&T access is trunk 2 (see **Section 5.8.1**). This trunk is assigned TAC code 602.

- From the Communication Manager console connection enter the command ***list trace tac xxx***, where ***xxx*** is a trunk access code defined for the SIP trunk to AT&T (e.g., 602). Then place the inbound call. The sample output is shown below.

  Note that Session Manager has already converted the IPFR-EF DNIS number specified in the AT&T Invite Request URI, to the Communication Manager extension 19001, before sending the Invite to Communication Manager.

- Similar Communication Manager call status commands are, ***list trace station x***, ***list trace vdn x***, and ***list trace vector x***. Other useful commands are ***status trunk x*** and ***status station x***.

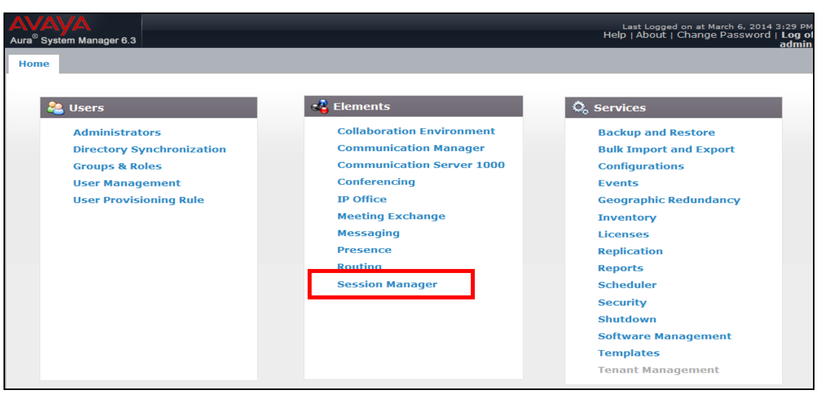
```
list trace tac 602                                                   Page    1
                                LIST TRACE
time            data

15:55:06 TRACE STARTED 04/19/2013 CM Release String cold-02.0.823.0-20396
15:55:16 SIP<INVITE sip:19001@customera.com SIP/2.0
15:55:16     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16     7ok0
15:55:16     active trunk-group 2 member 1    cid 0x2e9
15:55:16 SIP>SIP/2.0 180 Ringing
15:55:16     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:16     7ok0
15:55:16     dial 19001
15:55:16     ring station      19001 cid 0x2e9
15:55:16     G711MU ss:off ps:20
             rgn:1 [192.168.67.75]:18828
             rgn:1 [192.168.67.50]:16388
15:55:16     G729B ss:off ps:30
             rgn:2 [192.168.67.120]:16388
             rgn:1 [192.168.67.50]:16392
15:55:16     xoip options: fax:T38 modem:off tty:US  uid:0x5000b
             xoip ip: [192.168.67.50]:16392
15:55:18 SIP>SIP/2.0 200 OK
15:55:18     active station      19001 cid 0x2e9
15:55:18 SIP<ACK sip:7327373940@192.168.67.202:5062;transport=tcp SI
15:55:18 SIP>INVITE sip:192.168.67.120:5060;transport=tcp;gsid=14e31
15:55:18 SIP<SIP/2.0 100 Trying
15:55:18 SIP<SIP/2.0 200 OK
15:55:18 SIP>ACK sip:192.168.67.120:5060;transport=tcp;gsid=14e31350
```

10.4. Avaya Aura® Session Manager

The Main and Branch Session Manager configurations may be verified via System Manager.

10.4.1. Session Manager Status

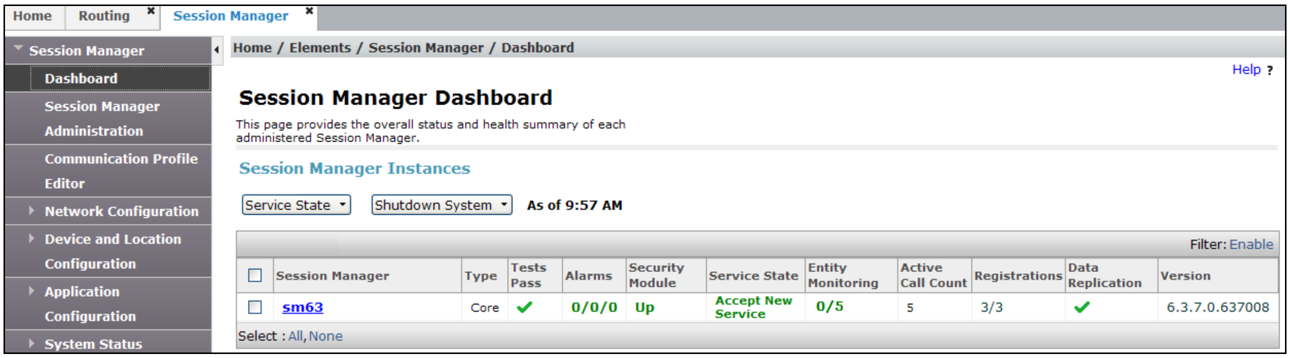
Step 1 – Using the procedures described in **Section 4**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



