Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the steps for configuring 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 the AT&T IP Flexible Reach - Enhanced Features service, using AT&T's **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Communication Manager/Local Survivable Processor and Avaya Aura® Branch Session Manager are survivable instances of Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Typically, the primary Avaya Aura® Communication Manager and Avaya Aura® Session Manager are located in a central site, with the Avaya Aura® Communication Manager/Local Survivable Processor and Avaya Aura® Branch Session Manager located in a remote location. The Avaya Session Border Controller for Enterprise is the point of connection between both of these sites and the AT&T IP Flexible Reach - Enhanced Features service.

The AT&T Flexible Reach 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 which are not part of IP Flexible Reach service.

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

Table of Contents

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager/Local Survivable Processor 6.3 (LSP), Avaya Aura® Branch Session Manager 6.3 (BSM), and Avaya Session Border Controller for Enterprise 6.2.1(Avaya SBCE), with the AT&T IP Flexible Reach - Enhanced Features service (IPFR-EF), using AT&T's **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Communication Manager/Local Survivable Processor and Avaya Aura® Branch Session Manager are survivable instances of Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

In the reference configuration, the primary Avaya Aura® Communication Manager and Avaya Aura® Session Manager are located in a "Main" site, with the Avaya Aura® Communication Manager/Local Survivable Processor and Avaya Aura® Branch Session Manager located in a remote "Branch" site.

Avaya Aura® System Manager, located in the Common site, is used to provision both the Main and Branch Avaya Aura® Session Manager platforms.

In the reference configuration the Avaya Session Border Controller for Enterprise is the point of connection between both of the Main and Branch sites to the AT&T IP Flexible Reach - Enhanced Features service[1], and is located in a separate "Common" site (as is the AT&T IP Flexible Reach - Enhanced Features service router).

If the Branch site looses connection with the Main site, then the Branch Avaya Aura® Communication Manager/Local Survivable Processor and Avaya Aura® Branch Session Manager will activate, reestablishing telephony and SIP trunk access for the Branch.

For more information on the functions and capabilities of Avaya Aura® Communication Manager see references **[4 & 5]** and for Avaya Aura® Session Manager see **[1]**. For more information on the functions and capabilities of the Avaya Session Border Controller for Enterprise, see **[8 & 9]**.

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 which are not part of IP Flexible Reach service. The AT&T IP Flexible Reach - Enhanced Features service utilizes AT&T's AVPN[2] or MIS/PNT[3] transport services.

[1] See the reference configuration descriptions in Sections 1.1, 2, and 3.
[2] AVPN supports compressed RTP (cRTP).
[3] MIS/PNT does not support cRTP.

1.1. Reference Configuration Considerations

The fail-over testing and configurations described in these application notes were constrained by resource limitations in the test environment (e.g., a single AT&T IP Flexible Reach-Enhanced Features service circuit). In an actual fail-over deployment, a customer would likely have a second AT&T IP Flexible Reach-Enhanced Features service circuit in the Branch location. The presence of this circuit in the Branch would then also require that an Avaya Session Border Controller for Enterprise be located in the Branch as well. In this manner, independent access between the Branch and the AT&T IP Flexible Reach-Enhanced Features service could be obtained. In addition, the AT&T IP Flexible Reach-Enhanced Features service provides an optional redundancy feature called Trunk Call Routing (TCR). Contact your AT&T representative for more information on this option.

Note – This document does not describe Avaya redundancy configurations such as:

- Avaya Enterprise Survivable Servers (ESS).
- Redundant Avaya Aura Session Managers.
- Redundant Avaya Session Border Controller for Enterprise.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise comprised of Main, Branch, and Common locations. The Main site included Session Manager, Communication Manager, and a G430 Media Gateway. The Branch site contains Avaya Aura® Communication Manager/Local Survivable Processor and Avaya Aura® Branch Session Manager, an Avaya G450 Media Gateway, Avaya SIP, H323, and Analog telephones, as well as a fax machine (Ventafax application).
- Voice Directory Numbers (VDN), and associated Vectors provisioned to provide Meet-Me conference capabilities in the Main and Branch sites.
- Avaya System Manager, the Avaya SBCE, as well as to the IPFR-EF service router, are located in a separate Common site, accessible to both the Main and Branch sites.
- An IPFR-EF service production circuit, to which the simulated enterprise Common site was connected via AVPN transport.

2.1. Interoperability Testing

The interoperability testing focused on the ability of the Branch site to fail-over and recover from a loss of connectivity to the Main site:

- Normal operations:
    - Branch telephones register to the Main site Session Manager (SIP telephones) or Communication Manager (H323 telephones).
    - The Main G430 Media Gateway, and the Branch G450 Media Gateway register to the Main site Communication Manager.
    - Branch telephones perform inbound and outbound IPFR-EF service call flows (see **Sections 3.2** and **3.3** for examples) via the Main site Session Manager, Communication Manager, and the Common site Avaya SBCE.

    - Inbound Meet-Me conference calls are processed via the Main site Meet-Me conference VDN/Vector.
- Fail-over operations:
    - Branch Communication Manager and Branch Session Manager activate.
    - Branch telephones register to the Branch Session Manager (SIP) or the Branch Communication Manager (H323).
    - Branch telephones perform inbound and outbound IPFR-EF service call flows via the Branch Session Manager, Branch Communication Manager, and the Avaya SBCE.
    - Inbound Meet-Me conference calls are processed via the Branch site Meet-Me conference VDN/Vector.
- Recovery operations:
    - Branch telephones reregister to the Main site Session Manager (SIP) or Communication Manager (H323).
        - Note that telephones with active calls will reregister after the call completes.
    - The Branch G450 Media Gateway registers to the Main site Communication Manager.
    - Branch telephones perform inbound and outbound IPFR-EF service call flows via the Main site Session Manager, Communication Manager, and the Avaya SBCE.
    - Inbound Meet-Me conference calls are processed via the Main site Meet-Me conference VDN/Vector.

The testing was performed using an IPFR-EF test plan provided by AT&T.

The following SIP trunking VoIP features were tested with the IPFR-EF service as part of this effort:

- SIP protocol verification.
- Inbound and outbound dialing including international calls.
- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.
- Basic telephony features such as hold, resume, conference, and transfer (attended and unattended).
- Call Forward with Diversion Header.
- Basic Avaya SIP Telephone/EC500 “mobility” calls (e.g., extend and return call).

The following IPFR-EF service features were tested as part of this effort:

- Network based Simultaneous Ring.
- Network based Sequential Ring (Locate Me).
- Network based “Blind Transfer” (Call redirection using Communication Manager Vector generated REFER).
- 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

Interoperability testing of the sample configuration and features described in **Section 2.1** were completed successfully. While no issues were encountered pertaining to the fail-over/recovery operations, the following observations were noted during testing:

2.2.1. Known Limitations

1. **Avaya Communication Manager Service Pack 4, (as well as Service Packs 2 and 3), block Refer usage.** During testing, it was found that even with the Network Call Redirection (NCR) option enabled, (see **Section 6.8.1**), Communication Manager was not issuing a Refer for "Blind Transfer" (Communication Manager Vector generated *Refer without Replaces* call redirection), or station initiated transfers (*Refer with Replaces*), if Service Packs 2, 3, or 4 are used. In the case of station initiated transfers, the transfers will be completed by using ReInvites. However the "Blind Transfer" processing will fail.
   - A Communication Manager MR has been opened, with a fix scheduled to be released with Service Pack 5.
   - The workaround is to use Communication Manager Service Pack 1, if Refer call processing is required prior to the Service Pack 5 release.

2. **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.
     - The workaround for this issue is to have the Avaya SBCE change the *SendOnly* parameter to *SendRecv* (see **Section 7.3.10**).

3. **Communication Manager Meet-Me conference can isolate PSTN parties if the conference takes place via an NCR enabled SIP trunk**.
   - This issue may occur if a three party Meet-Me conference is established via an NCR enabled trunk, with two parties on the PSTN and one party on Communication Manager station. Should the Communication Manager station leaves the conference, Communication Manager will issue a Refer, resulting in the two PSTN parties being directly connected by the IPFR-EF service, and Communication Manager ending the Meet-Me conference.
     - The workaround for this issue is to create a "Meet-Me Conference" SIP trunk with NCR *disabled*, used exclusively for customers using Meet-Me conference calls (see **Section 6.8.3)**.
     - Create a "general access" SIP trunk, with NCR *enabled*, for all other inbound and outbound calls (see **Section 6.8.1**). This supports the use of Refer for IPFR-EF "Blind Transfers" (call redirection) and station initiated call transfers (see **item 1** in this section).

4. **Codec negotiation with IPFR-EF Simultaneous Ring/Sequential Ring features.** The IPFR-EF network plays an “Answer Confirmation” announcement if the “secondary” number assigned to these features is answered. If that “secondary” number is associated with a Communication Manager IP endpoint, the ensuing codec negotiation results in the call being switched from a G.729 codec, briefly to a G.711 codec, and then returned to a G.729 codec for the duration of the call.
    - For this flow to return to G729, “shuffling” must be enabled for the associated Communication Manager IP station, otherwise the call will remain with G711.
    - Since Communication Manager TDM based stations (e.g., Digital and Analog) do not shuffle, using these types of stations as the “secondary” endpoint will result in the call remaining with G.711.
        - A workaround for non-shuffled endpoints is for the customer to disable the “Answer Confirmation” option for these IPFR-EF features. In this case no announcement is played and the calls will not switch to G.711.

5. **IPFR-EF Simultaneous Ring and Sequential Ring - Loss of calling display information on Communication Manager stations**. If the Communication Manager station associated with these IPFR-EF “secondary” number answers the call, the phone will not display the calling information. Based on the SIP signaling, Communication Manager expects a display update from the network. However, the subsequent network signaling does not contain new calling information.
    - The recommended workaround is described in **Section 6.8.1**, where Communication Manager will retrieve the display information using the *From* header. **Note that this solution is only applicable to Communication Manager 6.x platforms.**

6. **IPFR-EF Simultaneous Ring and Sequential Ring - Loss of audio if Communication Manager option “Initial IP-IP Direct Media” is enabled**. If the Communication Manager Signaling Group option “Initial IP-IP Direct Media” is enabled (see **Section 6.8.1**), loss of audio will occur if the “Secondary” station is answered. Therefore this option should remain disabled (default).
    - A Communication Manager MR has been opened.

7. **Avaya SBCE inserts Remote-Address header containing local CPE addressing**. The Avaya SBCE adds the Remote Address header to frames going to AT&T, advertizing local addressing.
    - The workaround is to have the Avaya SBCE remove this header (see **Section 7..3.10.1**.
    - An MR has been opened with the Avaya SBCE team.

8. **G.711 fax is not supported between Communication Manager and the IPFR-EF service.** Communication Manager does not support the protocol negotiation required for G.711 fax to work. T.38 fax is supported, however connections are limited to 9600. The sender and receiver of a fax call may use either Group 3 or Super Group 3 fax machines, but the T.38 fax protocol carries all fax transmissions as Group 3.

9. **IPFR-EF Sequential Ring – Loss of connection if Secondary party is busy.** The following IPFR_EF service limitation was observed during testing. If a PSTN Sequential Ring call is directed to the designated "Secondary" destination, and that destination returns a 486 Busy, PSTN does not hear a busy tone or any other call progress indications (ringing, reorder, etc.). After approximately 30 seconds the call is dropped.

10. **Removal of unnecessary SIP headers.** In an effort to reduce packet size (or block a header containing private addressing), the Avaya SBCE is provisioned to remove SIP headers not required by the AT&T IPFR-EF service (see **Section 7.4.3**).

11. **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 configuration used in these Application Notes is shown in **Figure 1** and consists of the following components:

- Main site:
    - Avaya Communication Manager 6.3, and Session Manager 6.3 running on separate platform servers.

    - Avaya G430 Media Gateway.
    - Avaya 96x1 SIP and H323 telephones.
- Branch site:
    - Avaya G450 Media Gateway, containing an S8300D Media Server.
    - Avaya Communication Manager 6.3 and Branch Session Manager 6.3 running on the S8300D (LSP).
    - Avaya 96x1 SIP and H323 telephones.
- Common site:
    - Avaya System Manager 6.3
    - Avaya SBCE and AT&T IPFR-EF access router.
- The IPFR-EF service Border Element (BE) uses SIP over UDP to communicate with the Avaya SBCE. In the reference configuration Session Manager, and Branch Session Manager, use SIP over TCP to communicate with both the Avaya SBCE and Communication Manager (Session Manager may use SIP over UDP, TCP, or TLS).
- Testing was performed using an IPFR-EF service production circuit.

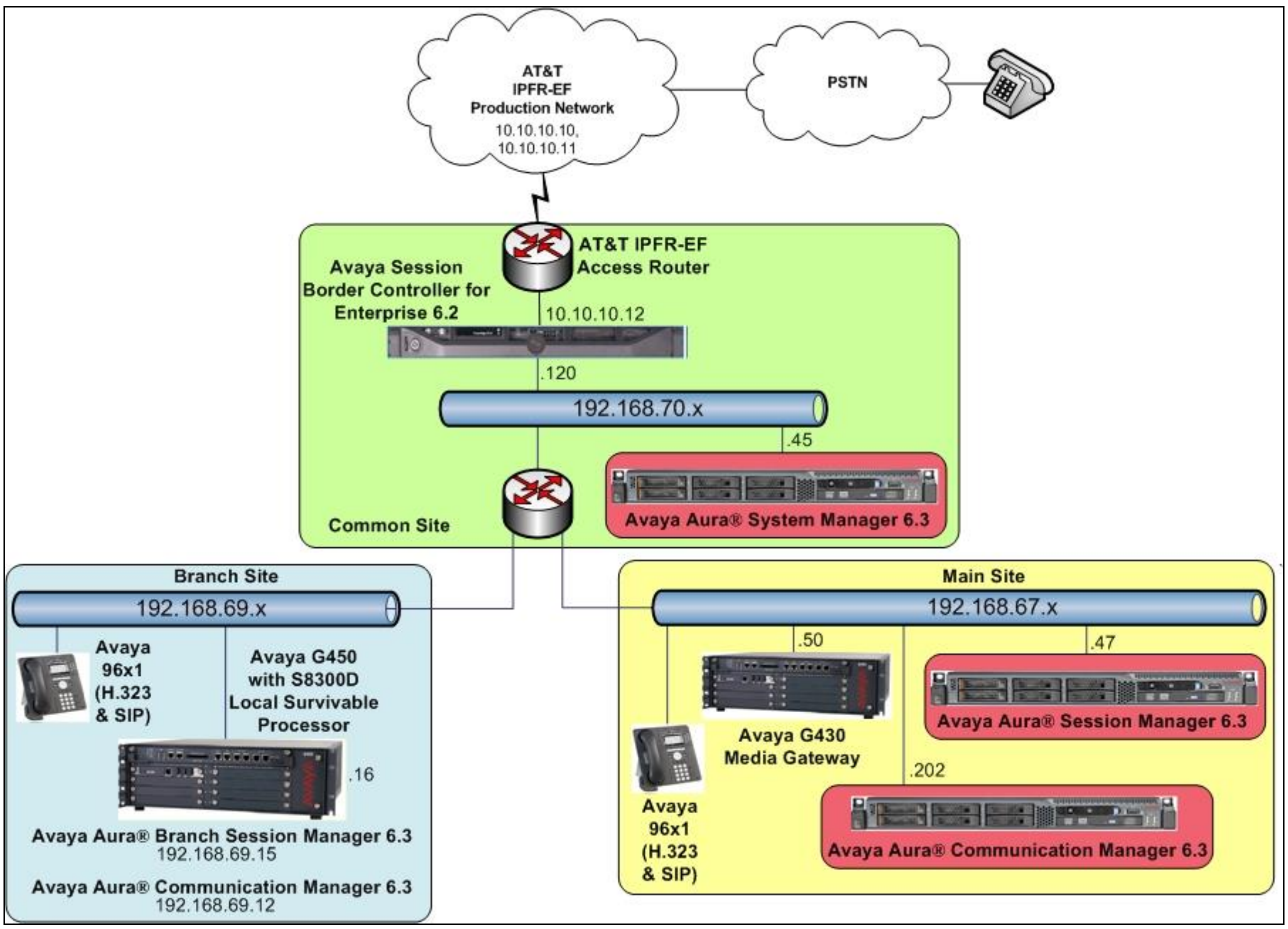


Figure 1: Reference configuration

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 configurations.

Note – The IPFR-EF service Border Element IP address and DID/DNIS digits are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DID/DNIS digits as part of the IPFR-EF provisioning process.

Component	Illustrative Value in these Application Notes
Main Site	
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
Branch Site	
Avaya Aura® Branch Session Manager	
Management IP Address	192.168.69.14
Network IP Address	192.168.69.15
Avaya Aura® Communication Manager	
IP Address	192.168.69.12
Avaya Aura® Communication Manager extensions	3xxxx
Common Site	
Avaya Aura® System Manager	
IP Address	192.168.70.45
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 IP Flexible Reach 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 address of **10.10.10.12** (Avaya SBCE public interface), **10.10.10.10,** and **10.10.10.11** (AT&T BE IP addresses), are specified.

3.2. AT&T IP Flexible Reach - Enhanced Features Service Call Flows

To understand how IPFR-EF service calls are handled by the Avaya CPE environment, three basic call flows are described in this section. However, for brevity, not all possible call flows are described.

3.2.1. Inbound

The first call scenario illustrated is an inbound IPFR-EF service call that arrives at the Avaya SBCE, to Session Manager, and is subsequently routed to Communication Manager, which in turn routes the call to a phone or fax.

1. A PSTN phone originates a call to an IPFR-EF service number.
2. The PSTN routes the call to the IPFR-EF service network.
3. The IPFR-EF service routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a phone or fax.

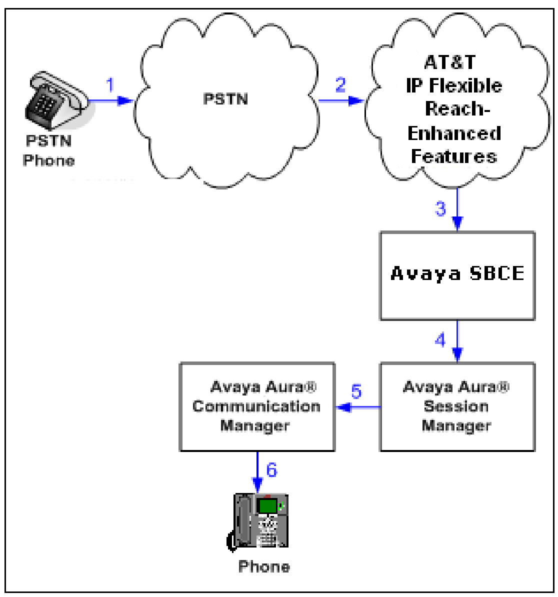


Figure 2: Inbound IPFR-EF Call

3.2.2. Outbound

The second call scenario illustrated is an outbound call initiated on Communication Manager, routed to Session Manager, and is subsequently sent to the Avaya SBCE for delivery to the IPFR-EF service.

1. A Communication Manager phone or fax originates a call to an IPFR-EF service number for delivery to the PSTN.
2. Communication Manager routes the call to Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to the IPFR-EF service.
5. The IPFR-EF service delivers the call to the PSTN.

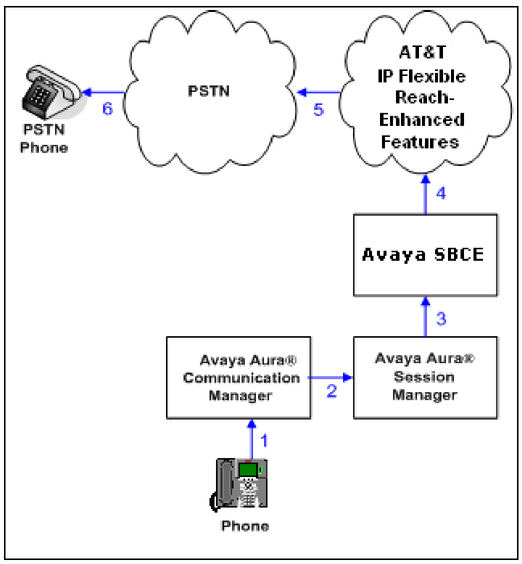


Figure 3: Outbound IPFR-EF Call

3.2.3. Call Forward Re-direction

The third call scenario illustrated is an inbound IPFR-EF service call that arrives at the Avaya SBCE, to Session Manager, and subsequently Communication Manager. Communication Manager routes the call to a destination station, however the station has set Call Forwarding to an alternate destination. Without answering the call, Communication Manager redirects the call back to the IPFR-EF service for routing to the alternate destination.

Note – In cases where calls are forwarded to an alternate destination such as an N11, NPA-555-1212, or 8xx numbers, the IPFR-EF service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 6.8**).

3. Same as the first call scenario in **Section 3.2.1**.
4. Because the Communication Manager phone has set Call Forward to another IPFR-EF service number, Communication Manager initiates a new call back out to Session Manager, the Avaya SBCE, and to the IPFR-EF service network.
5. The IPFR-EF service places a call to the alternate destination and upon answering; Communication Manager connects the calling party to the target party.

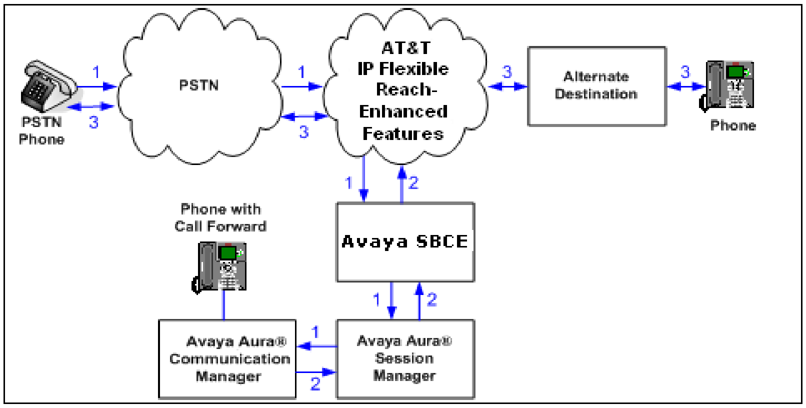


Figure 4: Station Re-directed (e.g. Call Forward) IPFR-EF Call

3.3. AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow

This section describes the call flow for IPFR-EF using SIP Refer to perform Network Based Blind Transfer. The Refer is generated by an inbound call to a Communication Manager Vector. The call scenario illustrated in figure below is an inbound IPFR-EF call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a vector. The vector answers the call and, using Refer, redirects the call back to the IP E-IPFR service for routing to an alternate destination.

1. A PSTN phone originates a call to an IPFR-EF number.
2. The PSTN routes the call to the IPFR-EF network.
3. IPFR-EF routes the call to the Avaya SBCE.
4. The Avaya SBCE performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Network Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Communication Manager routes the call to a VDN/Vector, which answers the call and plays an announcement, and attempts to redirect the call using a SIP REFER message. The SIP REFER message specifies the alternate destination, and is routed back through Session Manager on to the Avaya SBCE. The Avaya SBCE sends the REFER to the IPFR-EF service.
7. IPFR-EF places a call to the alternate destination specified in the REFER, and upon answer, connects the calling party to the alternate party.