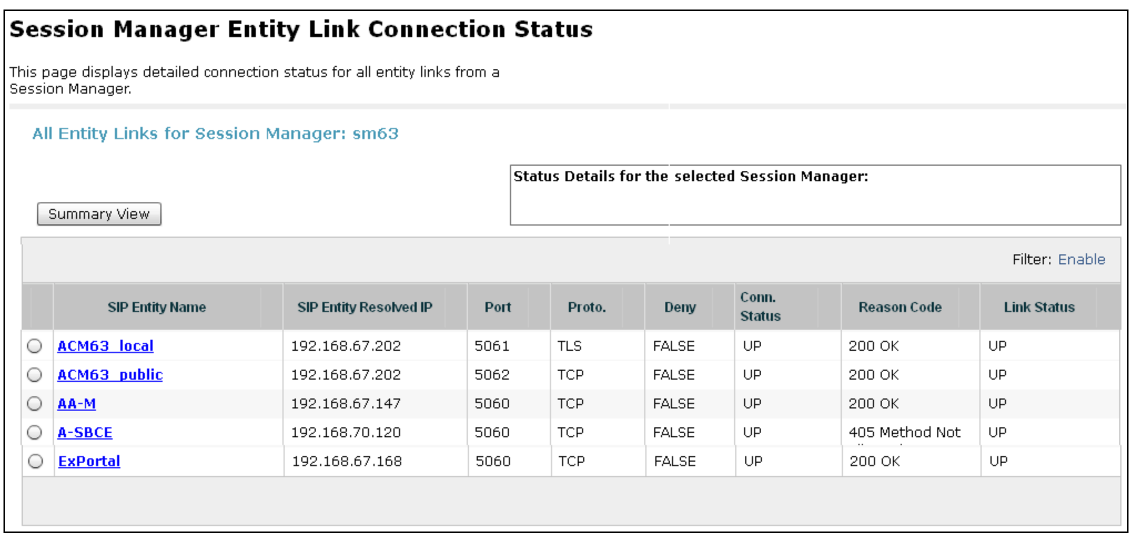
Step 2 – The Session Manager Dashboard is displayed. In the example below, Session Manager instance **sm63** is displayed.

Note that for Session Manager **sm63**, the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status.

In the **Entity Monitoring Column**, the Session Manager **sm63** shows that there are **0** (zero) alarms out of the **3** Entities defined.



Step 3 - Clicking on the **0/5** entry in the **Entity Monitoring** column for Session Manager **sm63**, results in the following display.



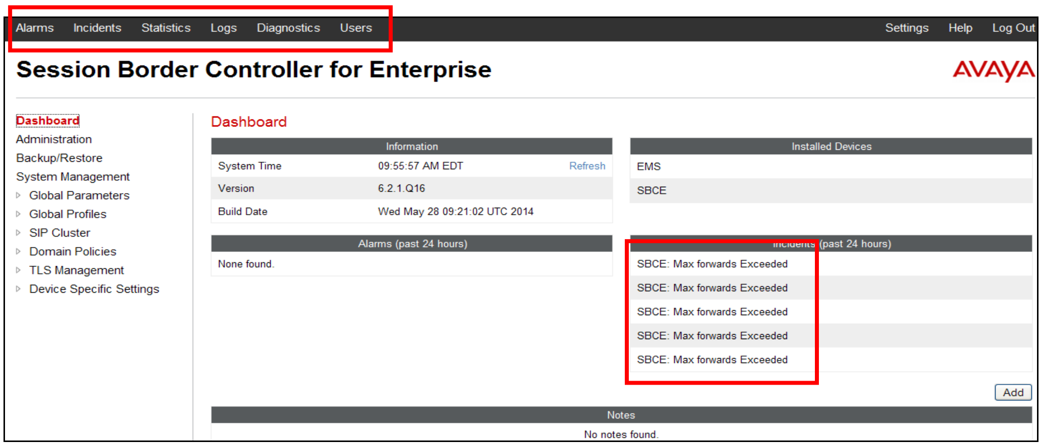
Note - The **A-SBCE** Entity **Reason Code** column indicates that Session Manager has received a SIP **405 Method Not Allowed** response to the SIP OPTIONS it has sent to the Avaya SBCE. The Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T Border Element. It is the AT&T Border Element that is generating the 405, which the Avaya SBCE sends back to Session Manager. This AT&T response is normal in the reference configuration test environment, and is sufficient for SIP Link Monitoring to consider the link up.

11. Avaya Session Border Controller for Enterprise

11.1. System Status

Various system conditions monitored by the Avaya SBCE may be displayed as follows.

Step 1 – Log into the Avaya SBCE as shown in **Section 9.2**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.



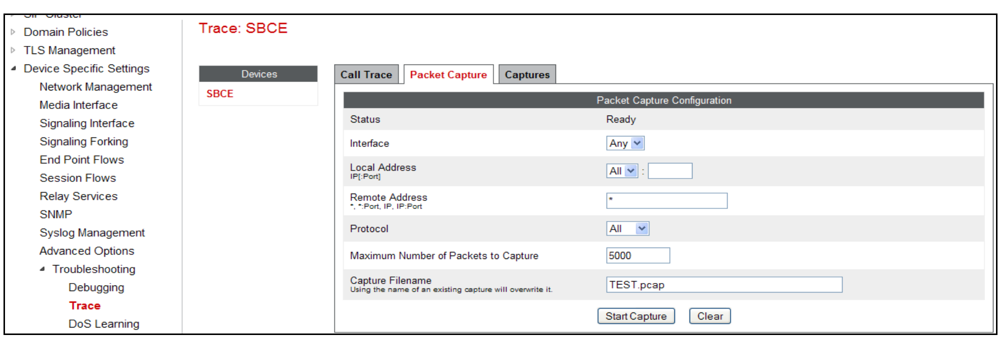
11.2. Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

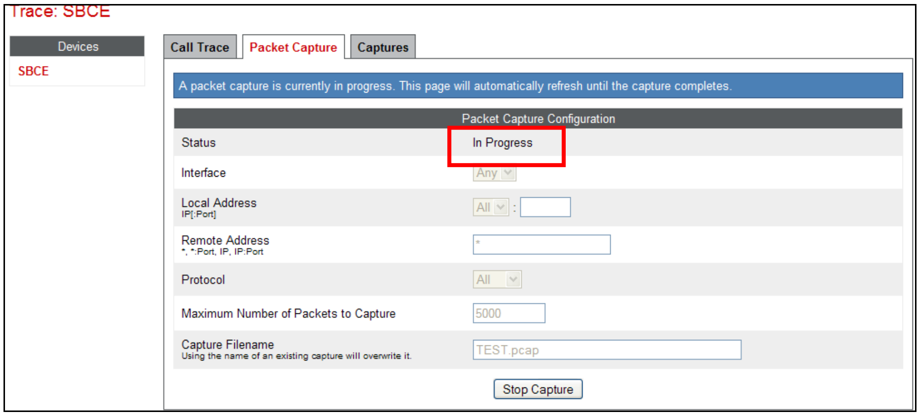
Step 1 - Navigate to UC-Sec Control Centre → Troubleshooting → Trace Settings

Step 2 - Select the **Packet Capture** tab and select the following:

- Select the desired **Interface** from the drop down menu. Selecting **Any** will result in a trace showing activity on both the A1 (inside) and B1 (outside) interfaces.
- Specify the **Maximum Number of Packets to Capture** (e.g., **5000**). Note that the number specified should be a best guess based on the duration of the test.
- Specify a **Capture Filename**.
- Click **Start Capture** to begin the trace.



The capture process will initialize and then display the following status window. Note that the **Status** will change to **In Progress** when the trace begins, and the screen will begin to refresh.