8. IPFR-EF clears the call on the redirecting/referring party (Communication Manager).

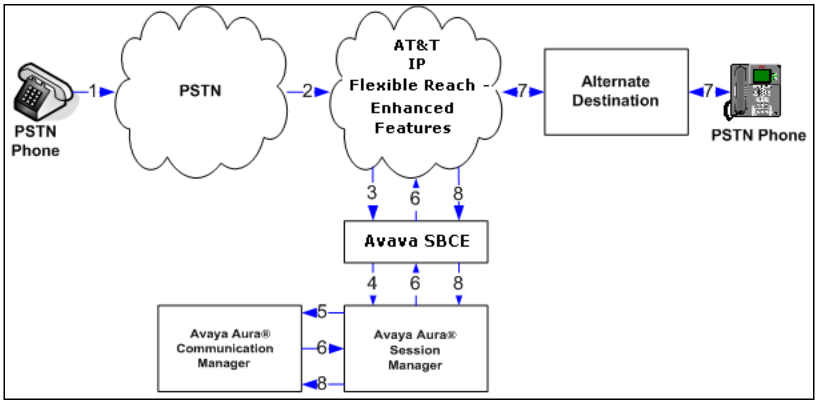


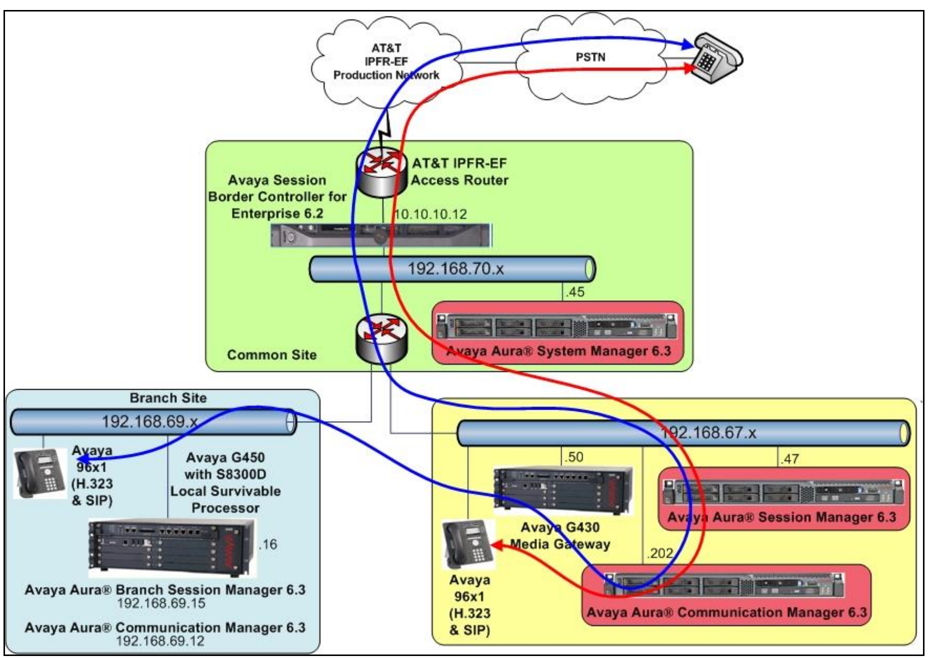
Figure 6: Network Based Blind Transfer Using Refer (Communication Manager Vector)

3.4. Main and Branch Site Call Flows

The following diagrams show the inbound and outbound call paths for normal and fail-over conditions.

3.4.1. Normal Call Flows

In this simplified example, inbound/outbound Main trunk calls are shown in red and inbound/outbound Branch trunk calls are shown in blue. Since the Main site is accessible to the Common and Branch sites, the Avaya SBCE directs inbound calls to the Main site Session Manager, which routes the calls to the Main Communication Manager. Depending on the destination, the call is then sent to either a Main or Branch telephones. Outbound calls take a similar path.

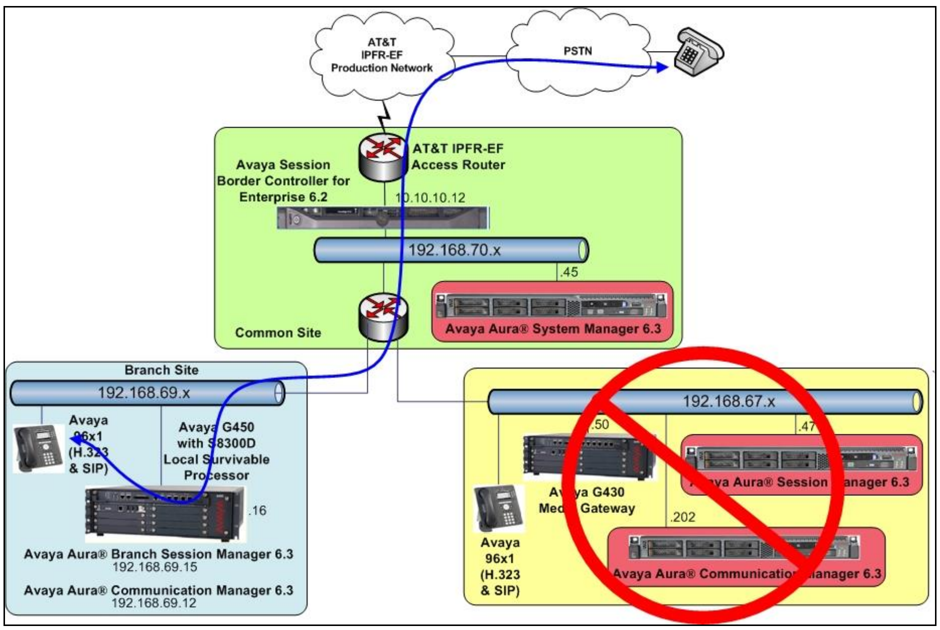


3.4.2. Fail-over Call Flows

In this simplified example, the Main site is not accessible to the Common or Branch sites. As a result, the Branch G450 looses registration with the Main Communications Manager. The LSP in the Branch site then activates both the Branch Communication Manager and Branch Session Manager instances running on the S8300D LSP (installed in the Branch G450).

The Branch telephones will have also detected a loss of connection to the Main Communication Manager (H323 telephones) and the Main Session Manager (SIP telephones). This causes the Branch H323 telephones to reregister to the Branch Communication Manager, and the Branch SIP telephones to reregister to the Branch Session Manager.

The Avaya SBCE in the Common site detects that its connection to the Main Session Manager has been lost, and then directs inbound calls to the Branch Session Manager. The Branch Session Manager then routes the calls to the Branch Communication Manager, and subsequently the Branch telephones. Outbound calls take a similar path.



3.4.3. Recovery

Once the connection to the Main site has been restored, the Branch G450 reregisters to the Main Communication Manager, the LSP deactivates the Branch Communication Manager and Branch Session Manager, and the Branch telephones reregister to the Main Communication Manager (H323 telephones) and the Main Session Manager (SIP telephones).

The Avaya SBCE detects that the connection to the Main Session Manager has been restored, and directs inbound calls back to the Main Session Manager. The call flows then resume to those shown in **Section 3.4.1**.

4. 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	 • 6.3.1.0.8002 • 6.3.6 (r3602103)
IBM 8800 server • Avaya Aura® Session Manager	 • 6.3 SP6 (6.3.6.0.636005)
IBM 8800 server • System Platform • Avaya Aura® Communication Manager	 • 6.3.1.0.8002 • 6.3 SP4 (03.0.124.0-21291), and 6.3 SP1 (03.0.124.0-20850)[4]
Avaya S8300D server • System Platform • Avaya Aura® Communication Manager	 • 6.3.1.0.8002 • 6.3 SP4 (03.0.124.0-21291), and 6.3 SP1 (03.0.124.0-20850)[5]
Avaya G430 Media Gateway • MM712 Digital card	• 34.5.1 • HW7 FW15
Avaya G450 Media Gateway • MM711 Analog card	• 34.5.1 • HW4 FW98
Dell R210 • Avaya Session Border Controller for Enterprise	• 6.2.1 Q07
Avaya 96x1 IP Telephone	• H.323 Version 6.3.037 • SIP Version 6.2.2.17
Avaya 6221 Analog telephone	-
Ventafax Home Version (Windows based Fax device)	• 7.0.202.494

Table 2: Equipment and Software Versions

[4] See Section 2.2.1, Item 1
[5] See Section 2.2.1, Item 1

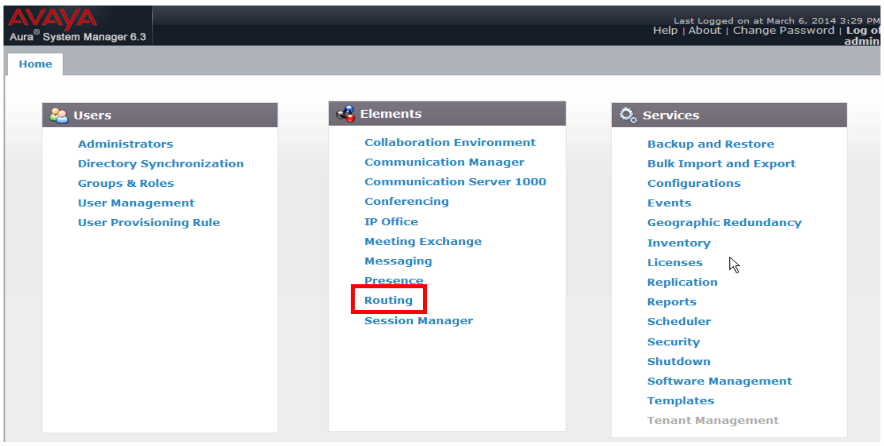
5. Configure Avaya Aura® Session Manager

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult **[1 & 2]** for further details if necessary.

This section provides the procedures for configuring the Main and Branch Session Managers to process inbound and outbound calls between the Main or Branch Communication Manager instances, and the Avaya SBCE. In the Reference configuration, all Session Manager provisioning is performed via the common System Manager platform located in the Common site. The following administration activities will be described for both the Main and Branch Session Manager:

- Define a SIP Domain
- Define Locations for Customer Premises Equipment (CPE), including the Main, Branch and Common sites.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager (Main and Branch), and the Avaya SBCE.
- Define SIP Entities corresponding to Communication Manager (Main and Branch), and the Avaya SBCE.
- Define Entity Links describing the SIP trunks between Communication Manager (Main and Branch), the Session Managers (Main and Branch), as well as the SIP trunks between the Session Managers (Main and Branch) and the Avaya SBCE.
- Define Routing Policies associated with the Communication Managers (Main and Branch), Session Managers (Main and Branch), and the Avaya SBCE.
- Define Dial Patterns, which govern which Routing Policy will be selected for call routing for the Main and Branch sites.

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**.



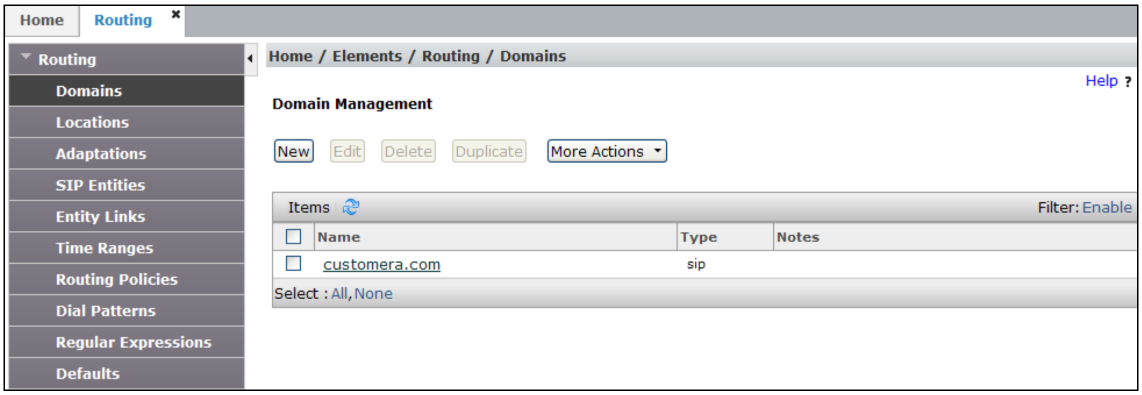
5.1. SIP Domain

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.



5.2. 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, three Locations are specified:

- **Main** (**192.168.67.***) – The primary customer site containing System Manager, Session Manager, and Communication Manager, the G430 Media Gateway, and telephones.
- **Branch** (**192.168.69.***) – The remote site containing the G450 Media Gateway, containing the S8300D Local Survivable Processor (LSP). Instances of Communication Manager and the Branch Session Manager run on the LSP. The site also contains telephones.
- **Common** (**192.168.70.***) – This site contains the Avaya SBCE as well as the IPFR-EF access router.

5.2.1. Main Location

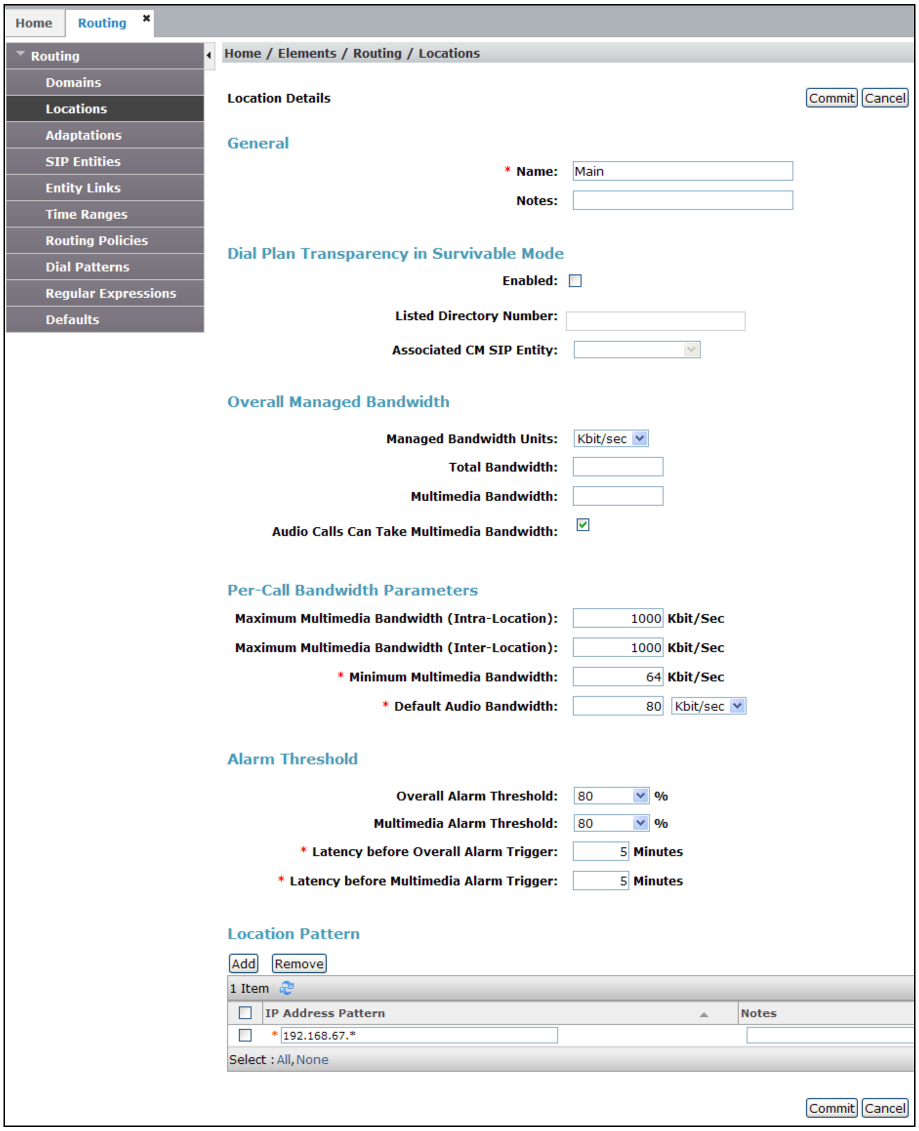
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **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.

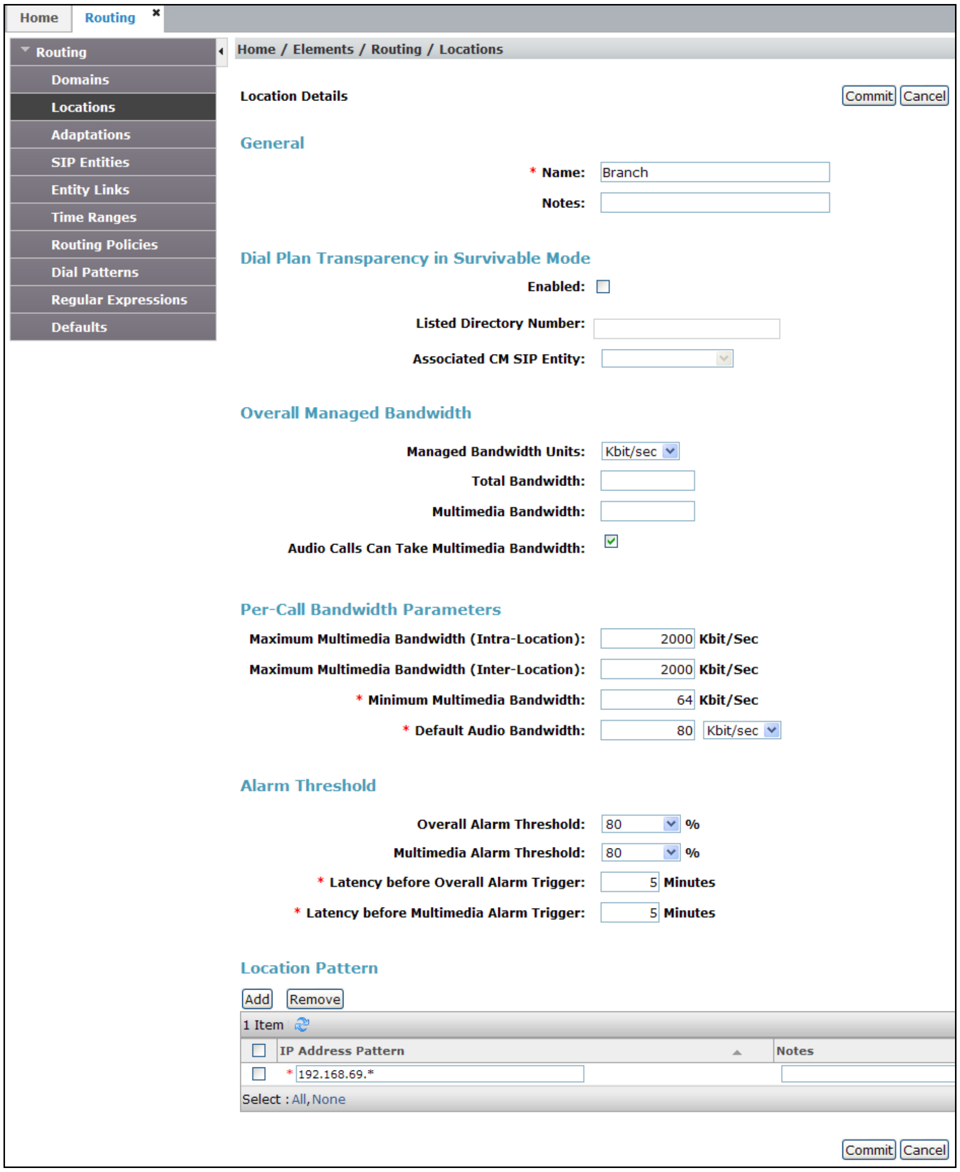
Step 3 - Click **Commit** to save.



5.2.2. Branch Location

Follow the steps from **Section 5.2.1** with the following changes:

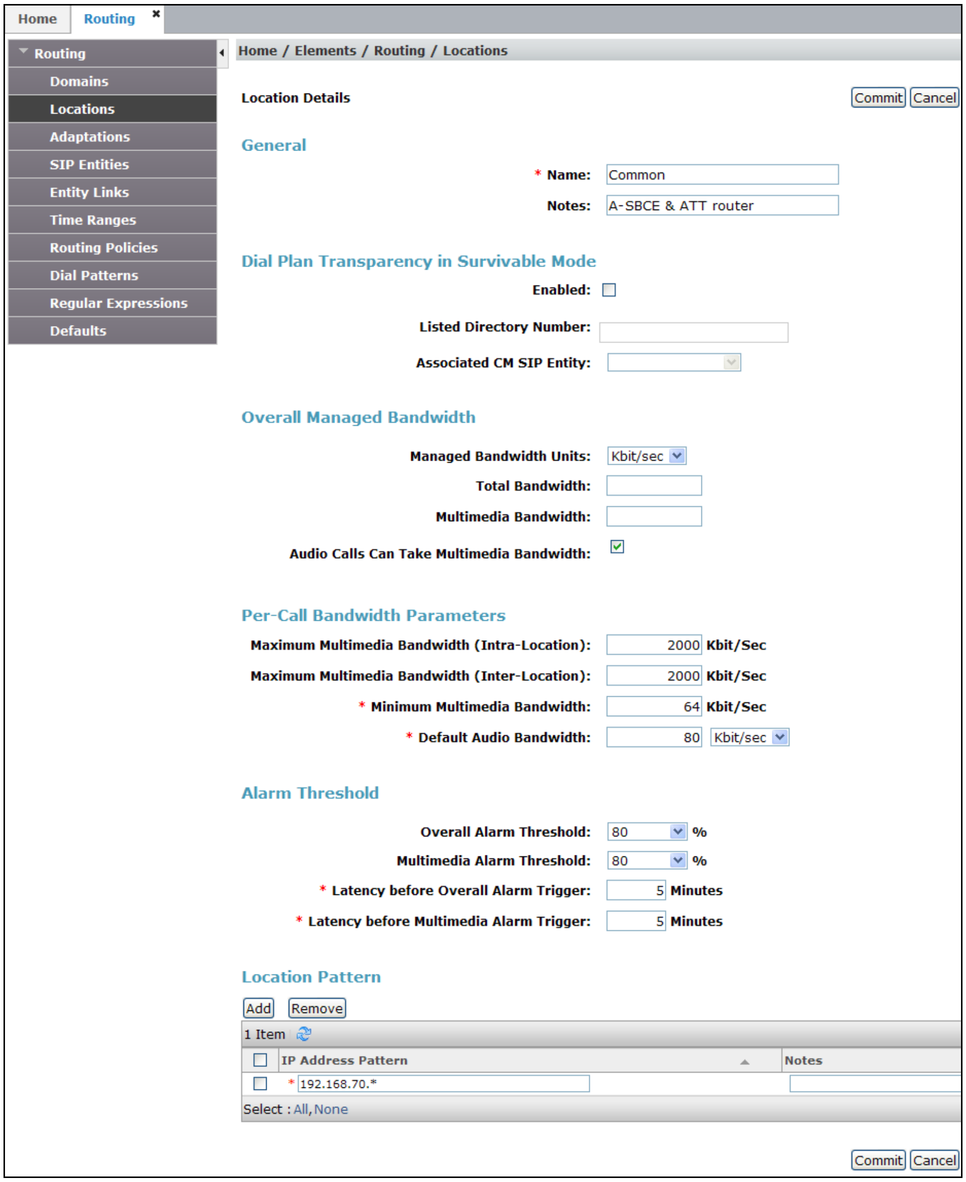
- **Name:** Enter a descriptive name for the Location (e.g., **Branch**).
- **IP Address Pattern:** Enter the IP address of the Branch subnet (e.g., **192.168.69.***).

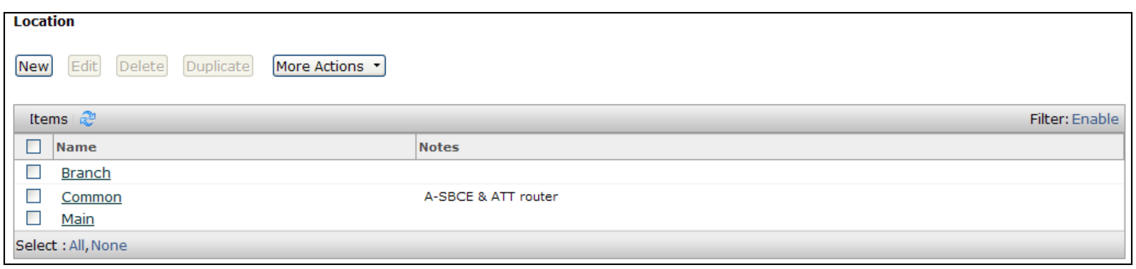


5.2.3. Common Location

Follow the steps from **Section 5.2.1** 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.***).





5.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers sent to/from AT&T, 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 5.3.1**) - Modification of SIP messages sent to Communication Manager extensions (Main or Branch).
  - The IP address of Session Manager (**192.168.67.47**) is replaced with the Avaya CPE SIP domain (**customera.com**) for destination domain.

  The AT&T Border Element IP address (**10.10.10.10**[6]) is replaced with **customera.com** for source domain.
  - The AT&T called number digit string in the Request URI is replaced with the associated Communication Manager extensions/VDNs.
- Calls to AT&T (**Section 5.3.2**) - Modification of SIP messages sent by Communication Manager extensions (Main or Branch).
  - The domain of Session Manager (**customera.com**) is replaced with the AT&T BE IP address (**10.10.10.10**[7]) in the destination headers.
  - The domain of Session Manager (**customera.com**) is replaced with the Avaya SBCE private IP address (**192.168.70.120**) in the origination headers.
  - The History-Info header is removed automatically by the **ATTAdapter**.
- Meet-Me Conference calls to the Main Communication Manager (**Section 5.3.3**)
  - The dedicated Meet-Me conference DNIS number is converted to the Meet-Me conference VDN extension in the Main site when the Main Session Manager is active.
- Meet-Me Conference calls to the Branch Communication Manager (**Section 5.3.4**)
  - The dedicated Meet-Me conference DNIS number is converted to the Meet-Me conference VDN extension in the Branch site, when the Branch Session Manager is active.

5.3.1. Adaptation for calls to Avaya Aura® Communication Manager Extensions

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager extensions from AT&T. Note that this Adaptation will be applied whether the Main or Branch Session Manager is active.

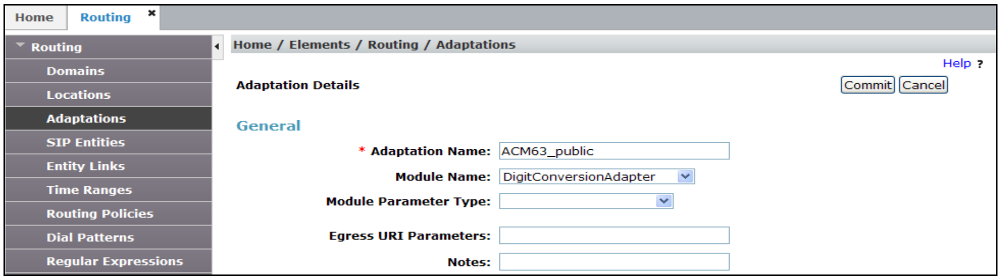
Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

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

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

---

[6] See the note in Section 3.1
[7] See the note in Section 3.1



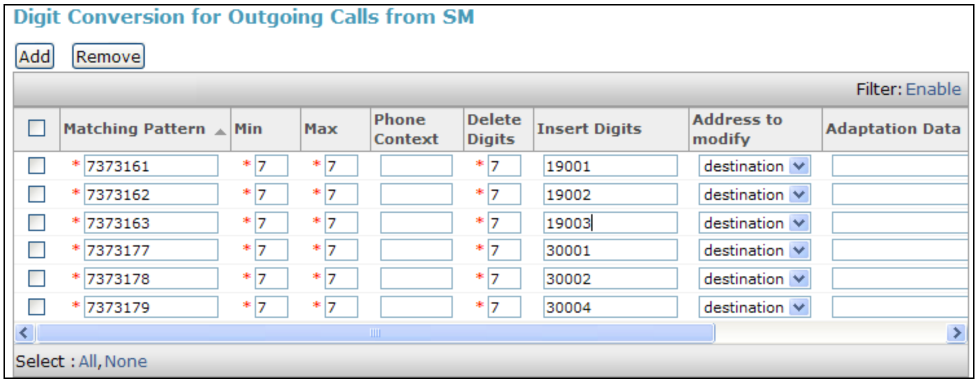
Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* digits from AT&T that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager).

3. **Example1 – destination Main extension**: 5553161 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension 19001 located in the Main site.
    - Enter **5553161** in the **Matching Pattern** column.
    - Enter **7** in the **Min/Max** columns.
    - Enter **7** in the **Delete Digits** column.
    - Enter **19001** 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.
4. **Example2 – destination Branch extension**: 5553177 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension 30001 located in the Branch site.
    - Enter **5553177** in the **Matching Pattern** column.
    - Enter **7** in the **Min/Max** columns.
    - Enter **7** in the **Delete Digits** column.
    - Enter **30001** 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 – As shown in the screen below, no **Digit Conversion for Incoming Calls to SM** were required in the reference configuration.

Note – In the reference configuration, the AT&T IPFR-EF service delivered 7 digit DNIS numbers.


Digit Conversion for Outgoing Calls from SM

Add Remove

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
☐	* 7373161	* 7	* 7		* 7	19001	destination	
☐	* 7373162	* 7	* 7		* 7	19002	destination	
☐	* 7373163	* 7	* 7		* 7	19003	destination	
☐	* 7373177	* 7	* 7		* 7	30001	destination	
☐	* 7373178	* 7	* 7		* 7	30002	destination	
☐	* 7373179	* 7	* 7		* 7	30004	destination	

Select : All, None

5.3.2. Adaptation for calls to the AT&T IP Flexible Reach – Enhanced Features Service

The Adaptation administered in this section is used for modification of SIP messages from Communication Manager to AT&T. Note that this Adaptation will be applied whether the Main or Branch Session Manager is active.

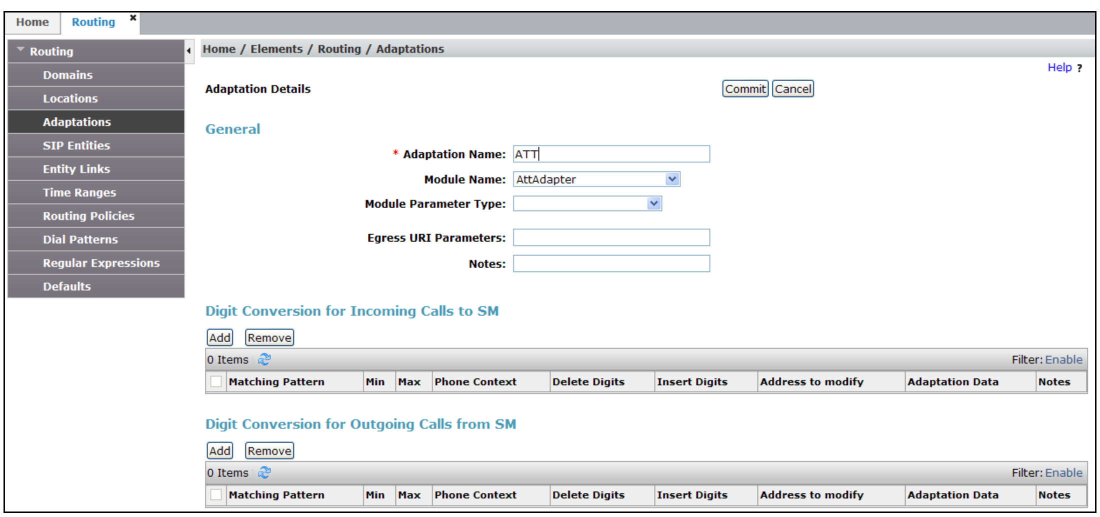
Step 1 - In the left pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown).

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

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**). The AttAdapter will automatically remove History-Info headers, (which the IPFR-EF service does not support), sent by Communication Manager (see **Section 6.8.1**).

Step 3 - Click on **Commit**.

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



5.3.3. Adaptation for Meet-Me Conference calls to the Main Communication Manager

The dedicated Meet-Me conference DNIS number is converted to the Meet-Me conference VDN extension in the Main site only when the Main Session Manager is active.

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:

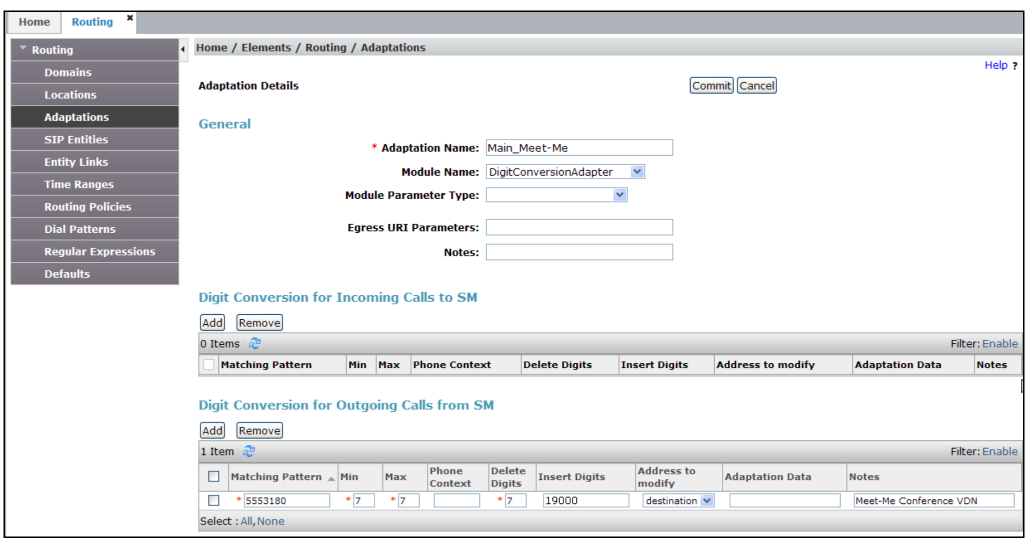
1. A descriptive **Name**, (e.g., **Main_Meet-Me**).
2. Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).

Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section.

3. 5553180 is the DNIS string selected for the Meet-Me conference. It is associated with Main Communication Manager VDN extension 19000.
   - Enter **5553180** in the **Matching Pattern** column.
   - Enter **7** in the **Min/Max** columns.
   - Enter **7** in the **Delete Digits** column.
   - Enter **19000** 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 Incoming Digit Conversion was required in the reference configuration.

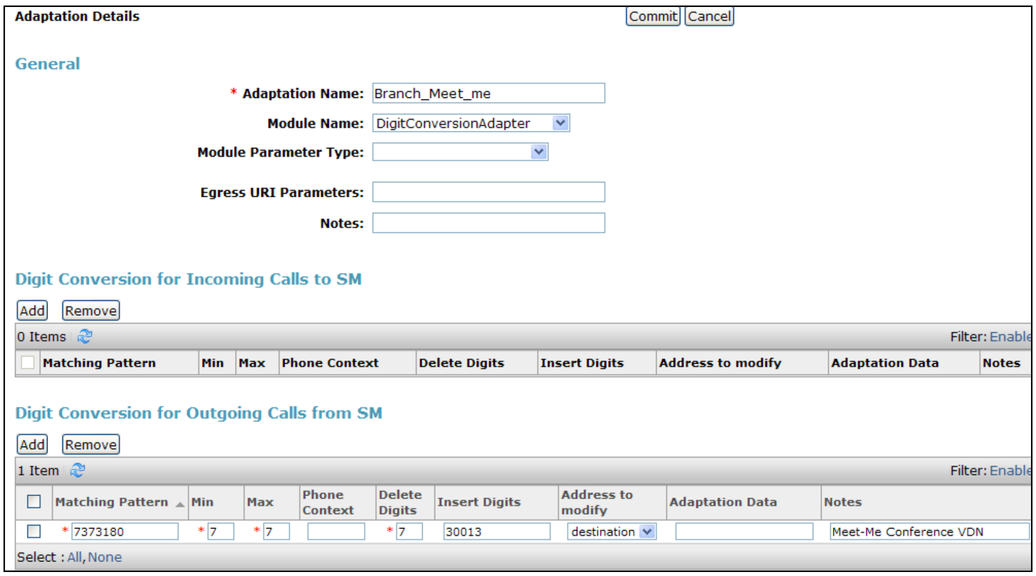


5.3.4. Adaptation for Meet-Me Conference calls to the Branch Communication Manager

The dedicated Meet-Me conference DNIS number is converted to the Meet-Me conference VDN extension in the Branch site (30013) only when the Branch Session Manager is active.

Step 1 – Follow the steps shown in **Section 5.3.3**, with the following changes:

1. In the **Adaptation Details** page, enter a descriptive **Name**, (e.g., **Branch_Meet-Me**).
2. Scroll down to the **Digit Conversion for Outgoing Calls from SM** section:
    - Enter **5553180** in the **Matching Pattern** column.
    - Enter **30013** in the **Insert Digits** column.



5.4. SIP Entities

Note – In the creation of the SIP Entities below, the Main and Branch Session Manager platforms are defined, each specifying their associated IP addresses (**Sections 5.4.1** & **5.4.2**). Communication Manager SIP trunk Entities are defined for the Local and AT&T SIP Trunks (**Sections 5.4.3** and **5.4.4),** as well as a SIP Trunk for Meet-Me conference calls (**Section 5.4.5**). The IP address of the Main Communication Manager platform is used for each of these Entities.

No SIP Entity needs to be provisioned for the Branch Communication Manager instance. When the Branch Communication Manager and Branch Session Manager are installed, (as part of the common installation procedure), internal provisioning is performed that automatically defines a SIP Entity for the Branch Communication Manager, using the IP address of the Branch Communication Manager. This internally generated SIP Entity is called **avaya-lsp-fs** (see **Section 8.4.1**).

The Branch Session Manager uses the **avaya-lsp-fs** SIP Entity to communicate with the Branch Communication Manager when the Branch site activates, but uses the Main Communication Manager SIP trunk Entities for call processing. Associated Main Communication Manager Entity Links, Routing Policies, and Dial Patterns are used by the Branch Session Manager as well. However, a separate SIP Entity must be defined for the Branch Meet-Me conference SIP trunk (**Section 5.4.6**).

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

- Main Session Manager platform (**Section 5.4.1**).
- Branch Session Manager platform (**Section 5.4.2**).
- Main/Branch Communication Manager for AT&T trunk access (**Section 5.4.3**) – This entity, and its associated Entity Link (using TCP with port 5062, is for calls to/from AT&T and Communication Manager via the Avaya SBCE. Note that this connection will be associated with the NCR *enabled* trunk on Communication Manager (see **Section 2.2.1,** Item **1**).
- Main/Branch Communication Manager for local trunk access (**Section 5.4.4**) – This entity, and it's associated Entity Link (using TCP with port 5060), is primarily for traffic between Avaya SIP telephones and Communication Manager.
- Main Communication Manager for Meet-Me conference trunk access (**Section 5.4.5**) – If support for Meet-Me conferences is required, then this Entity, and its associated Entity Link must be added. Note that this connection will be associated with the NCR *disabled* trunk on Communication Manager (see **Section 2.2.1,** Item **1**).
- Branch Communication Manager for Meet-Me conference trunk access (**Section 5.4.6**) – If support for Meet-Me conferences is required, then this Entity, and its associated Entity Link must be added. Note that this connection will be associated with the NCR *disabled* trunk on Communication Manager (see **Section 2.2.1,** Item **1**).
- Avaya SBCE platform (**Section 5.4.7**) - This entity, and its associated Entity Link (using TCP and port 5060), is for calls to/from the IPFR-EF service via the Avaya SBCE.

Note – In the reference configuration, TCP is used as the transport protocol between Session Manager and the Communication Manager (ports 5060, 5062, and 5080), and the Avaya SBCE (port 5060). This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS to be used as the transport protocol whenever possible. The connection between the Avaya SBCE and the AT&T IPFR-EF service uses UDP/5060 per AT&T requirements.

5.4.1. Avaya Aura® Session Manager SIP Entity (Main site)

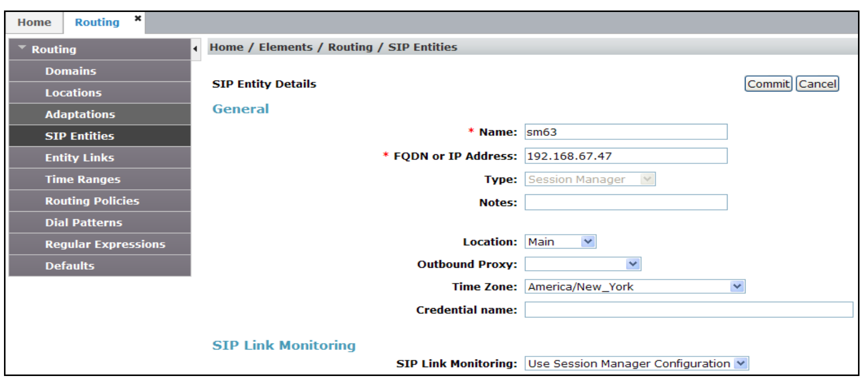
Step 1- In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).

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

- **Name –** Enter a descriptive name for Session Manager (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 5.2.1)**.
- **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 5.1** (e.g., **customera.com**)

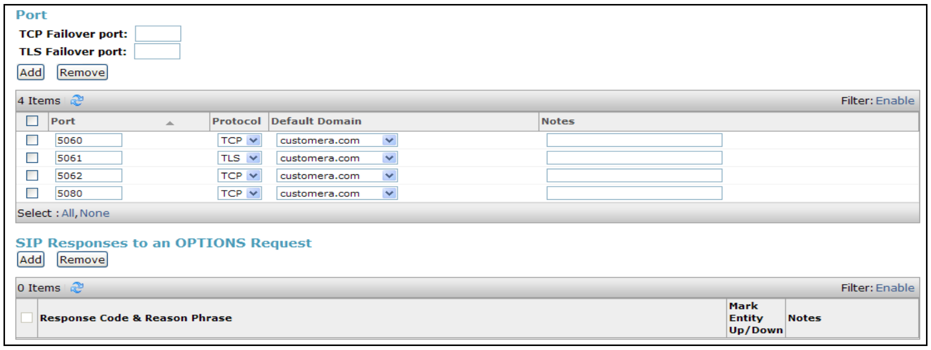
Step 5 - Repeat **Step 4** to provision entries for:

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

- **5080** for **Port** and **TCP** for **Protocol**.
- **5061** for **Port** and **TLS** for **Protocol**. While TLS is not used in the reference configuration, it is included here for completeness.

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

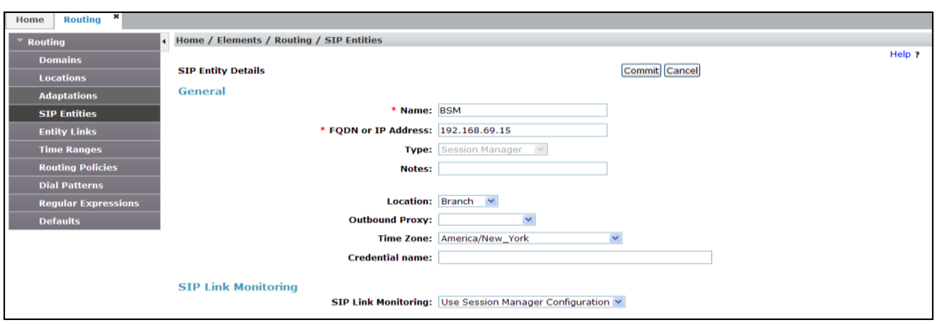
Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**. The **SIP Responses to an OPTIONS Request** section of the form is not used in the reference configuration.



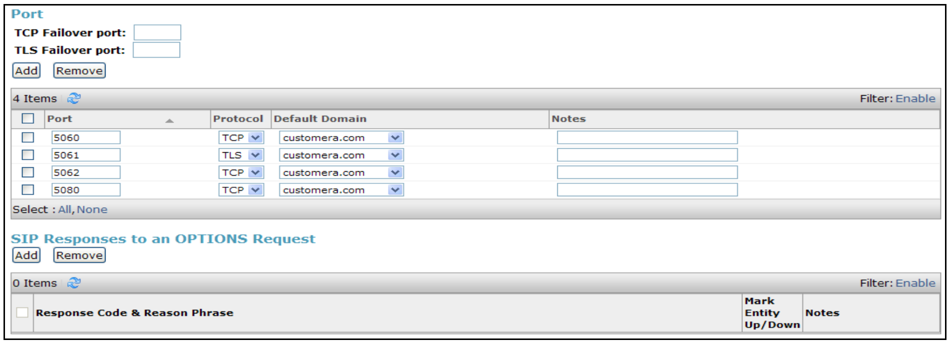
5.4.2. Avaya Aura® Session Manager SIP Entity (Branch Site)

Follow the procedures shown in **Section 5.4.1**, with the following changes:
Step 1 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name for Session Manager (e.g., **BSM**).
- **FQDN or IP Address –** Enter the IP address of the Branch Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **192.168.69.15**).
- **Type –** Verify **Session Manager** is selected.
- **Location** – Select location **Branch** (**Section 5.2.2)**.



The **Port** and **SIP Responses to an OPTIONS Request** sections are the same as in **Section 5.4.1**.



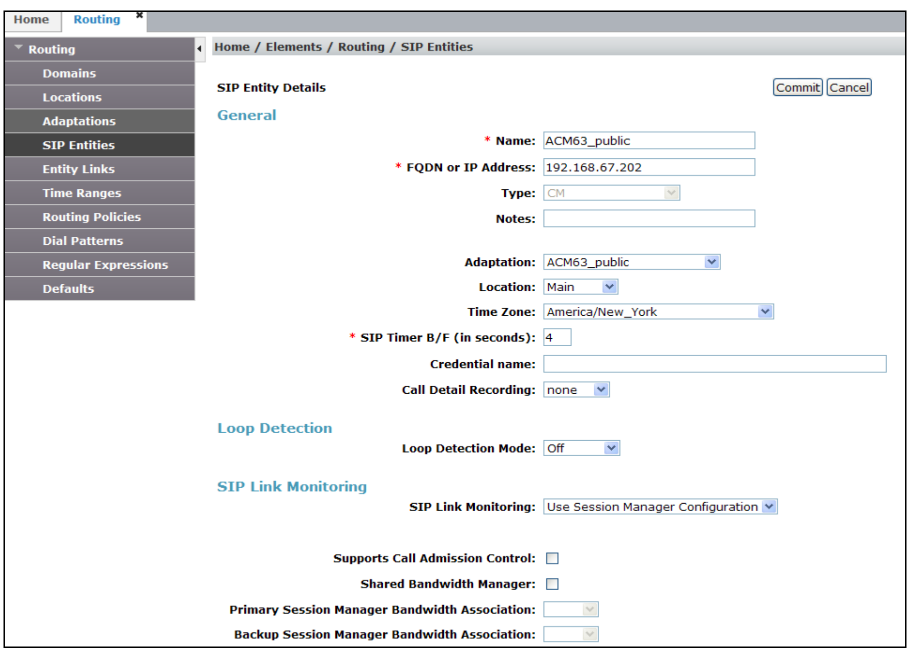
5.4.3. Avaya Aura® Communication Manager SIP Entity – Public Trunk

Step 1 - 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 for the Communication Manager public trunk (e.g. **ACM63_public**).
- **FQDN or IP Address –** Enter the IP address of the Main Communication Manager Processor Ethernet (procr) described in **Section 6.5** (e.g. **192.168.67.202**).
- **Type –** Select **CM**.
- **Adaptation –** Select the Adaptation **ACM63_public** administered in **Section 5.3.1**.
- **Location** – Select a Location **Main** administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
  - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
  - Use the default values for the remaining parameters.