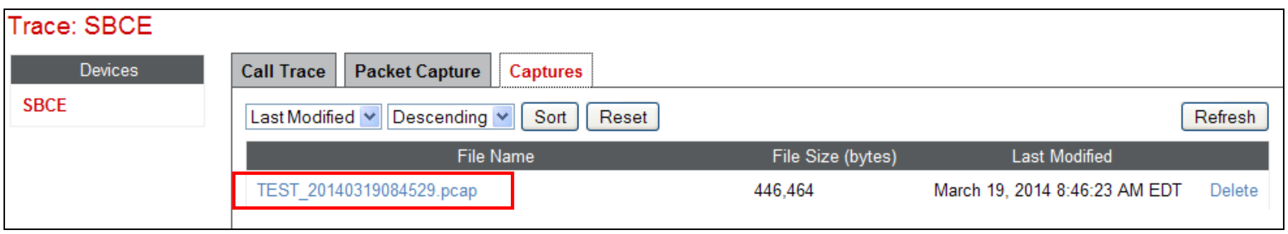


Step 3 – Run the test.

Step 4 – At the conclusion of the test. Select the **Stop Capture** button shown above.

Step 5 - Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.

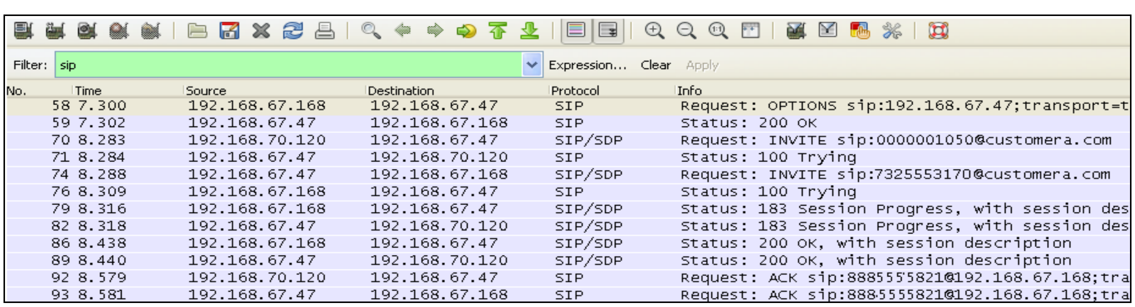
Step 6 - Click on the **File Name** link to download the file and use Wireshark to open the trace.



11.3. SIP Protocol Analyzer Traces

A SIP protocol analyzer (e.g., Wireshark), may be used to monitor the SIP traffic. The following trace sequence was taken at the Session Manager (192.168.67.47) interface, and shows communication between it, the Avaya SBCE (192.168.70.120), and Communication Manager (192.168.67.202). The trace shows an inbound call from the AT&T IPFR-EF service to Experience Portal, and the subsequent redirection of the call (Refer) from Experience Portal to a Communication Manager Agent.

- Frames 70 and 74 show the AT&T Invite path Avaya SBCE → Session Manager → Experience Portal.



- After the caller makes a menu selection, Experience portal sends a Refer to the Avaya SBCE containing the associated Communication Manager Agent/Skill VDN extension 44001 (frames 129 & 130).

93 8.581	192.168.67.47	192.168.67.168	SIP	Request: ACK sip:8885555821@192.168.67.1
129 11.626	192.168.67.168	192.168.67.47	SIP	Request: REFER sip:192.168.70.120:5060;t
130 11.628	192.168.67.47	192.168.70.120	SIP	Request: REFER sip:192.168.70.120:5060;t
131 11.629	192.168.70.120	192.168.67.47	SIP	Status: 202 Accepted
132 11.629	192.168.70.120	192.168.67.47	SIP/sipfrag	Request: NOTIFY sip:8885555821@192.168.6
135 11.631	192.168.67.47	192.168.67.168	SIP	Status: 202 Accepted
137 11.631	192.168.67.47	192.168.67.168	SIP/sipfrag	Request: NOTIFY sip:8885555821@192.168.6
139 11.640	192.168.67.168	192.168.67.47	SIP	Status: 200 OK
141 11.642	192.168.67.47	192.168.70.120	SIP	Status: 200 OK

```
        [Severity level: Note]
        [Group: Undecoded]
 ⊟ Contact: <sip:8885555821@192.168.67.168;transport=tcp>
   ⊟ Contact-URI: sip:8885555821@192.168.67.168;transport=tcp
        Contactt-URI User Part: 8884575821
        Contact-URI Host Part: 192.168.67.168
     Contact parameter: transport=tcp>
   Refer-To: <sip:44001@customera.com;user=phone>
   Content-Length: 0
```

- The Avaya SBCE generates an Invite for 44001 and it is sent from Avaya SBCE → Session Manager →Communication Manager, where the Agent answers the call.