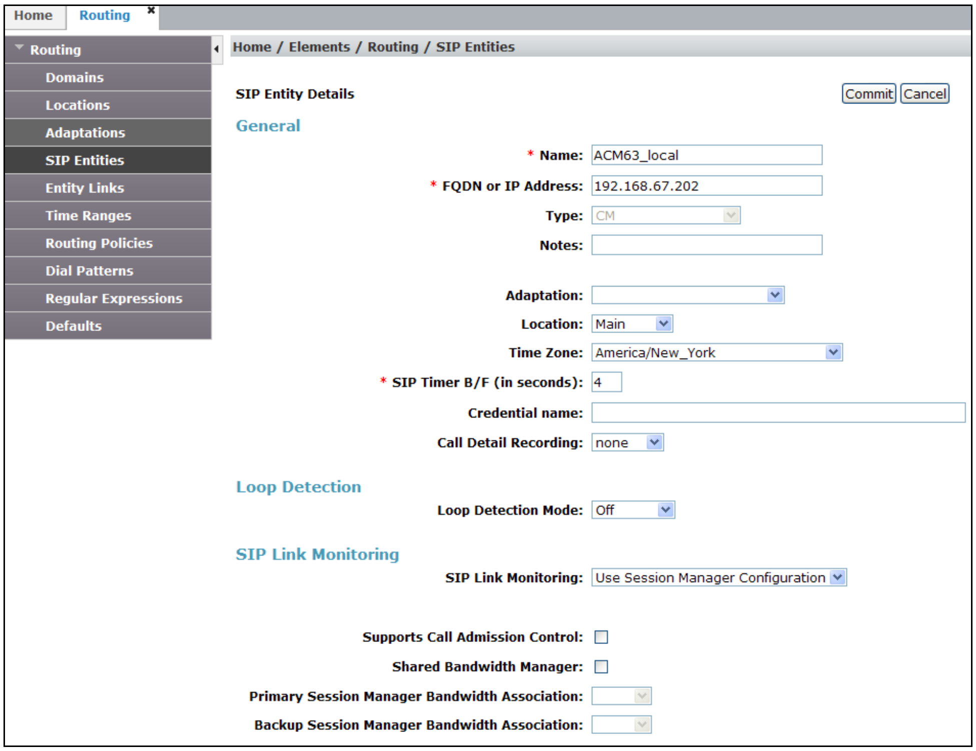
Step 3 - Click on **Commit** (not shown).



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

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 5.4.3** with the following changes:

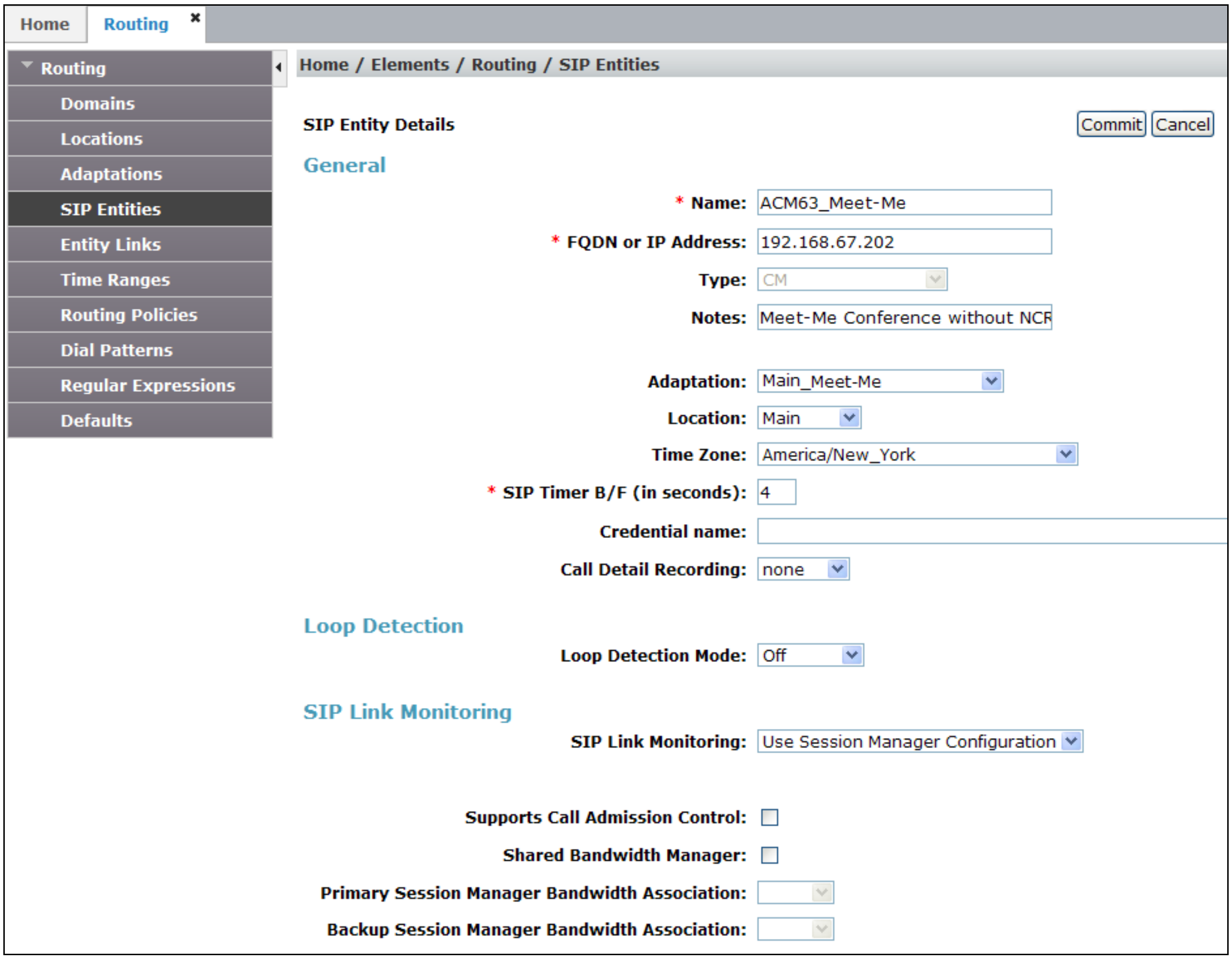
- **Name** – Enter a descriptive name for the Communication Manager public trunk (e.g. A**CM63_local**).
- Note that this Entity has no Adaptation defined.



5.4.5. Avaya Aura® Communication Manager SIP Entity – Main Site Meet-Me Trunk

As described in **Section 2.2.1, Item 3**, a separate Meet-Me conference SIP trunk must be defined. To configure the Meet-Me conference SIP Entity, repeat the steps in **Section 5.4.3** with the following changes:

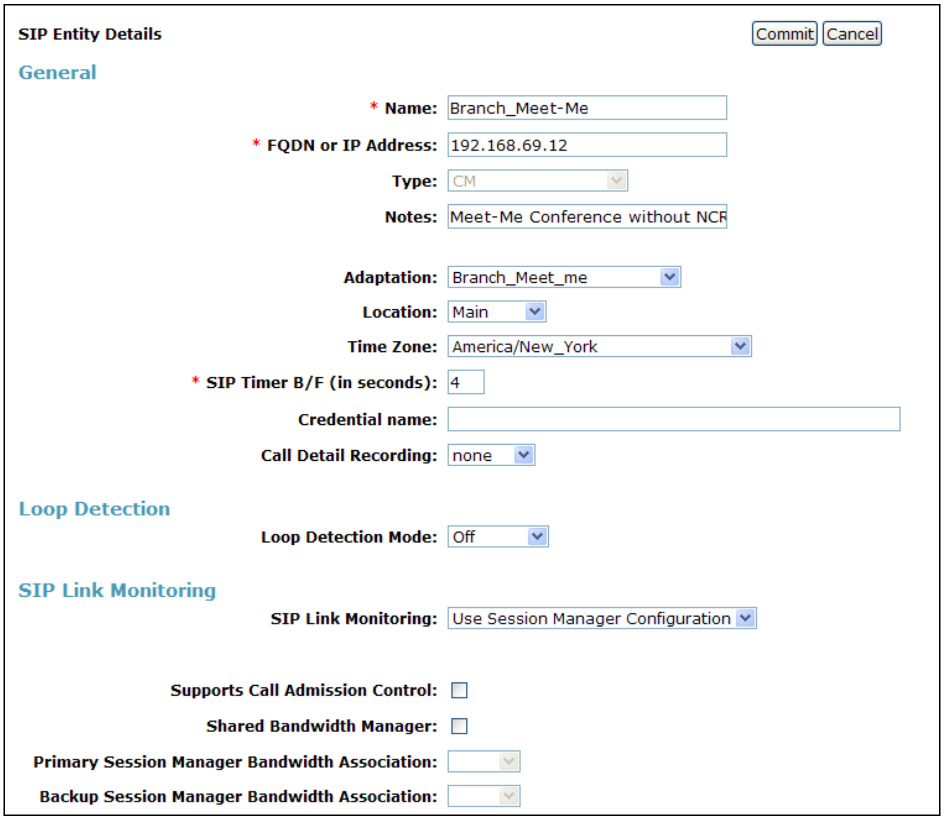
- **Name** – Enter a descriptive name for Session Manager (e.g., **ACM63_Meet-Me**).
- **Adaptations** – Select Adaptation **Main_Meet-Me** (**Section 5.3.3**).



5.4.6. Avaya Aura® Communication Manager SIP Entity – Branch Site Meet-Me Trunk

Repeat the steps in **Section 5.4.5** with the following changes:

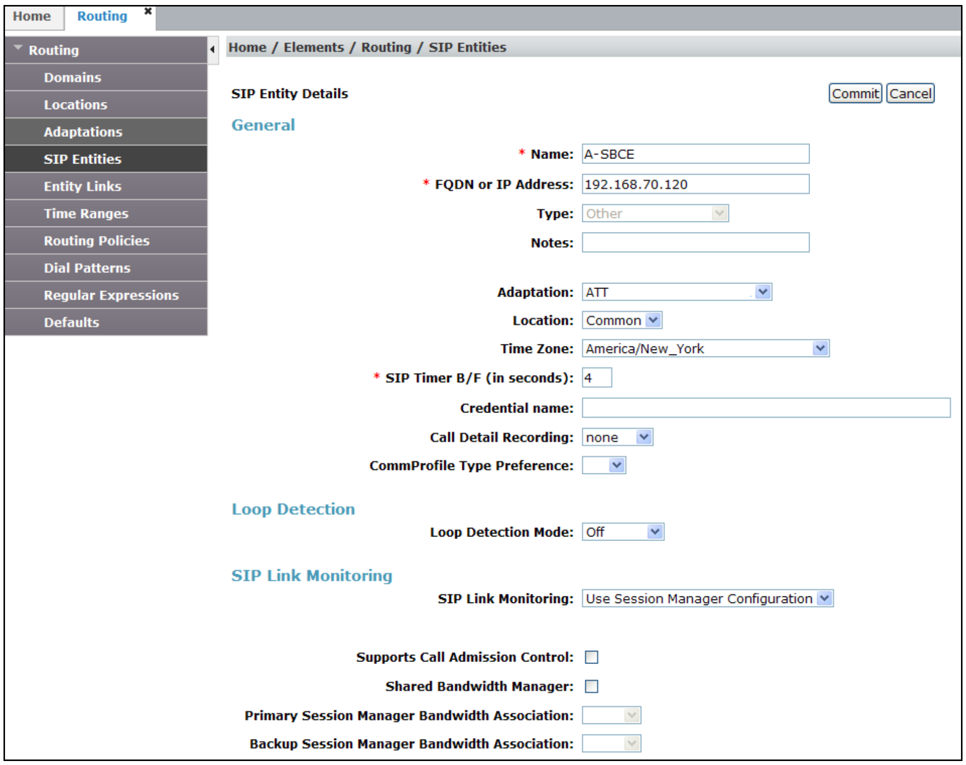
- **Name** – Enter a descriptive name for Session Manager (e.g., **Branch_Meet-Me**).
- **IP Address** – Enter the IP address of the Communication Manger (LSP) in the Branch site (e.g., **192.168.69.12**).
- **Adaptations** – Select Adaptation **Branch_Meet-Me** (**Section 5.3.4**).



5.4.7. Avaya Session Border Controller for Enterprise SIP Entity

To configure the Avaya SBCE SIP Entity, repeat the steps in **Section 5.4.1** with the following changes:

- **Name –** Enter a descriptive name for Session Manager (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 7.5.1**).
- **Type –** Verify **Other** is selected.
- **Adaptations –** Select Adaptation **ATT** (**Section 5.3.2**).
- **Location** – Select location **Common** (**Section 5.2.3)**.



5.5. Entity Links

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

- Main Session Manager to Main Communication Manager Public trunk (**Section 5.5.1**).
- Main Session Manager to Main Communication Manager Local trunk (**Section 5.5.2**).
- Main Session Manager to Main Communication Manager Meet-Me trunk (**Section 5.5.3**).
- Main Session Manager to Avaya SBCE (**Section 5.5.4**).
- Branch Session Manager to Main Communication Manager Public Trunk (**Section 5.5.5**).
- Branch Session Manager to Main Communication Manager Local Trunk (**Section 5.5.6**).
- Branch Session Manager to Branch Communication Manager Meet-Me trunk (**Section 5.5.7**).
- Branch Session Manager to Avaya SBCE (**Section 5.5.8**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 5.4**.

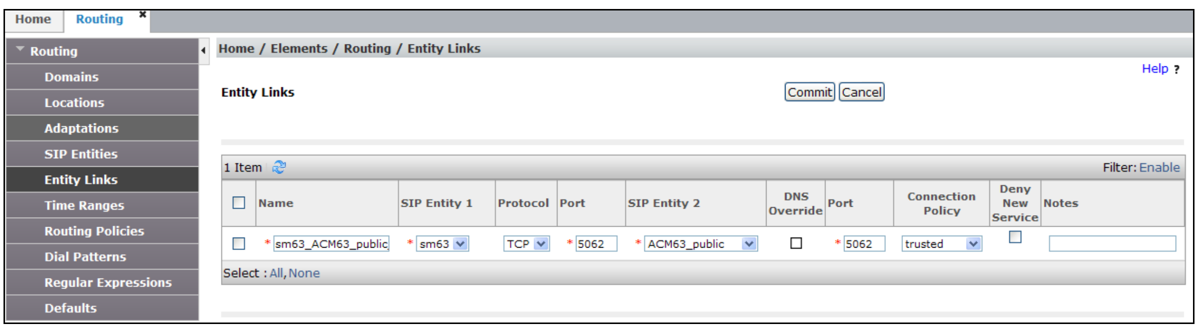
Note – See the information in **Section 5.4** regarding the transport protocols and ports used in the reference configuration.

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

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 Communication Manager (e.g., **sm63_ACM63_public**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for the Main Session Manager (e.g., **sm63**).
- **SIP Entity 1 Port** – Enter **5062**.
- **Protocol** – Select **TCP** (see **Section 6.8.1**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.3** for the Communication Manager public entity (e.g., **ACM63_public**).
- **SIP Entity 2 Port** - Enter **5062** (see **Section 6.8.1**).
- **Connection Policy – Select Trusted**.

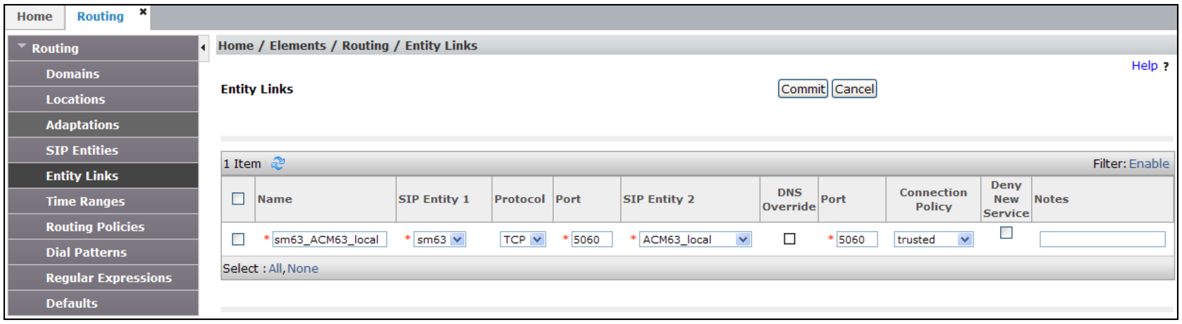
Step 3 - Click on **Commit**.



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

To configure this Entity Link, repeat the steps in **Section 5.5.1**, with the following changes:

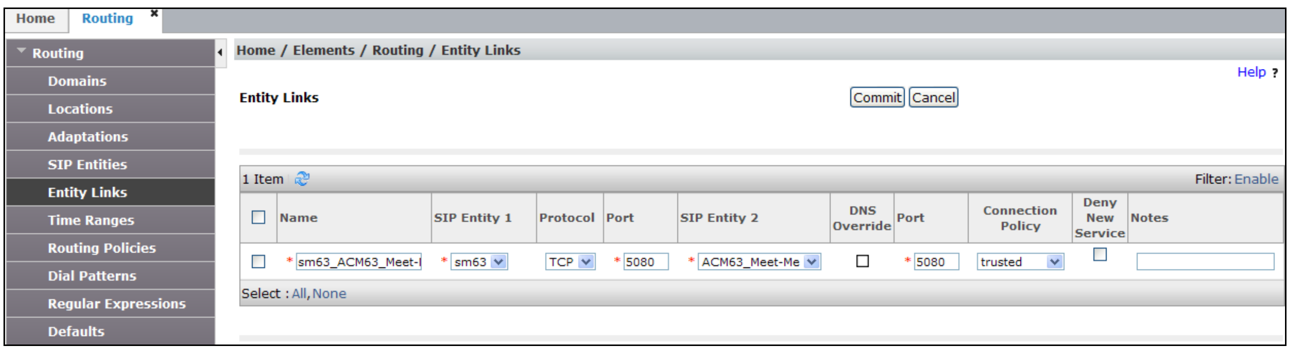
- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **sm63_ACM63_local**).
- **SIP Entity 1 Port** – Enter **5060**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.4** for the Communication Manager public entity (e.g., **ACM63_local**).
- **SIP Entity 2 Port** - Enter **5060** (see **Section 6.8.2**).



5.5.3. Main Session Manager Entity Link to Main Avaya Aura® Communication Manager – Meet-Me Trunk

To configure this Entity Link, repeat the steps in **Section 5.5.1**, with the following changes:

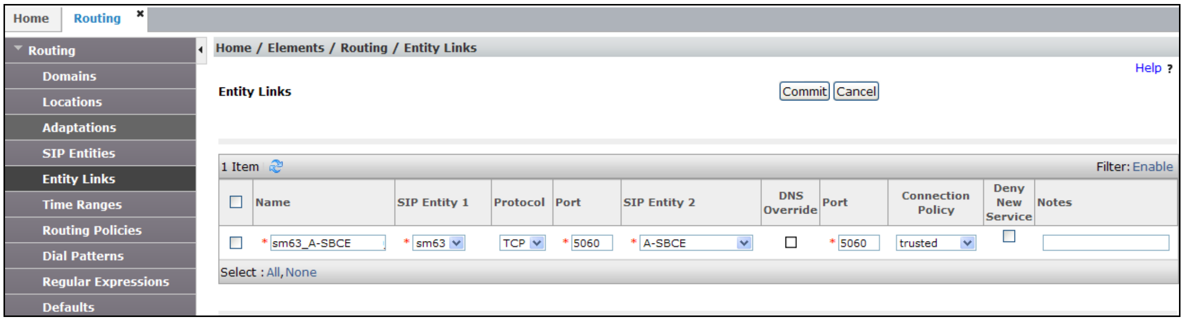
- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **sm63_ACM63_Meet-Me**).
- **SIP Entity 1 Port** – Enter **5080**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.5** for the Communication Manager public entity (e.g., **ACM63_Meet-Me**).
- **SIP Entity 2 Port** - Enter **5080** (see **Section 6.8.3**).



5.5.4. Main 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 5.5.2**, with the following changes:

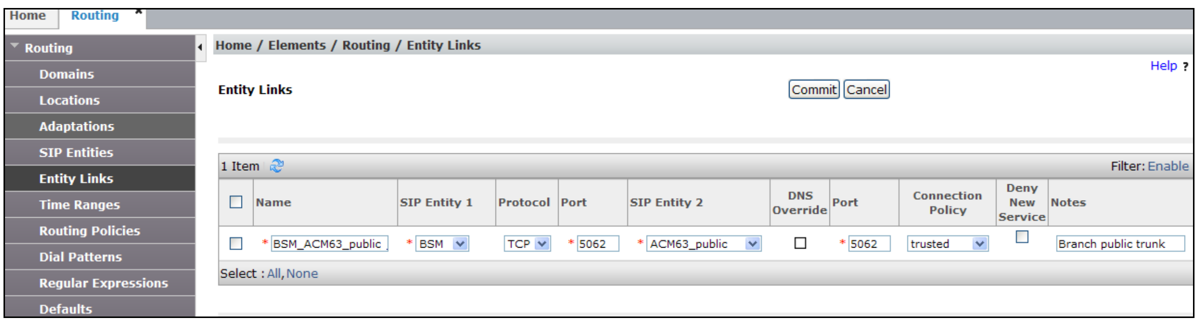
- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **sm63_A-SBCE**).
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.7** for the Communication Manager public entity (e.g., **A-SBCE**).



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

To configure this Entity Link, follow the steps in **Section 5.5.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **BSM_ACM63_public**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.2** for the Branch Session Manager (e.g., **BSM**).



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

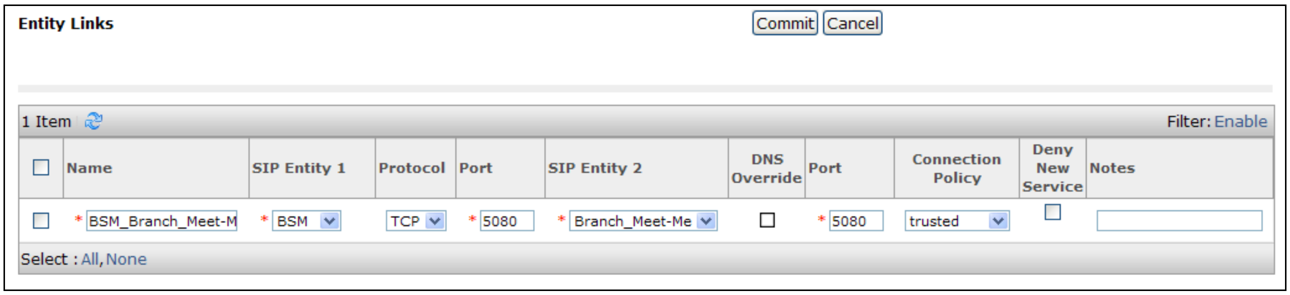
To configure this Entity Link, follow the steps shown in **Section 5.5.2** with the following changes:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **BSM_ACM63_local**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.2** for the Main Session Manager (e.g., **BSM**).

5.5.7. Branch Session Manager Entity Link to Branch Avaya Aura® Communication Manager – Meet-Me Trunk

To configure this Entity Link, follow the steps shown in **Section 5.5.3** with the following changes:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **BSM_Branch_Meet-Me**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.2** for the Branch Session Manager (e.g., **BSM**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.6** for the Branch Session Manager Meet-Me conference (e.g., **Branch_Meet-Me**).



5.5.8. Branch Session Manager Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE

To configure this Entity Link, follow the steps shown in **Section 5.5.4** with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **BSM_A-SBCE**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.2** for the Branch Session Manager (e.g., **BSM**).

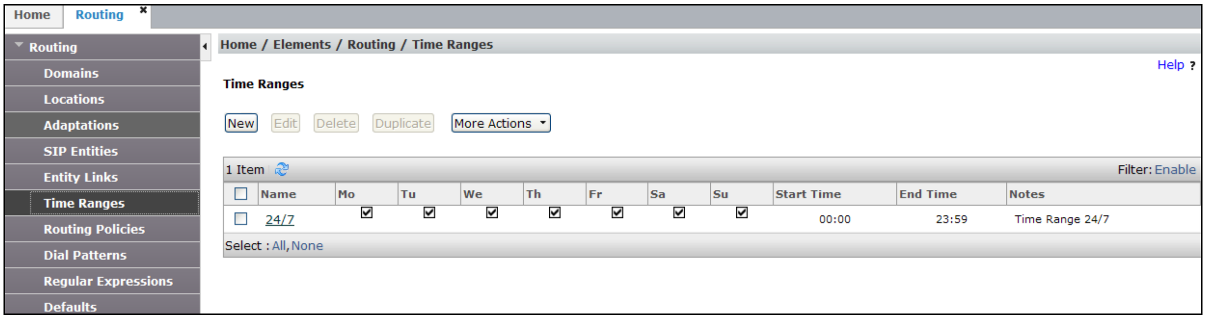
5.6. Time Ranges – (Optional)

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.



5.7. Routing Policies

In this section, the following Routing Policies are administered:

- Inbound calls to Communication Manager extensions from AT&T (**Section 5.7.1**).
- Inbound calls to Main Communication Manager Meet-Me Conference from AT&T (**Section 5.7.2**).
- Inbound calls to Branch Communication Manager Meet-Me Conference from AT&T (**Section 5.7.3**).
- Outbound calls to AT&T/PSTN (**Section 5.7.4**).

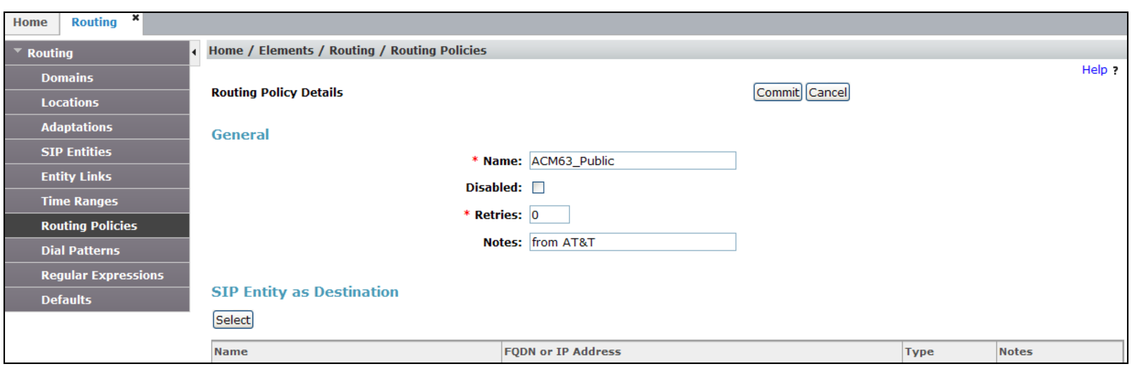
5.7.1. Routing Policy for AT&T Routing to Avaya Aura® Communication Manager

This Routing Policy is used for inbound calls from AT&T, and will be used whether Communication Manager is active in the Main or Branch site.

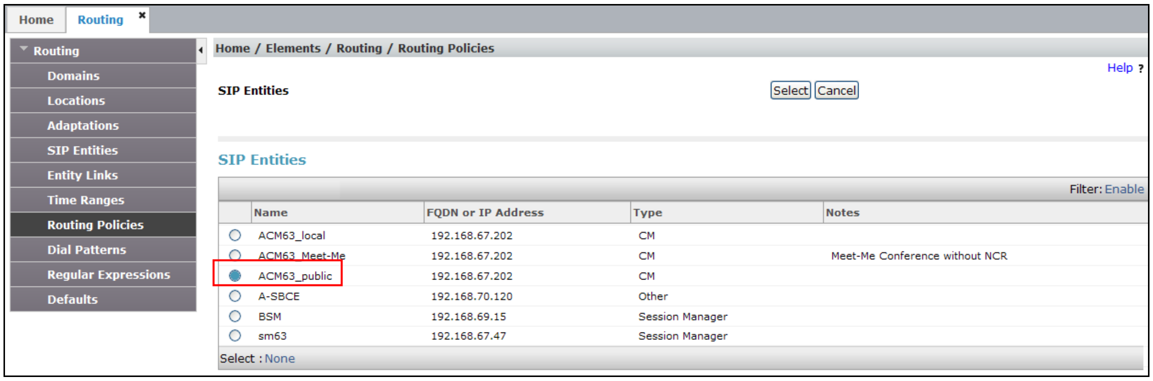
Step 1 - In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., **ACM63_Public**), 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 5.4.3** for the Communication Manager public SIP Entity (**ACM63_Public**), and click on **Select**.



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

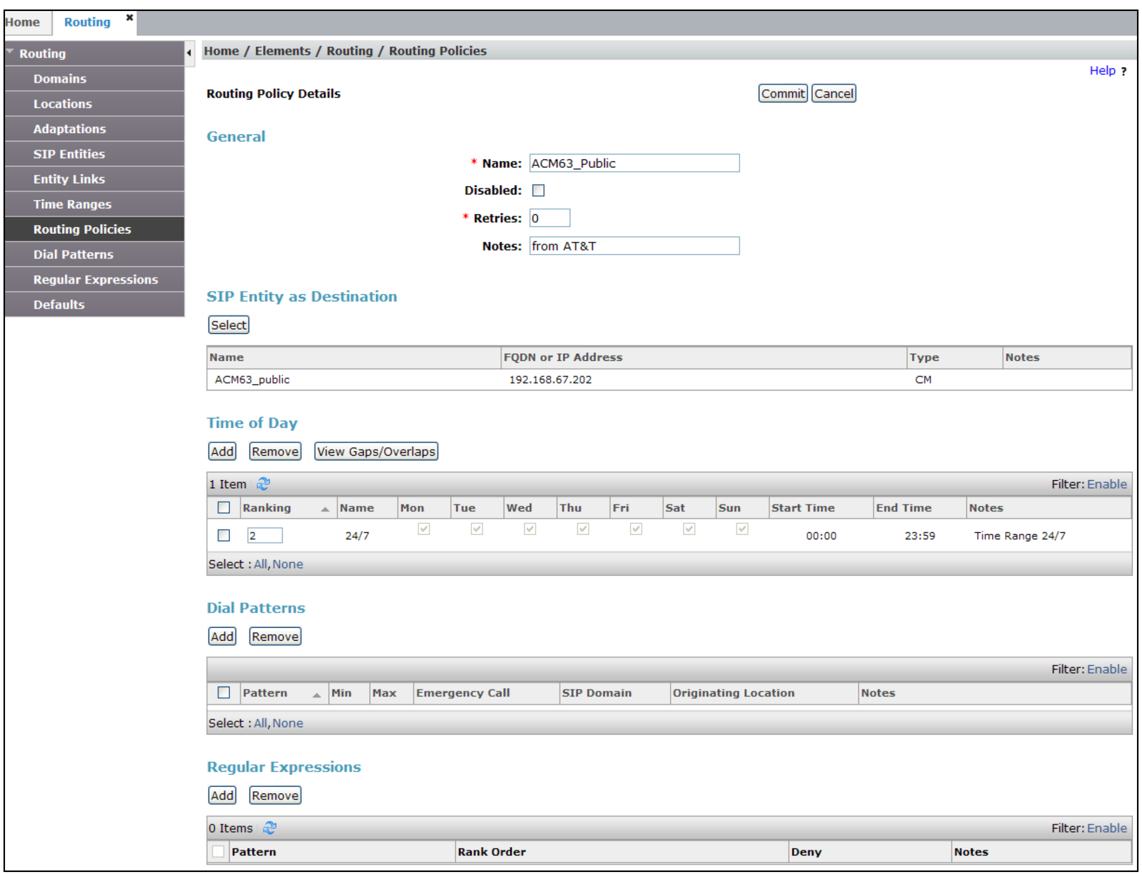
Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.

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 - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.

Step 9 - No **Regular Expressions** were used in the reference configuration.

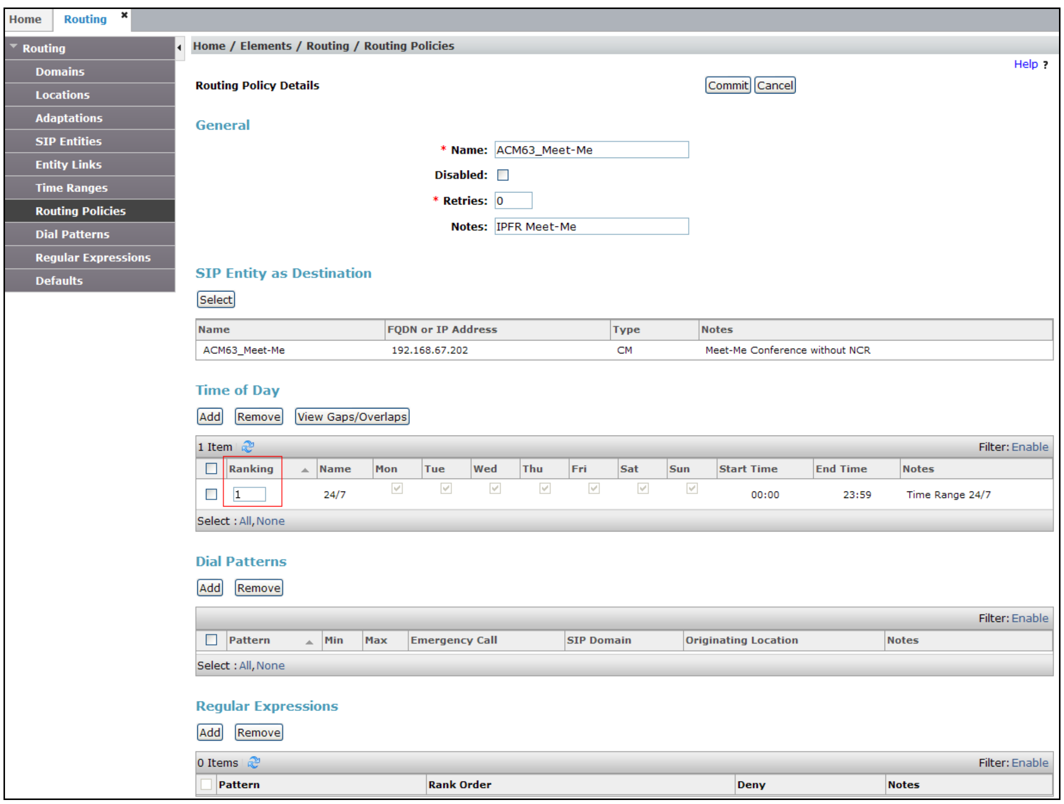
Step 10 - Click on **Commit**.



5.7.2. Routing Policy for Inbound Routing to Avaya Aura® Communication Manager Meet-Me Conference – Main Site

As described in **Section 2.2.1**, **Item 3**, an issue was found with Meet-Me conference calls when Network Call Redirection (NCR) is enabled on Communication Manager. This requires Meet-Me conference calls to use a separate SIP trunk with NCR disabled. As a result separate routing is required to deliver Meet-Me conference calls to this trunk. Repeat the steps in **Section 5.7.1** with the following differences:

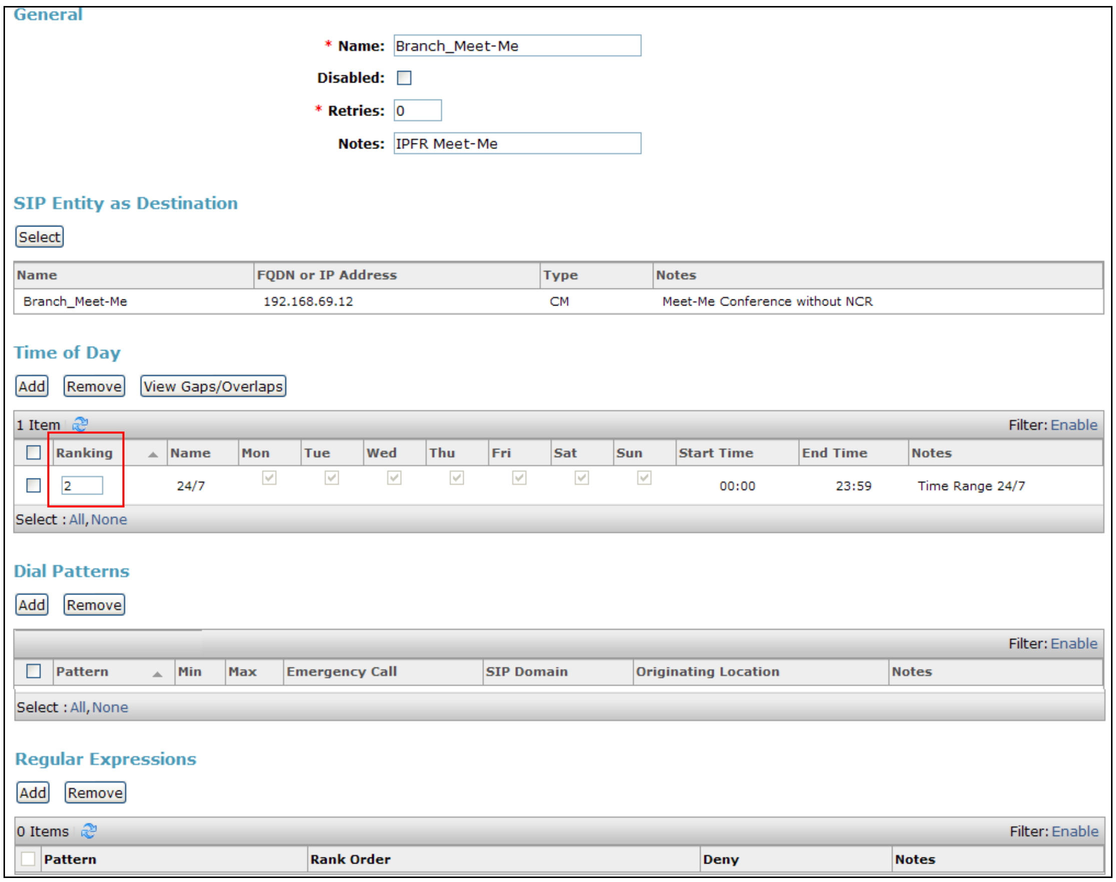
- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g. **ACM63_Meet-Me**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.5** for the Main Communication manager Meet-Me conference (e.g. **ACM63_Meet-Me**).
- In the **Time of Day** section, change the ranking number to **1**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.



5.7.3. Routing Policy for Inbound Routing to Avaya Aura® Communication Manager Meet-Me Conference – Branch Site

Repeat the steps in **Section 5.7.2** with the following differences:

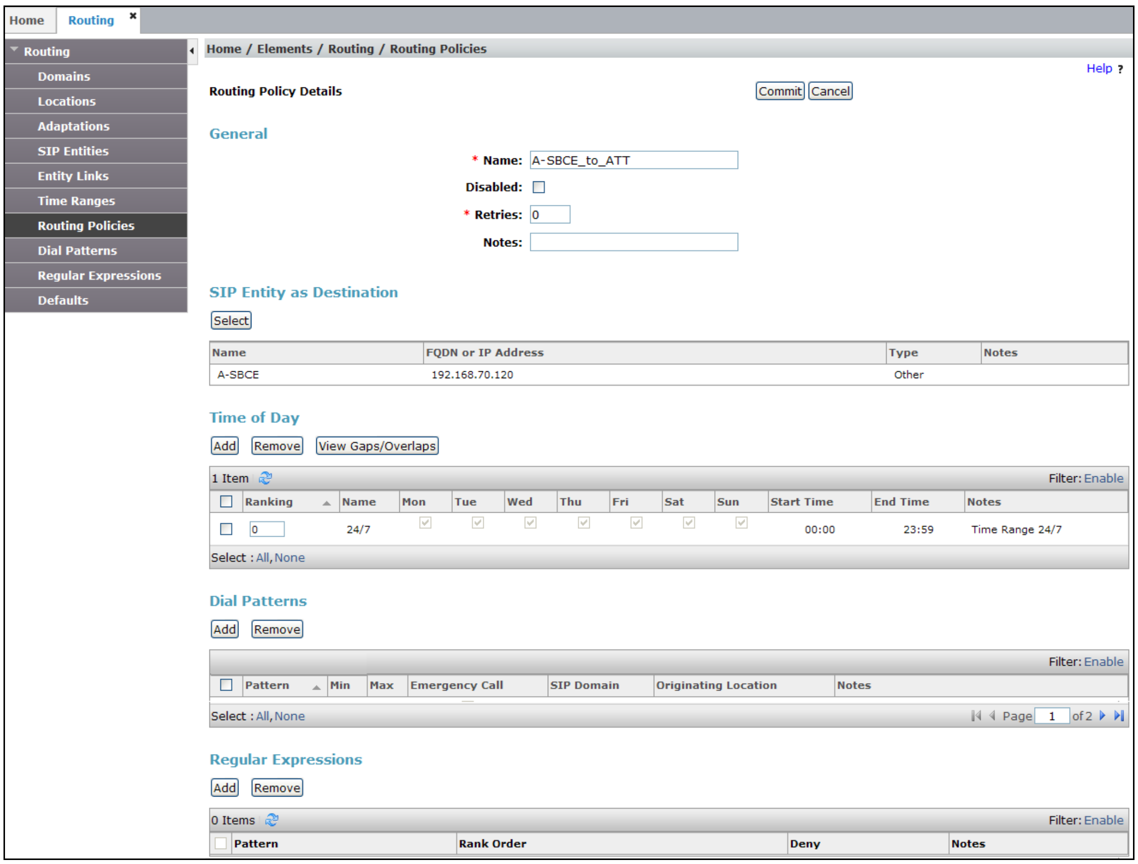
- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g. **Branch_Meet-Me**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.6** for the Branch Communication manager Meet-Me conference (e.g. **Branch_Meet-Me**).
- In the **Time of Day** section, change the ranking number to **2**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.



5.7.4. Routing Policy for Outbound Calls to AT&T

This Routing Policy is used for Outbound calls to AT&T. Repeat the steps in **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to the AT&T IPFR-EF service via the Avaya SBCE (e.g. **A-SCBE_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 5.4.7** for the Avaya SBCE SIP Entity (e.g. **A-SBCE**).
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.



5.8. Dial Patterns

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

- Inbound PSTN calls via the IPFR-EF service to the Main Communication Manager (**Section 5.8.1**). See the note in **Section 5.4** regarding Dial Patterns used to access the Branch Branch Communication Manager.
- Outbound calls to AT&T (**Section 5.8.2**).
- Inbound calls to Communication Manager Meet-Me conference, Main and Branch site (**Section 5.8.3**).

5.8.1. Matching Inbound PSTN Calls to Avaya Aura® Communication Manager

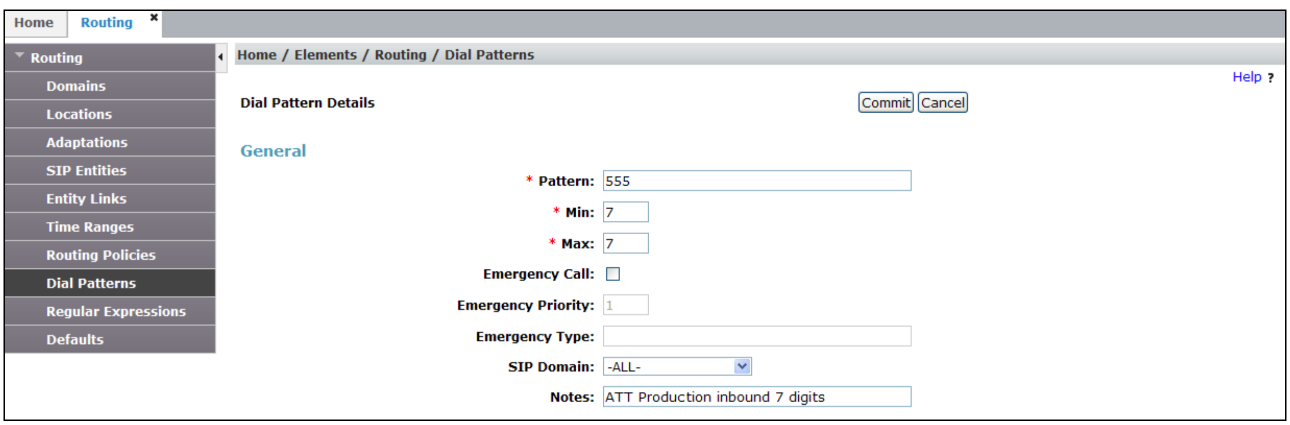
In the reference configuration inbound calls from the IPFR-EF service used 7 digits in the SIP Request URI. This pattern is matched for further call processing.

Note – Be sure to match on the digit string specified in the AT&T Request URI, not the 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** – In the reference configuration, AT&T sends a 7 digit number in the Request URI with the format 555xxxx. Enter **555**. Note - The Adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 555xxxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **7**.
- **SIP Domain** – Select **-ALL-**, to select all of the administered SIP Domains.