143 11.759	192.168.70.120	192.168.67.47	SIP/SDP	Request: INVITE sip:44001@customera.com;
144 11.761	192.168.67.47	192.168.70.120	SIP	Status: 100 Trying
147 11.764	192.168.67.47	192.168.67.202	SIP/SDP	Request: INVITE sip:44001@customera.com;
150 11.765	192.168.67.202	192.168.67.47	SIP	Status: 100 Trying
155 11.768	192.168.67.202	192.168.67.47	SIP/SDP	Status: 180 Ringing, with session descri
158 11.770	192.168.67.47	192.168.70.120	SIP/SDP	Status: 180 Ringing, with session descri
161 11.771	192.168.70.120	192.168.67.47	SIP/sipfrag	Request: NOTIFY sip:8885555821@192.168.6
162 11.772	192.168.67.47	192.168.67.168	SIP/sipfrag	Request: NOTIFY sip:8885555821@192.168.6
163 11.781	192.168.67.168	192.168.67.47	SIP	Status: 200 OK
165 11.783	192.168.67.47	192.168.70.120	SIP	Status: 200 OK
187 13.738	192.168.67.202	192.168.67.47	SIP/SDP	Status: 200 OK, with session descriptior
191 13.741	192.168.67.47	192.168.70.120	SIP/SDP	Status: 200 OK, with session descriptior

12. Conclusion

As illustrated in these Application Notes, Avaya Experience Portal 7.0, Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, and the Avaya Session Border Controller for Enterprise 6.2.1 can be configured to interoperate successfully with the AT&T IP Flexible Reach - Enhanced Features service, within the limitations described in **Section 2.2**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

13. References

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

Avaya Experience Portal

[1] **Implementing Avaya Aura® Experience Portal on a single server**, Release 7.0, Issue 1, December 2013

[2] **Administering Avaya Aura® Experience Portal**, Release 7.0, Issue 1, December 2013

[3] **Troubleshooting Avaya Aura® Experience Portal**, Release 7.0, Issue 1, December 2013

[4] **Implementing Proactive Outreach Manager**, Release 3.0, Issue 1, February 2014

Avaya Aura® Session Manager/System Manager

[5] **Administering Avaya Aura® Session Manager,** Release 6.3, Issue 3, October 2013

[6] **Administering Avaya Aura® System Manager,** Release 6.3, Issue 3, October 2013

Avaya Aura® Communication Manager

[7] **Administering Avaya Aura® Communication Manager,** Release 6.3, 03-300509, Issue 9, October 2013

[8] **Implementing Avaya Aura® Communication Manager,** Release 6.3, 03-603558, Issue 5, October 2013

[9] **Administration for the Avaya G430 Branch Gateway,** Release 6.203-603228, Issue 3.0, December 2012

[10] ***Programming Call Vectors in Avaya Aura® Call Center***, 6.0, June 2010

Avaya Session Border Controller for Enterprise

[11] **Installing Avaya Session Border Controller for Enterprise,** Release 6.2, Issue 3, June 2013

[12] **Administering Avaya Session Border Controller for Enterprise,** Release 6.2, Issue 2, January 2014

Avaya Aura® Messaging

[13] **Administering Avaya Aura® Messaging**, Release 6.3, Issue 1, March 2014

AT&T IP Flexible Reach-Enhanced Features Service Descriptions:

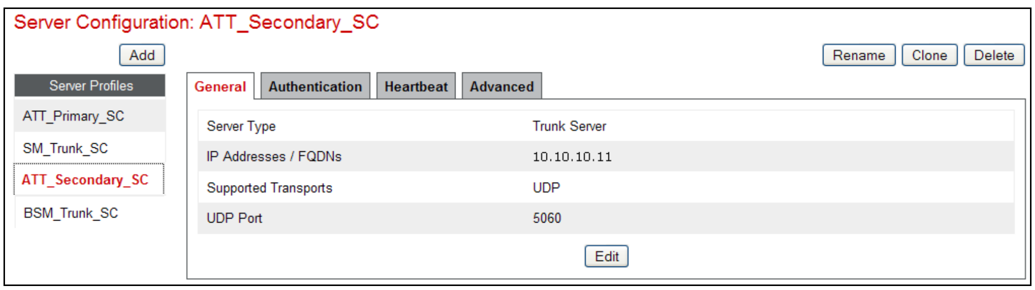
[14] AT&T IP Flexible Reach - Enhanced Features Service description - http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/