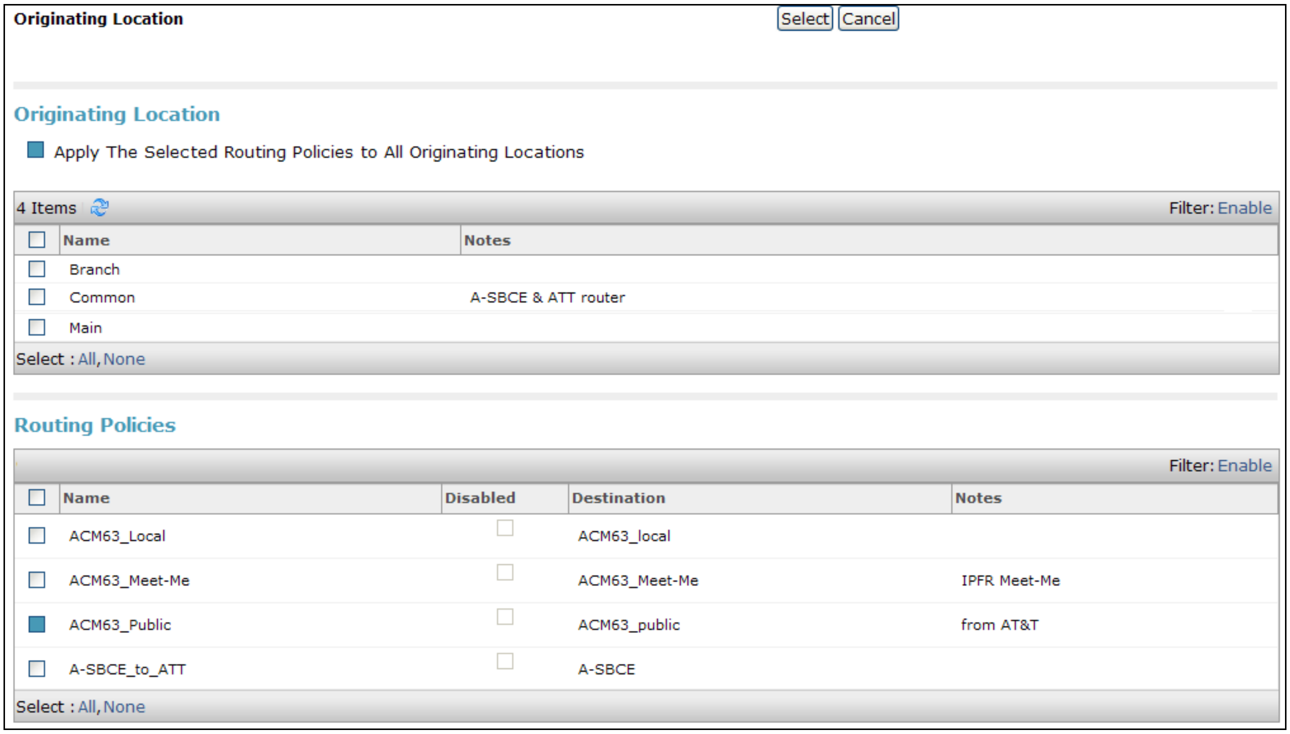


Step 3 – Scrolling down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on **Add**.

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 the Communication Manager public trunk in **Section 5.7.1** (e.g., **ACM63_Public**).

Step 6 – Click on **Select**.



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

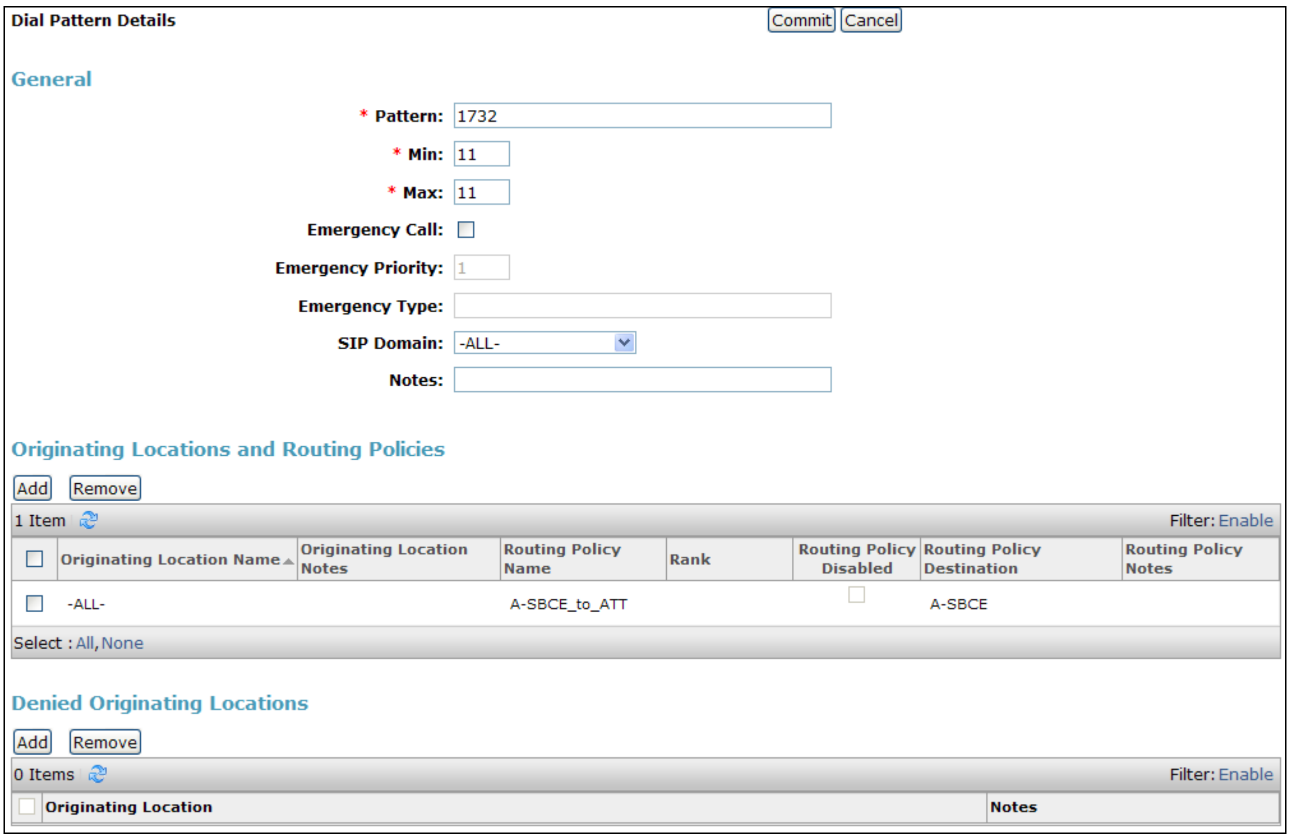
Step 8 - Repeat **Steps 1-7** for any additional inbound dial patterns.

5.8.2. Matching Outbound Calls to AT&T

In this section, Dial Patterns are administered for all outbound calls to AT&T. In the reference configuration 1xxxyyyxxxx, x11, and 011 international calls were verified. In addition, IPFR-EF Call Forward feature access codes (e.g., *7Xyyyzzzxxxx & *9Xyyyzzzxxxx) were verified.

Step 1 - Repeat the steps shown in **Section 5.8.1**, with the following changes:

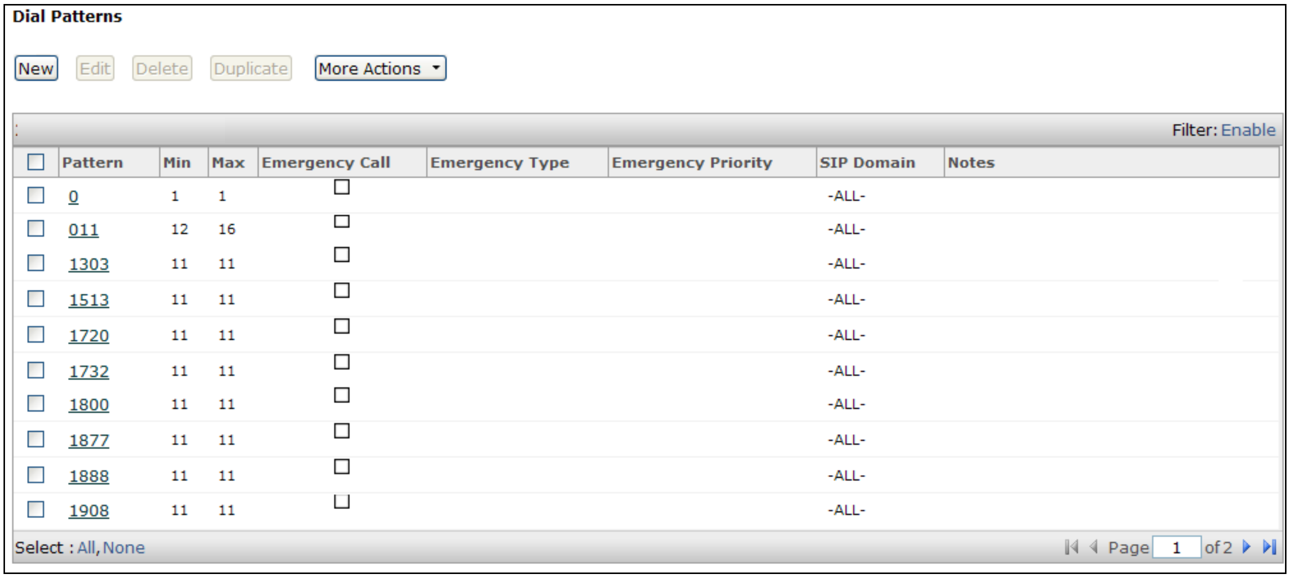
- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to AT&T/PSTN (e.g. **1732**).
- Enter a **Min** and **Max** pattern of **11**.
- In the **Routing Policies** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to the Routing Policy administered for routing calls to AT&T in **Section 5.7.4** (e.g., **A-SBCE_to_ATT**).



Step 2 - Repeat **Step 1** to add patterns for IPFR-EF Call Forward access codes with patterns ***7** and ***9**, and **Min/Max=13.**

Step 3 - Repeat **Step 1** to add patterns for international calls with pattern **011** with **Min=11** and **Max=16**.

Step 4 - Repeat **Step 1** to add any additional outbound patterns.



Dial Patterns

New | Edit | Delete | Duplicate | More Actions

Filter: Enable

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
0	1	1	☐			-ALL-	
011	12	16	☐			-ALL-	
1303	11	11	☐			-ALL-	
1513	11	11	☐			-ALL-	
1720	11	11	☐			-ALL-	
1732	11	11	☐			-ALL-	
1800	11	11	☐			-ALL-	
1877	11	11	☐			-ALL-	
1888	11	11	☐			-ALL-	
1908	11	11	☐			-ALL-	

Select : All, None

Page 1 of 2

5.8.3. Matching Inbound Calls to Avaya Aura® Communication Manager Meet-Me Conference – Main and Branch Sites

As described in **Section 2.2.1**, **Item 3**, an issue was found with Meet-Me conference calls when Network Call Redirection (NCR) is enabled on Communication Manager. This requires Meet-Me conference calls to use a separate SIP trunk with NCR disabled. As a result a specific IPFR-EF access number(s) must be selected for user to generate inbound Meet-Me conference calls. This unique Dial Pattern is required to deliver Meet-Me conference calls to this dedicated trunk. In addition, separate Dial Patterns must be defined for the Main and Branch sites, because different extensions are used to defined the Meet-Me VDN at each site.

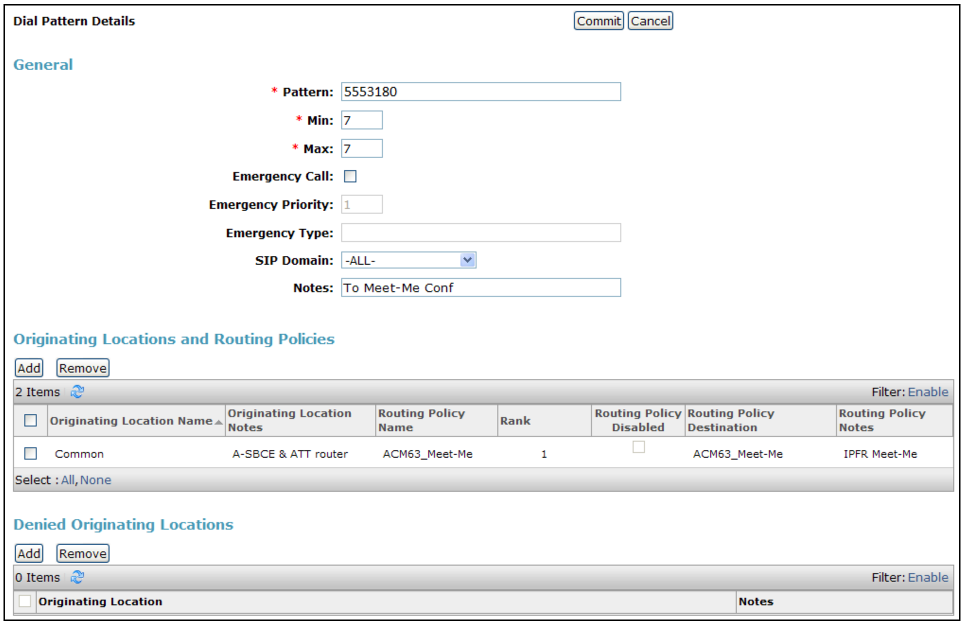
In the reference configuration, the designated Meet-Me conference IPFR-EF access number generates a R-URI with the digits 5553180.

5.8.3.1 Dial Pattern – Main Site Meet-Me VDN Extension

In the reference configuration the Main Communication Manager extension 19000 was used for the Meet-Me VDN in the Main site (see **Section 6.16.2**).

Step 1 – Repeat the steps in **Section 5.8.1** with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern matching the IPFR-EF access number selected for inbound Meet-Me conference calls (e.g., **5553180**).
- In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to Location **Common** (**Section 5.2.3**).
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy **ACM63_Meet-Me** (**Section 5.7.2**).

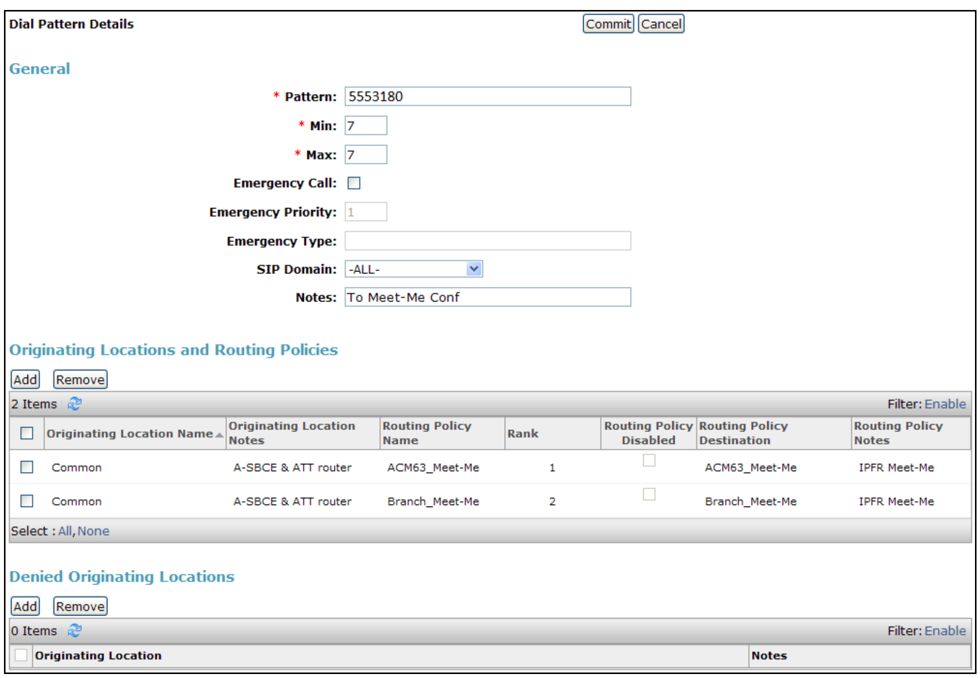


5.8.3.2 Dial Pattern – Branch Site Meet-Me VDN Extension

In the reference configuration the Branch Communication Manager extension 30013 was used for the Meet-Me VDN in the Branch site (see **Section 6.16.4**).

Step 1 – Repeat the steps in **Section 5.8.3.1** with the following differences:

- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy **Branch_Meet-Me** (**Section 5.7.3**).



6. Configure Avaya Aura® Communication Manager

Note – The following provisioning is performed on the Main Communication Manager. However, when the provisioning is saved (**see Section 6.17**), it is saved to the Branch Communication Manager as well.

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 **[4 & 5]** and 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.

6.1. 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 **Enhanced EC500?**, **IP Stations?**, **IP Trunks?**, and **ISDN/SIP Network Call Redirection?** fields are set to **y**.

Note that the Main Communication Manager **Local Survivable Processor** option is set to **n**.

```
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.)
```

Step 5 - On **Page 5** of the form, verify that the **Private Networking** and **Processor Ethernet** fields are set to **y**.

```
display system-parameters customer-options                      Page   5 of  11
                                OPTIONAL FEATURES
              Multinational Locations? n           Station and Trunk MSP? y
 Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                   Multiple Locations? n
                                            System Management Data Transfer? n
         Personal Station Access (PSA)? y              Tenant Partitioning? y
                      PNC Duplication? n       Terminal Trans. Init. (TTI)? y
                 Port Network Support? y               Time of Day Routing? y
                      Posted Messages? y       TN2501 VAL Maximum Capacity? y
                                                      Uniform Dialing Plan? y
                   Private Networking? y     Usage Allocation Enhancements? y
            Processor and System MSP? y
                   Processor Ethernet? y                Wideband Switching? y
                                                                  Wireless? n
                        Remote Office? y
         Restrict Call Forward Off Net? y
                Secondary Data Module? y

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

6.2. 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
      Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

6.3. 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 extensions in the Main site.
  - The digit **3** for Communication Manager extensions in the Branch site.
- 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 6.8**.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**), e.g., access code **8** for Automatic Alternate Routing dialing, see **Section 6.12**.
- 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 6.11**.

```
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
   6            3   dac
   8            1   fac
   9            1   fac
   *            3   fac
   #            3   fac
```

6.4. IP Node Names

Node names define IP addresses to various Avaya components in the enterprise. Note that a Processor Ethernet (procr) based Communication Manager platform is used in the reference configuration for the Main Communication Manager, (the Branch Communication Manager is a procr based platform as well). The Main Communication Manager procr IP address was used to define the Communication Manager SIP Entities in **Section 5.4**.

Step 1 - Enter the **change node-names ip** command, and add a node name and IP address for the following:

- Avaya SBCE private network interface (e.g., **A-SBCE** and **192.168.70.120**).
- Branch Session Manager SIP signaling interface (e.g., **BSM** and **192.168.69.15**).
- Branch Communication Manager (e.g., **S8300D** and **192.168.69.12**).
- Session Manager SIP signaling interface (e.g., **SM63** and **192.168.67.47**).
- Note that the Main 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
BSM                 192.168.69.15
S8300D              192.168.69.12
SM63                192.168.67.47
default             0.0.0.0
procr               192.168.67.202
procr6              ::
```

6.5. 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
```

6.6. 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 Main site (region 1), one for the AT&T SIP trunk (region 2), and one for the Branch site (region 3).

6.6.1. IP Network Region 1 – Main Site 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:

a) Enter a descriptive name (e.g., **Main**).

- Enter the enterprise domain (e.g., **customera.com**) in the **Authoritative Domain** field (see **Section 5.1**).
- 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.
- Next to region **3** in the **dst rgn** column, enter **1** for the codec set (this means region 1 is permitted to talk to region 3 and it will use codec set 1 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
 3    1     y    NoLimit                                             n       t
```

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

Repeat the steps in **Section 6.6.1** 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**.
- Set codec set **2** for **dst rgn 3**.
- 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
 3    2     y    NoLimit                                             n       t
```

6.6.3. IP Network Region 3 – Branch Site Region

Repeat the steps in **Section 6.6.1** with the following changes:

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

- Enter a descriptive name (e.g., **Branch**).
- Enter **1** for the **Codec Set** parameter.

Step 2 – On **Page 3** of the form:

- In line **1** of the **Backup Servers** field, enter the node name of the Branch LSP, defined in **Section 6.4**, (e.g., **S8300D**).
- Use defaults for all other values on this page.

```
change ip-network-region 3                                      Page   3 of  20
                               IP NETWORK REGION
INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
 Incoming LDN Extension:
 Conversion To Full Public Number - Delete:    Insert:
 Maximum Number of Trunks to Use for IGAR:
 Dial Plan Transparency in Survivable Mode? n
BACKUP SERVERS(IN PRIORITY ORDER)     H.323 SECURITY PROFILES
 1   S8300D                           1   challenge
 2                                    2
 3                                    3
 4                                    4
 5
 6                                    Allow SIP URI Conversion? y
TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
   Near End Establishes TCP Signaling Socket? y
                       Near End TCP Port Min: 61440
                       Near End TCP Port Max: 61444
```

Step 3 – On **Page 4** of the form:

- Set codec set **1** for **dst rgn 1**.
- Set codec set **2** for **dst rgn 2**.
- Note that **dst rgn 3**is pre-populated with codec set **1** (from page 1 provisioning).

```
change ip-network-region 3                                      Page   4 of  20
 Source Region: 3     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     y    NoLimit                                             n       t
 2    2     y    NoLimit                                             n       t
 3    1                                                                all
```

6.7. IP Codec Parameters

6.7.1. Codecs for IP Network Region 1 (calls to/from the Main Site)

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**). On **Page 1** of the **ip-codec-set** form, ensure that **G.711MU**, **G.729A**, and **G.729B** are included in the codec list. Note that the packet interval size will default to 20ms.

```
change ip-codec-set 1                                           Page   1 of   2
                          IP Codec Set
    Codec Set: 1
    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.729A           n          2        20
 3: G.729B           n          2        20
```

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

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

6.7.2. Codecs for IP Network Region 2 (calls to/from AT&T)

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g., **2**). This IP codec set will be used for IPFR-EF calls. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown, however the order of G.729B and G.729A may be reversed as required. Set **3** for the **Frames Per Pkt**. This will automatically populate **30** for the Packet Size (ms).

```
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          2        30
```

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

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

6.8. SIP Trunks

Three SIP trunks are defined on Communication Manager in the reference configuration:

- AT&T access – SIP Trunk 2
  - Note that this trunk will use TCP port 5062 as described in **Section 5.5.1**.
- Avaya SIP telephone access – SIP Trunk 1
  - Note that this trunk will use TCP port 5060 as described in **Section 5.5.2**.

- Avaya Meet-Me conference access – SIP Trunk 3
    - Note that this trunk will use TCP port 5080 as described in **Section 5.5.3**.

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group.

Note – Although TCP is used as the transport protocols between the Avaya CPE components, UDP was used between the Avaya SBCE and the IPFR-EF service. See the note in **Section 5.4** regarding the use of TCP and TLS transport protocols in the CPE.

6.8.1. SIP Trunk for AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager (and the BSM) used for IPFR-EF calls. This trunk corresponds to the **ACM63_Public** SIP Entity defined in **Section 5.4.3**.

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 6.4**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.4** (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 6.6.2**.
- **Far-end Domain** – Enter **customera.com**. This is the domain provisioned for Session Manager in **Section 5.1**.
- **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.
- Verify that **Initial IP-IP Direct Media** is set to **n** (default). See **Item 6** in **Section 2.2.1**.
- 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                                               Page   1 of  21
                                 TRUNK GROUP
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** is set to **y**. See **Section 2.2.1, Item 3** regarding the use of Network Call Redirection (NCR) with Meet-Me conference.
- Set **Send Diversion Header** to **y**. This is required for Communication Manager station Call Forward scenarios to IPFR-EF service.
- Set **Telephone Event Payload Type** to the RTP payload type recommended by the IPFR-EF service (e.g., **100**).
- Set **Identity for Calling Party Display** to **From**. Note that he display issue described in **Section 2.2.1**, **Item 5** may be resolved by setting the ***Identity for Calling Party Display:*** parameter to ***From***. However this parameter is only available on Communication Manager 6.x platforms.

> **Note** – The IPFR-EF service does not support History Info header. As shown below, by default this header is supported by Communication Manager. In the reference configuration, the History Info header is automatically removed from SIP signaling by Session Manager, as part of the AttAdapter (see **Section 5.3.2**). Alternatively, History Info may be disabled here.

```
add trunk-group 2                                               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? 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: From
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

6.8.2. Local SIP Trunk (Avaya SIP Telephone Access)

This trunk corresponds to the **ACM63_Local** SIP Entity defined in **Section 5.4.4**.

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 6.8.1** with the following changes:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.6.1**.

```
add signaling-group 1                                           Page   1 of   1
                                SIGNALING GROUP
 Group Number: 1             Group Type: sip
  IMS Enabled? n       Transport Method: tcp
        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: 5060                 Far-end Listen Port: 5060
                                         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 6.8.1** 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 6.8.1**.

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

- Same as **Section 6.8.1**.

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

- Set **Network Call Redirection** to **n**.
- Set **Diversion header** to **n**.
- 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
```

6.8.3. SIP Trunk for Meet-Me Conference Calls

This trunk corresponds to the **ACM63_Meet-Me** SIP Entity defined in **Section 5.4.5**.

Step 1 – Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **5**), and repeat the steps in **Section 6.8.1** with the following changes:

- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5080**
- **Far-end Network Region** – Set to the IP network region **2**, as defined in **Section 6.6.2**.

```
add signaling-group 5                                           Page   1 of   1
                                SIGNALING GROUP
 Group Number: 5              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        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: 5080                 Far-end Listen Port: 5080
                                         Far-end Network Region: 2
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., **5**). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 6.8.1** with the following changes:

- **Group Name** – Enter a descriptive name (e.g., **Meet-Me_Conf**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **605**).
- **Service Type** – Set to **public-ntwrk**
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **5**).

```
add trunk-group 5                                               Page   1 of  21
                                TRUNK GROUP
Group Number: 5                    Group Type: sip           CDR Reports: y
  Group Name: Meet-Me_Conf                COR: 1        TN: 1        TAC: 605
   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: 5
                                                    Number of Members: 10
```

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

- Same as **Section 6.8.1**.

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

- Same as **Section 6.8.1**.

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

- Set **Network Call Redirection** to **n**.
- Set **Diversion header** to **n**.
- Use default values for all other settings.

```
add trunk-group 5                                               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: From
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                              Enable Q-SIP? n
```

6.9. Private Numbering

In the reference configuration, the private-numbering form, (used in conjunction with the **Numbering Format: private** setting in **Section 6.8.1**), is used to convert Communication Manager local extensions to IPFR-EF DNIS numbers, for inclusion in any SIP headers directed to the IPFR-EF service via the public trunk.

Step 1 – 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 6.3** (e.g., **1** and **3**).
- **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 Communication Manager extensions for the Main (19xxx) and Branch (3xxxx) sites, and their corresponding IPFR-EF DNIS numbers (for the public trunk to AT&T):

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter a Communication Manager 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., **7325553170**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 4 – Repeat **Step 3** for all IPFR-EF DNIS numbers and their corresponding Communication Manager extensions.

```
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   19001          2           7325553170        10
         5   19002          2           7325553171        10
         5   30001          2           7325553177        10
         5   30002          2           7325553178        10
```

6.10. Route Patterns

Route Patterns are used to direct calls to the public (e.g., AT&T access) and local (e.g., Avaya SIP telephone) SIP trunks.

6.10.1. 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 6.11**. 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 6.8.1**).

```
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
```

6.10.2. Route Pattern for Calls to Avaya SIP Telephones

This form defines the local SIP trunk, based on the route-pattern selected by the AAR table in **Section 6.12** (e.g., calls to Avaya SIP telephone extensions).

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
```

6.11. 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 6.3**. 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 6.10.1**).

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

6.12. Automatic Alternate Routing (AAR) Dialing

AAR is used to direct coverage calls for Avaya SIP telephone extensions to route-pattern 1 defined in **Section 6.10.2**.

Step 1 – Enter the following:

- **Dialed String –** Enter **19** (Main site extensions including SIP telephones).
- **Min** & **Max** – Enter **5**.
- **Route Pattern** – Enter **1**.
- **Call Type** – Enter **aar**.
- **Step 2** – Repeat **Step 1** specifying **30** as the **Dialed String** (Branch site extensions including SIP telephones).

```
change aar analysis 0                                                  Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1
          Dialed            Total      Route     Call    Node  ANI
          String           Min  Max   Pattern    Type    Num   Reqd
    19                     5    5      1         aar           n
    30                     5    5      1         aar           n
```

6.13. Media Gateway Recovery Rule

When Media Gateways are provisioned for fail-over, a recovery rule is applied that determines how the Media Gateway will recover from that failure.

Step 1 – Enter the command **cha system-parameters mg-recovery rule x**, where x is the rule identifier (e.g., **1**).

Step 2 – Enter the following on the form:

- **Rule Name**: Enter a descriptive name (e.g., **Branch**).
- **Migrate H.248 MG to primary**: The value **immediately** was used in the reference configuration to facilitate fail-over testing. Other options may be used as required. This entry means that the Media Gateway will attempt to reregister back to the Main Communication as soon as connections are reestablished, (based on the timer below), without waiting for active calls to complete. Calls that are active will remain connected, but features will not be available to them (see the note on the form).
- **Minimum time of network stability:** Use the default value of **3** (minutes). This value determines how long the Media Gateway will wait before reregistering. The delay helps avoid "toggling" conditions when the connection state is erratic.

```
change system-parameters mg-recovery-rule 1                            Page   1 of   1
             SYSTEM PARAMETERS MEDIA GATEWAY AUTOMATIC RECOVERY RULE
 Recovery Rule Number: 1
 Rule Name: Branch
 Migrate H.248 MG to primary: immediately
 Minimum time of network stability: 3
 WARNING: The MG shall be migrated at the first possible opportunity. The MG may
 be migrated with a number of active calls.  These calls shall have their talk
 paths preserved, but no additional processing of features shall be honored.
 The user must hang up in order to regain access to all features.
 NOTE: set 'Migrate H.248 MG to primary' to Blank to disable rule.
```

6.14. Avaya Media Gateway Provisioning

In the reference configuration, two Media Gateways are provisioned, a G430 and a G450. The G430 is located in the Main site and is used for local DSP resources, announcements, Music On Hold, etc. The G450 is also used for similar functions in the Branch location; however the G450 is also used as the platform for the S8300D Local Survivable Processor (LSP).

Note – Only the Media Gateway provisioning associated with the fail-over functionalities described in these application notes, are shown below. See **[6 & 7]** for more information of Media Gateway provisioning.

In addition, the *MOH.wav* file was used as the Music on Hold source in the reference configuration. Other music sources, including external sources, may be used; however, options and methods for generating Music on Hold is beyond the scope of this document.

6.14.1. G430 Provisioning

6.14.1.1 G430 Registration to the Main Communication Manager

The G430 in the Main site only registers to the Main Communication Manager.
Step 1 – Use SSH to connect to the G430. Note that the Media Gateway prompt will contain ??? if the Media Gateway is not registered to Communication Manager (e.g., ***G430-???(super)#***).
Step 2 - Enter the **show system** command and copy down the G430 serial number (e.g., **10IS04271590**).
Step 3 – Enter the **set mgc list x.x.x.x** command where x.x.x.x is the IP address of the Main Communication Manager Procr (e.g., **192.168.67.202**, see **Section 6.4**).
Step 4 – Enter the **copy run copy start command** to save the G430 configuration.
Step 5 – On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **1**). The Media Gateway form will open (not shown). Enter the following parameters:

- Set **Type** = **g430**
- Set **Name** = Enter a descriptive name (e.g., **G430**)
- Set **Serial Number** = Enter the serial number copied from Step 2 (e.g., **10IS04271590**).
- Set the **Encrypt Link** parameter as desired (**n** was used in the reference configuration).
- Set **Network Region** = **1**

Wait a few minutes for the G430 to register to the Main Communication Manager. When the Media Gateway registers, the G430 SSH connection prompt will change to reflect the Media Gateway Identifier assigned in **Step 5** (e.g., ***G430-001(super)#***).
Step 6 – Enter the **display media-gateway 1** command, and verify that the G430 has registered.

Note that the **Recovery Rule** is set to **None** (default).

```
display media-gateway 1                                          Page   1 of   2
                             MEDIA GATEWAY 1
                    Type: g430
                    Name: g430
               Serial No: 10IS04271590
            Encrypt Link? n                  Enable CF? n
          Network Region: 1                   Location: 1
                                             Site Data:
           Recovery Rule: none
              Registered?  y
   FW Version/HW Vintage: 34 .5  .1  /1
       MGP IPV4 Address: 192.168.67.50
       MGP IPV6 Address:
   Controller IP Address: 192.168.67.202
             MAC Address: 00:1b:4f:3c:52:59
```

Step 8 – Enter the **change media-gateway 1** command, and go to **page 2**. Enter **gateway-announcements** at the **v9:** parameter.

```
change media-gateway 1                                          Page   2 of   2
                             MEDIA GATEWAY 1
                                 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
```

Step 9 – After entering this parameter you will be prompted to activate the announcement board. Enter the command **enable announcement-board 1v9**.

6.14.2. G450 Provisioning

6.14.2.1 G450 Registration to the Main Communication Manager

The G450 in the Branch site registers to the Main Communication Manager under normal circumstances. However, if contact with the Main site is lost, the G450 must reregister to the Branch Branch Communication Manager when it activates. Repeat the steps in Section **6.14.1.1**, with the following changes:

Step 1 – Enter the **set mgc list x.x.x.x,y.y.y.y** command where x.x.x.x is the IP address of the Main Communication Manager Procr (e.g., **192.168.67.202**, see **Section 6.4**), and y.y.y.y is the IP address of the Branch Communication Manager S8300D (e.g., **192.168.69.12**, see **Section 6.4**). Note that the two IP addresses are separated by a comma.

Step 2 – Enter the **copy run copy start** command to save the G450 configuration**.**

Step 3 – On Communication Manager, enter the **add media-gateway x** command where x is an available Media Gateway identifier (e.g., **2**). The Media Gateway form will open (not shown). Enter the following parameters:

- Set **Type** = **g450**
- Set **Name** = Enter a descriptive name (e.g., **G450**)
- Set **Serial Number** = Enter the G450 serial number.
- Set **Network Region** = **3**
- Set **Recovery Rule** to **1** (see **Section 6.13**).

Wait a few minutes for the G450 to register to the Main Communication Manager. When the Media Gateway registers, the G450 SSH prompt will change to reflect the Media Gateway Identifier assigned in **Step 3** (e.g., ***G450-002(super)#***).

Step 4 – Enter the **display media-gateway 2** command, and verify that the G450 has registered.

```
display media-gateway 2                                            Page   1 of   2
                             MEDIA GATEWAY 2
                    Type: g450
                    Name: G450
               Serial No: 09IS53298916
            Encrypt Link? n                  Enable CF? n
          Network Region: 3                   Location: 1
                                             Site Data:
           Recovery Rule: 1
              Registered?  y
   FW Version/HW Vintage: 34 .5  .1  /1
        MGP IPV4 Address: 192.168.69.16
        MGP IPV6 Address:
   Controller IP Address: 192.168.67.202
             MAC Address: 00:1b:4f:3e:53:68
```

Step 5 – Enter the **change media-gateway 2** command, and go to **page 2**. Enter **gateway-announcements** at the **v9:** parameter.

```
change media-gateway 2                                             Page   2 of   2
                             MEDIA GATEWAY 2
                                 Type: g450
Slot   Module Type            Name                     DSP Type  FW/HW version
 V1:   S8300                  ICC MM                   MP80      112  6
 V2:
 V3:   MM711                  ANA MM
 V4:
 V5:
 V6:
 V7:
 V8:                                                 Max Survivable IP Ext: 8
 V9:   gateway-announcements  ANN VMM
```

Step 9 – After entering this parameter you will be prompted to activate the announcement board. Enter the command **enable announcement-board 2v9**.

6.15. Music on Hold

6.15.1. Music on Hold Source File

Note – The creation of Music on Hold sources and/or announcements are beyond the scope of this document. The descriptions below reference fail-over provisioning only.

The file **MOH.wav** was previously created on the G430 as a Music on Hold source. This file must be copied to the G450 Media Gateway in the Branch, so that the Branch can use it as its Music on Hold source during a fail-over.

Step 1 – On Communication Manager, enable file transfer on the G430 v9 announcement board defined in **Section 6.14.1.1**, by entering the command **enable filexfer**, using the following parameters. Note that after several minutes this login will automatically be disabled.

- **Login**: assign a login name (e.g., **file**).
- **Password** and **Reenter Password**: assign a password (e.g., **xfer**).
- **Secure:** enter **n** (setting to *n* allows FTP rather than SFTP to be used).
- **Board Address**: enter **01v9**

Step 2 – Use an FTP program such as WinSCP, to connect to the G430 v9 board, using the credentials defined above.

Step 3 – Copy off the Music on Hold source file (e.g., **MOH.wav**).

Step 4 – Repeat **Step 1** to create a file transfer account for the G450 v9 board, using **02v9** as the **Board Address**.

Step 5 – Repeat **Steps 1** and **2** to connect to the G450 v9 board, and copy the Music on Hold file downloaded from the G430, onto the G450.

6.15.2. Music on Hold Audio Group

The two Music on Hold sources created above must be specified in an Audio Group.

Step 1 – On Communication Manager, enter the command **add audio-group x**, where x is an available identifier (e.g., **1**). Enter the following values:

- Enter a **Group Name** (e.g., **MOH**).
- In source location **1:** enter **001v9** for the G430.
- In source location **2:** enter **002v9** for the G450.

Note that the lower portions of the display below were removed for brevity.

```
change audio-group 1                                            Page   1 of   5
                                 AUDIO GROUP 1
                                Group Name: MOH
AUDIO SOURCE LOCATION
  1: 001V9    16:           31:           46:           61:           76:
  2: 002V9    17:           32:           47:           62:           77:
  3:          18:           33:           48:           63:           78:
  4:          19:           34:           49:           64:           79:
  5:          20:           35:           50:           65:           80:
```

6.15.3. Music on Hold Announcement

Create an announcement that will be used as the Music on Hold source.

Step 1 – On Communication Manager enter the command **add announcement x**, where x is an available extension. Enter the following values:

- **Extension:** Enter an available extension (e.g., **19099**)
- **Annc Name:** Enter a descriptive name (e.g., **MOH**).
- **Annc Type:** Enter **iteg-mus**.
- **Group/Board:** Enter **G1** (for Group 1, defined in Section **6.15.2**).
- Use default values for the other fields.

```
add announcement 19099                                            Page   1 of   1
                       ANNOUNCEMENTS/AUDIO SOURCES
  Extension: 19099                             COR: 1
  Annc Name: MOH                                TN: 1
  Annc Type: integ-mus                      Queue? b
Group/Board: G1
  Protected? n                               Rate: 64
```

6.15.4. Music on Hold Sources

The announcement provisioned above is defined as a music source.

Step 1 – On Communication Manager, enter the command **change music-sources**. Enter the following values:

- **Source No.** : select a source number (e.g., **1**).
- **Type**: specify **music**
- **Source Type:** specify **ext 19099**
- **Description**: enter a description (e.g., **MOH**).

```
change music-sources                                                 Page   1 of   7
                                   MUSIC SOURCES
      Source No.   Type   Source                          Description

          1:       music  Type: ext   19099               MOH
          2:       none
```

6.16. Meet-Me Conference Vectors and Voice Directory Numbers (VDN)

In the reference configuration, separate VDNs, and associated Vectors, are provisioned to provide the Meet-Me conference functionality in the Main (normal conditions) and Branch (fail-over) sites.

Note – The Meet-Me Conference Vector and VDN programming is beyond the scope of this document. The Vectors and VDN shown below are examples and are included for completeness. In addition, the creation of the announcements specified in the vectors is beyond the scope of this document.

6.16.1. Main Site Meet-Me Vector

This vector greets the caller and asks for the meeting access code.

```
change vector 6                                                 Page   1 of   6
                                  CALL VECTOR
    Number: 6                Name: MeetMeConf
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? y           Lock? y
     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    5   secs hearing ringback
02 collect      6    digits after announcement 12013
03 goto step    5            if digits          =      meet-me-access
04 goto step    2            if unconditionally
05 route-to     meetme
06 stop
```

6.16.2. Main Site VDN

Note that this VDN extension is specified in the Dial Pattern in **Section 5.8**.

```
change vdn 19000                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER
                             Extension: 19000
                                  Name: MeetMeConf
                           Destination: Vector Number        6
                  Meet-me Conferencing? y
                                   COR: 1
                                    TN: 1
```

```
change vdn 19000                                                Page   2 of   3
                            VECTOR DIRECTORY NUMBER
                  MEET-ME CONFERENCE PARAMETERS:
                    Conference Access Code: *
                     Conference Controller: 19099
                           Conference Type: 6-party
```

```
change vdn 19000                                                Page   3 of   3
                            VECTOR DIRECTORY NUMBER
                                 VDN VARIABLES
                    Var  Description       Assignment
                    V1
                    V2
                    V3
                    V4
                    V5
                    V6
                    V7
                    V8
                    V9
                     VDN Time-Zone Offset  + 00:00
                     Daylight Saving Rule: system
 Use VDN Time Zone For Holiday Vectoring*? n
    Apply Ringback for Auto Answer calls*? y
```

6.16.3. Branch Site Meet-Me Vector

Note that the announcements used by the Branch site are created on the Branch G450.

```
change vector 45                                                Page   1 of   6
                                  CALL VECTOR
    Number: 45              Name: Branch_MMC
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? y           Lock? y
     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    5   secs hearing ringback
02 collect      6    digits after announcement 30011
03 goto step    5            if digits           =      meet-me-access
04 goto step    2            if unconditionally
05 announcement 30012
06 route-to     meetme
07 stop
```

6.16.4. Branch Site VDN

Note that this VDN extension is specified in the Dial Pattern in **Section 5.8**.

```
change vdn 30013                                                Page   1 of   3
                            VECTOR DIRECTORY NUMBER
                             Extension: 30013
                                  Name: Branch_MMC
                           Destination: Vector Number        45
                  Meet-me Conferencing? y
                                   COR: 1
                                    TN: 1
```

```
change vdn 30013                                                Page   2 of   3
                            VECTOR DIRECTORY NUMBER
                  MEET-ME CONFERENCE PARAMETERS:
                    Conference Access Code: *
                     Conference Controller: 30000
                           Conference Type: 6-party
```

```
change vdn 30013                                                Page   3 of   3
                            VECTOR DIRECTORY NUMBER
                                 VDN VARIABLES
                    Var  Description       Assignment
                    V1
                    V2
                    V3
                    V4
                    V5
                    V6
                    V7
                    V8
                    V9
                     VDN Time-Zone Offset  + 00:00
                     Daylight Saving Rule: system
 Use VDN Time Zone For Holiday Vectoring*? n
    Apply Ringback for Auto Answer calls*? y
```


6.17. Save Translations

After the Communication Manager provisioning is completed, it must be saved to the Main Communication Manager, as well as to the Branch Communication Manager.

Step 1 – Enter the command **save translation all**. This will save translation on the Main Communication Manager as well as the Branch Communication Manager. Note that it will take several minutes for the LSP to receive and save the translations (see **Section 8.3**).

7. Configure Avaya Session Border Controller for Enterprise

Note: Only the Avaya SBCE provisioning required for the reference configuration is described in these Application Notes.

7.1. Initial Installation/Provisioning

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to **[8]** and **[9]** for additional information.

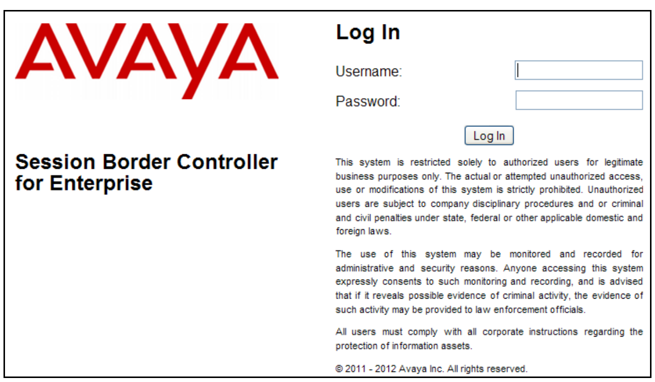
IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition 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 both the Main site (192.168.67.x) and the Branch site (192.168.69.x).) The connection to AT&T uses the Avaya SBCE public interface B1 (IP address 10.10.10.12[8]).