14. Addendum 1 – Redundancy to Multiple AT&T Border Elements

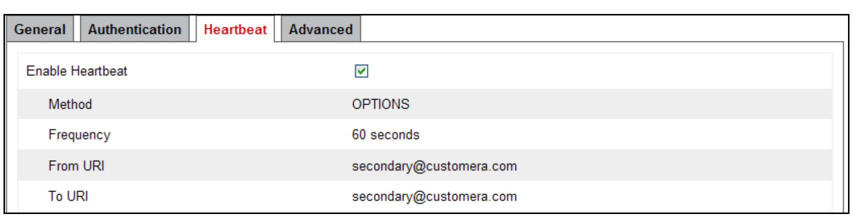
The AT&T IPFR-EF service may provide multiple network Border Elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration. Given two AT&T Border Elements **10.10.10.10** and **10.10.10.11** (see the note in **Section 3.1**) the Avaya SBCE is provisioned as follows to include the secondary trunk connection to 10.10.10.11 (the primary AT&T trunk connection to 10.10.10.10 is defined in **Section 9.3.6**).

14.1. Configure the Secondary Location in Server Configuration

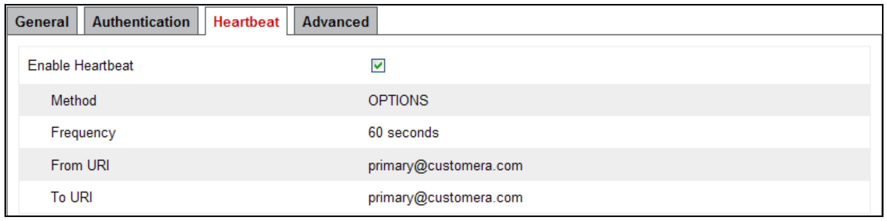
1. Select **Global Profiles → Server Configuration** from the menu on the left (not shown).
2. Select **Add Profile**
    a) **Name: ATT_Secondary_SC**
    b) On the **General** tab , select **Server Type: Trunk Server**
    c) **IP Address: 10.10.10.11** (sample address for a secondary location)
    d) **Supported Transports**: Check **UDP** and **UDP Port: 5060**
    e) Select **Finish** (not shown). The completed **General** tab is shown below.



3. On the **Authentication** tab:
    a) Select **Next** (not shown)
4. On the **Heartbeat** tab:
    a) Check **Enable Heartbeat**
    b) **Method: OPTIONS**
    c) **Frequency:** As desired (e.g., 60 seconds).
    d) **From URI** and **To URI : secondary@customera.com**
    e) Select **Next** (not shown)
5. On the **Advanced** Tab
    a) Click **Finish** (not shown). The completed Heartbeat tab is shown below.

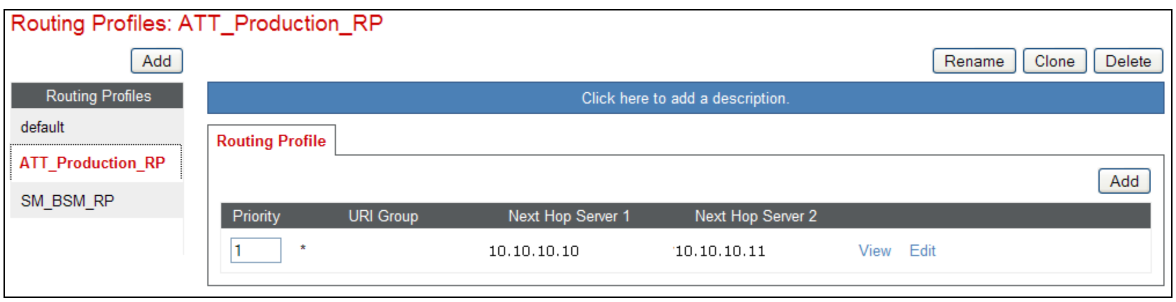


6. Select the **Server Configuration** created in **Section 9.3.6** (e.g., **ATT_Primary_SC**)
7. Select the **Heartbeat Tab** and select **Edit**
8. Repeat **Steps 6 – 7,** using the information shown below, and then click **Finish** (not shown).



14.2. Add Secondary IP Address to Routing

1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Routing**
3. Select the routing profile created in **Section 9.3.4** (e.g., **ATT_Production_RP**)
4. Click the pencil icon at the end of the line to edit (not shown)
    a) Enter the IP Address of the secondary location in the **Next Hop Server 2** (e.g., **10.10.10.11**)
5. Click **Finish** (not shown).

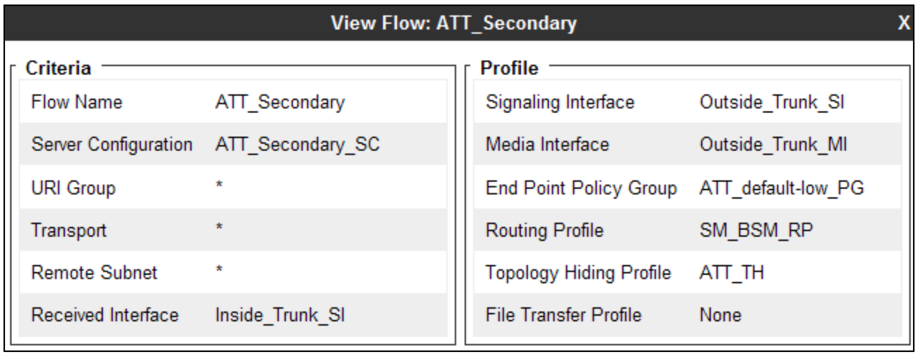


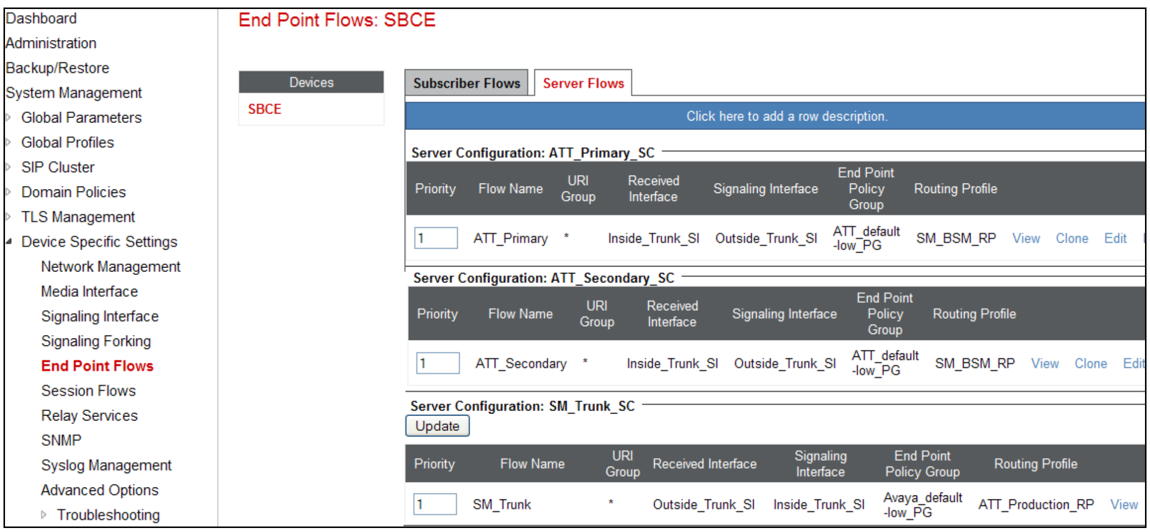
14.3. Configure End Point Flows – Server Flow - ATT_Secondary

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** Tab
4. Select **Add Flow**
    a) **Name: ATT_Secondary**
    b) **Server Configuration: ATT_Secondary _SC**
    c) **URI Group: ***
    d) **Transport: ***
    e) **Remote Subnet: ***
    f) **Received Interface: Inside_Trunk_SI** (**Section 9.5.4**).
    g) **Signaling Interface: Outside_Trunk_ SI** (**Section 9.5.4**).
    h) **Media Interface: Outside_trunk_MI** (**Section 9.5.3**).
    i) **End Point Policy Group**: **ATT_default-low_PG** (**Section 9.4.5**).

j) **Routing Profile: SM_BSM_RP** (**Section 9.3.3**).
k) **Topology Hiding Profile: ATT_TH** (**Section 9.3.8**).
l) **File Transfer Profile: None**

5. Click **Finish** (not shown).





When completed, the Avaya SBCE will issue OPTIONS messages to the primary (10.10.10.10) and secondary (10.10.10.11) Border Elements.

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.