7.2. Log into the Avaya SBCE

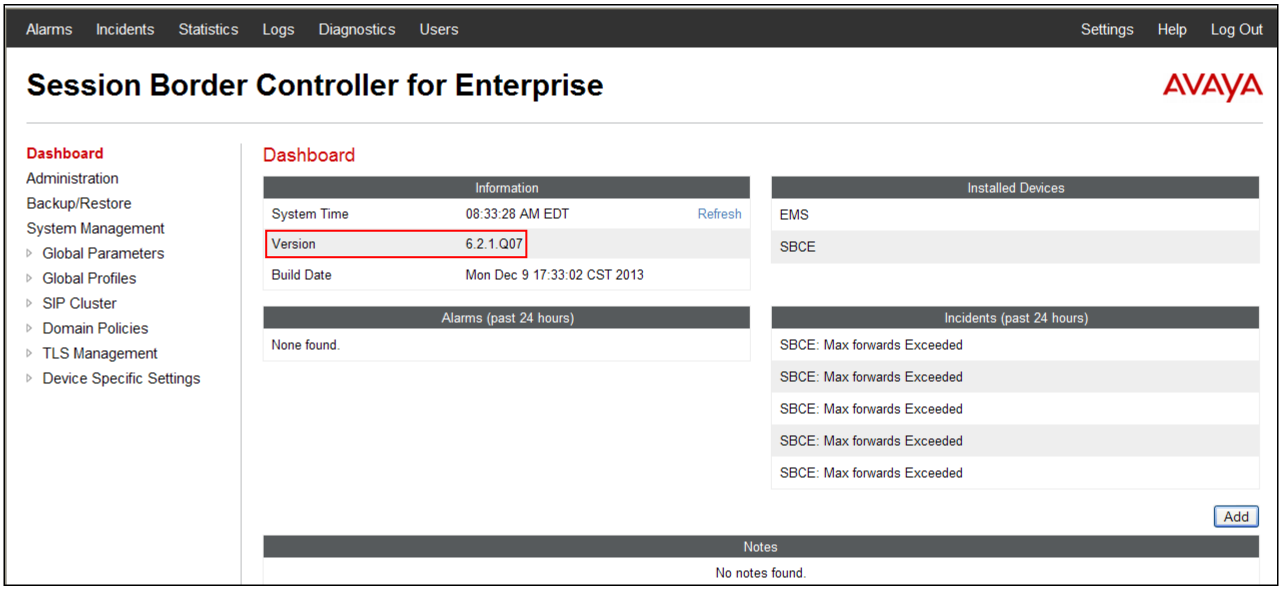
The follow provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

A. 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).
B. Enter the **Username** and **Password**.



C. The main menu window will open. Note that the installed software version is displayed.

[8] See the note in **Section 3.1**



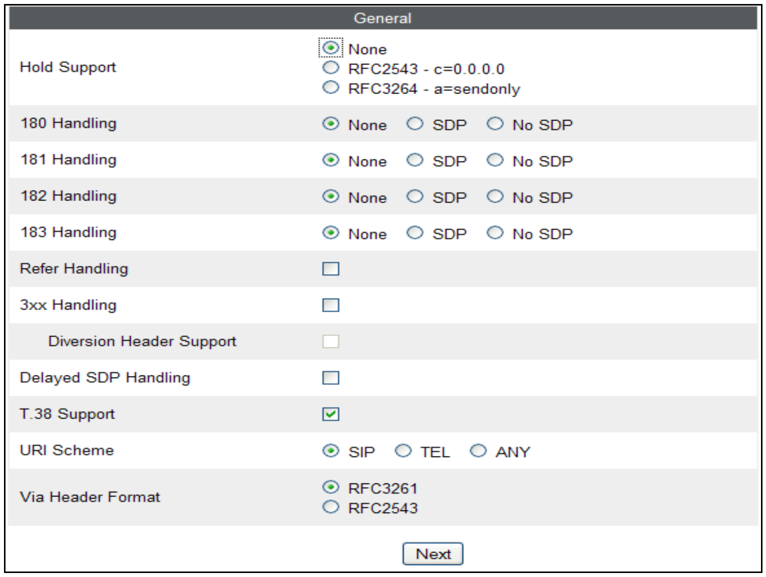
7.3. Global Profiles

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

7.3.1. Server Interworking – Avaya

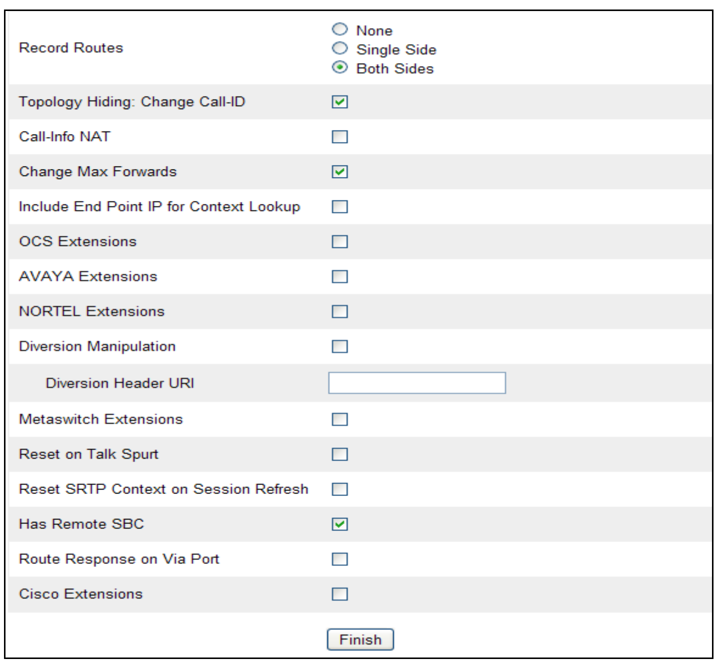
Server Interworking allows user to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the connection to Avaya IP Office via the “DMZ” network.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Interworking** (not shown).
3. Select the **Add** button (not shown) and the **Profile** name window will open (not shown).
4. Enter profile name: (e.g., **Avaya_Trunk_SI**), and click **Next**.
5. The **General** screen will open.
   a. Check **T38 Support**.
   b. All other options can be left with default values
   c. Click **Next**



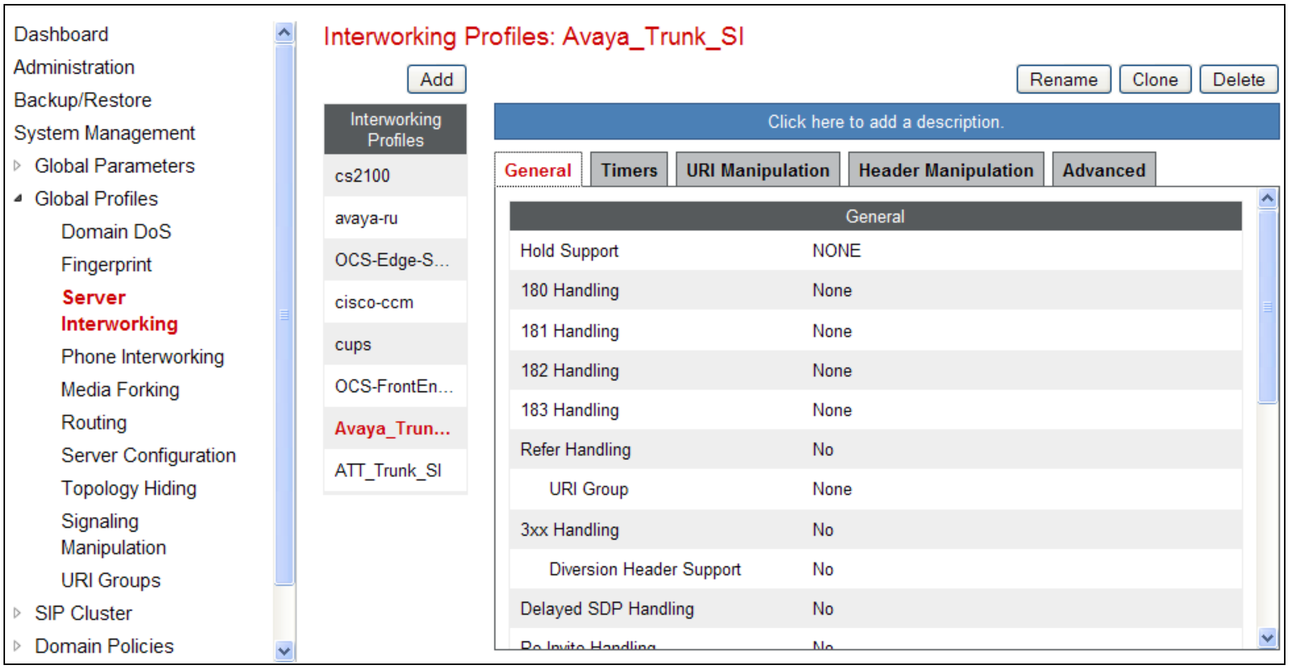
General	
Hold Support	(•) None ( ) RFC2543 - c=0.0.0.0 ( ) RFC3264 - a=sendonly
180 Handling	(•) None ( ) SDP ( ) No SDP
181 Handling	(•) None ( ) SDP ( ) No SDP
182 Handling	(•) None ( ) SDP ( ) No SDP
183 Handling	(•) None ( ) SDP ( ) No SDP
Refer Handling	☐
3xx Handling	☐
Diversion Header Support	☐
Delayed SDP Handling	☐
T.38 Support	☑
URI Scheme	(•) SIP ( ) TEL ( ) ANY
Via Header Format	(•) RFC3261 ( ) RFC2543
	Next

6. On the **Privacy/DTMF** window (not shown), select **Next** to accept default values.
7. On the **SIP Timers/Transport Timers** window (not shown), select **Next** to accept default values.
8. On the **Advanced** tab, accept the default values, and click **Finish**.



Record Routes	( ) None ( ) Single Side (•) Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	☐
Change Max Forwards	☑
Include End Point IP for Context Lookup	☐
OCS Extensions	☐
AVAYA Extensions	☐
NORTEL Extensions	☐
Diversion Manipulation	☐
Diversion Header URI	
Metaswitch Extensions	☐
Reset on Talk Spurt	☐
Reset SRTP Context on Session Refresh	☐
Has Remote SBC	☑
Route Response on Via Port	☐
Cisco Extensions	☐
	Finish

The following screenshot shows the completed **General** tab form.



7.3.2. Server Interworking – AT&T

Repeat the steps shown in **Section 7.3.1** to add an Interworking Profile for the connection to AT&T via the public network.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Interworking**.
3. Select **Add Profile**.
4. On the **General** Tab (not shown):
    a. Enter a profile name**:** (e.g., **ATT_Trunk_SI**)
    b. Check **T38 Support**
    c. All other options can be left as default.
    d. Click **Next**
5. At the **Privacy** tab (not shown), select **Next** to accept default values.
6. At the **Interworking Profile** tab (not shown), select **Next** to accept default values.
7. On the last screen (**Advanced** options, not shown), accept the default values, and click **Finish**.

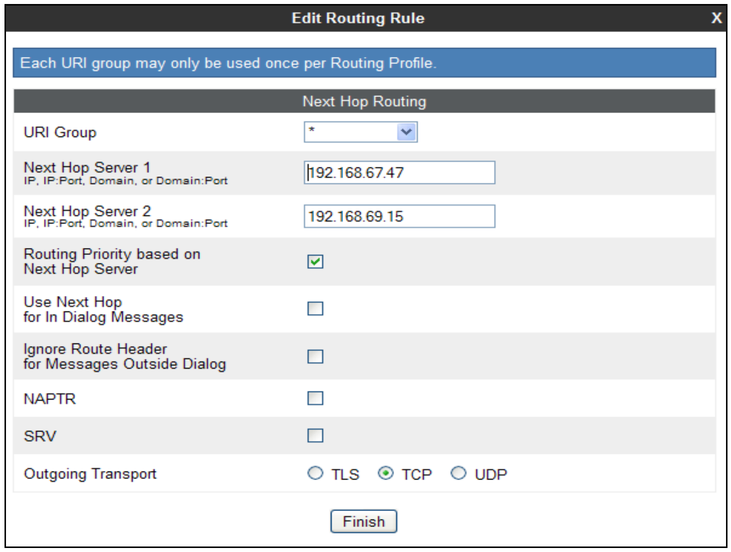
7.3.3. Routing – To Session Manager (Main and Branch)

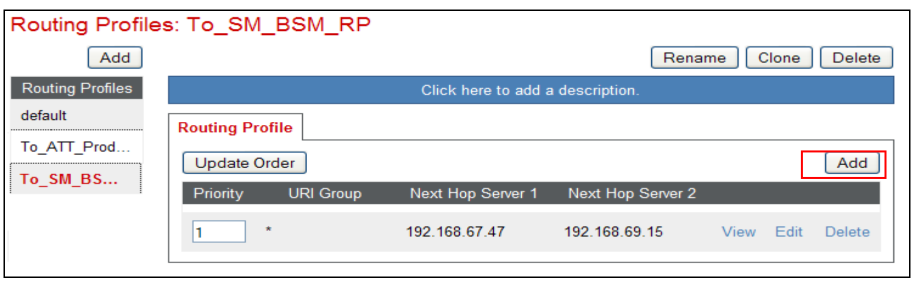
The following routing profile provides routing to both the Main Session Manager and to the Branch Session Manager.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select the **Routing** tab (not shown).
3. Select **Add Profile** (not shown).
4. Enter **Profile Name**: (e.g., **To_SM_BSM_RP)**.
5. Click **Next** and enter the following for regular inbound calls:
    a. In the **URI Group** field specify *

b. **Next Hop Server 1**: **192.168.67.47** (Main Session Manager)
c. **Next Hop Server 2**: **192.168.69.15** (Branch Session Manager)
d. Verify **Routing Priority Based on Next Hop Server** is selected (default).
e. **Outgoing Transport**: **TCP**
f. Accept remaining default values

6. Click **Finish**.



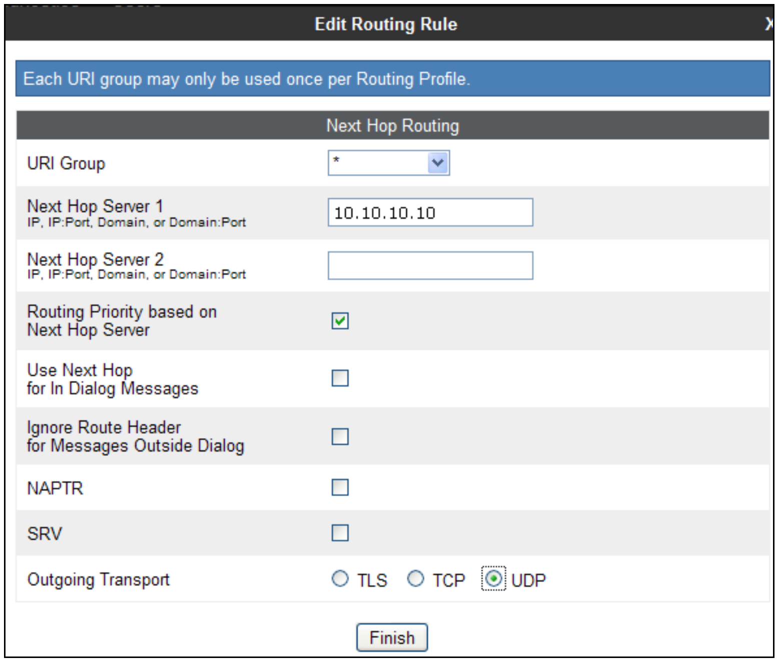


7.3.4. Routing – To AT&T

Repeat the steps in **Section 7.3.3**, with the following changes, to add a Routing Profile for the connection to AT&T.

1. Enter Profile Name: (e.g., **To_ATT_Production_RP)**.
2. Click **Next**, then enter the following:
   a. **Next Hop Server 1: 10.10.10.10** (Primary AT&T Border Element IP address[9])
   b. Verify **Routing Priority Based on Next Hop Server** is selected (default).
   c. **Outgoing Transport**: **UDP**
3. Click **Finish**.

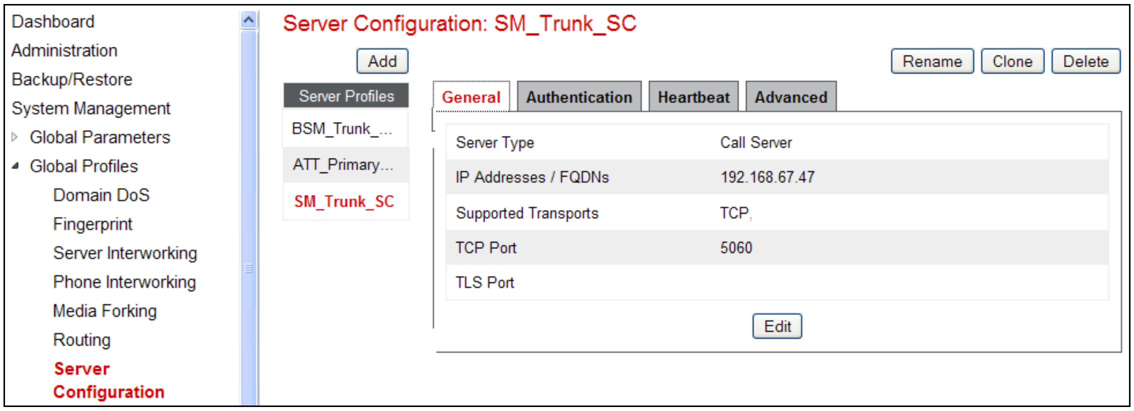
[9] See the note **Section 3.1**

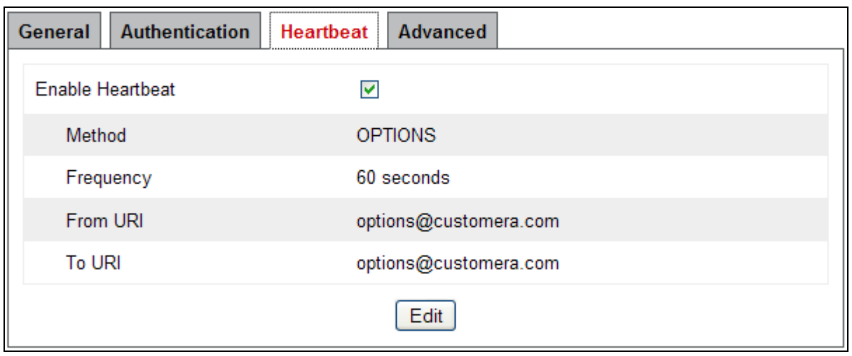


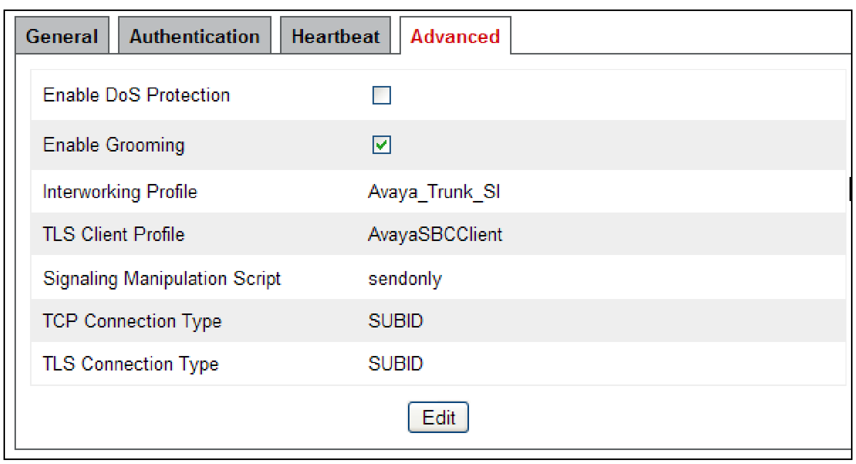
7.3.5. Server Configuration – Main Session Manager

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**.
3. Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **SM_Trunk_SC**) and click **Next**.
4. The **Add Server Configuration Profile - General** window will open (not shown).
    a. Select **Server Type**: **Call Server**
    b. **IP Address**: **192.168.67.47**
    c. **Supported Transports**: Check **TCP** (see the note in **Section 5.4**).
    d. **TCP Port**: **5060**
    e. Select **Next**
5. The **Add Server Configuration Profile - Authentication** window will open (not shown).
    a. Select **Next** to accept default values.
6. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
    a. Check **Enable Heartbeat**
    b. **Method: OPTIONS**
    c. **Frequency:** As desired (e.g., **60 seconds**).
    d. **From URI: options@customera.com**
    e. **To URI: options@customera.com**
    f. Select **Next** (not shown)
7. The **Add Server Configuration Profile - Advanced** window will open.
    a. Select **Avaya_Trunk_SI** (created in **Section 7.3.1**), for **Interworking Profile**.
    b. In the **Signaling Manipulation Script** field select **sendonly** (created in **Section 7.3.10**).
    c. Select **Finish**.

The following screen shots show the completed **General**, **Heartbeat**, and **Advanced** tabs, that are displayed after **Finish** has been selected for each.



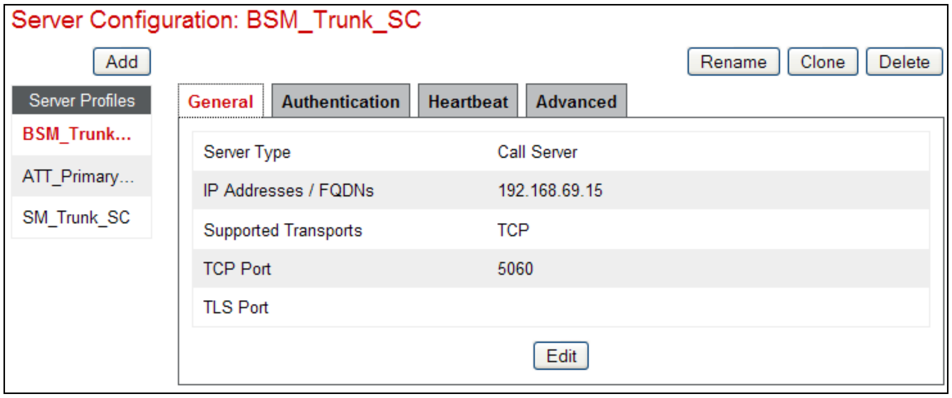


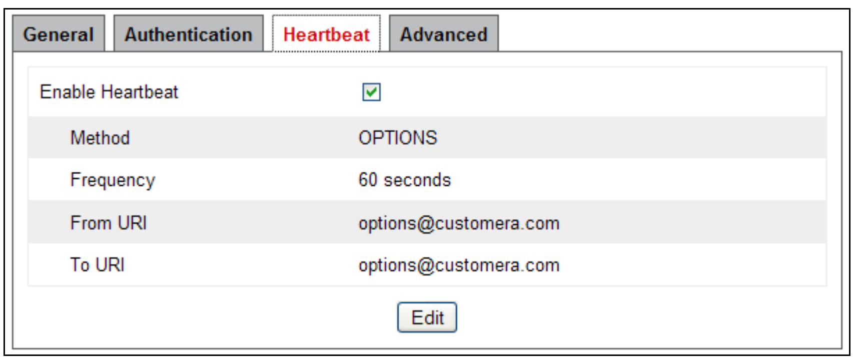


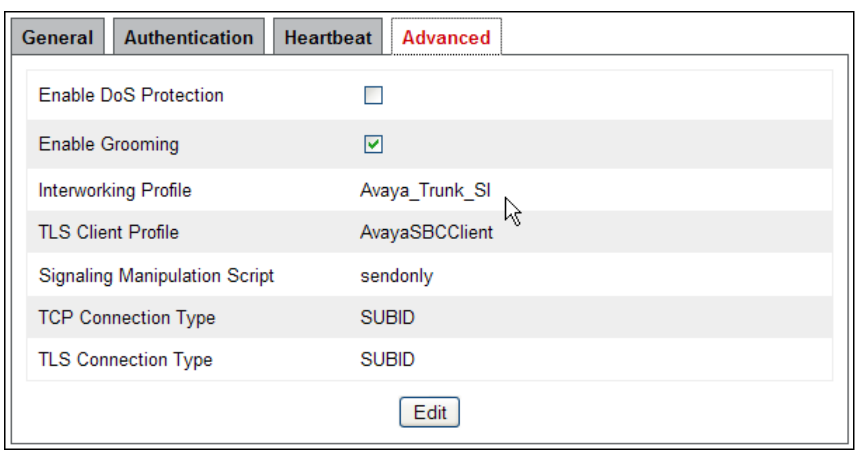
7.3.6. Server Configuration – Branch Session Manager

Repeat the steps in **Section 7.3.5**, with the following changes:

1. Enter a Profile Name (e.g., **BSM_Trunk_SC**) and click **Next**.
2. The **Add Server Configuration Profile - General** window:
   a. **IP Address**: **192.168.69.15**
   b. Select **Finish**.







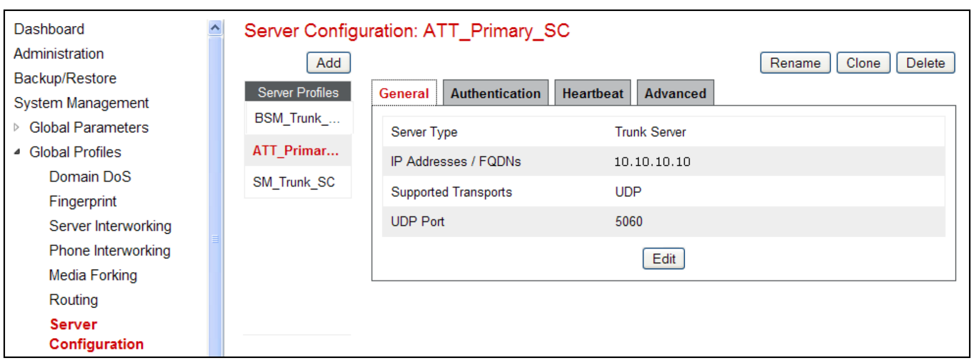
7.3.7. Server Configuration – AT&T

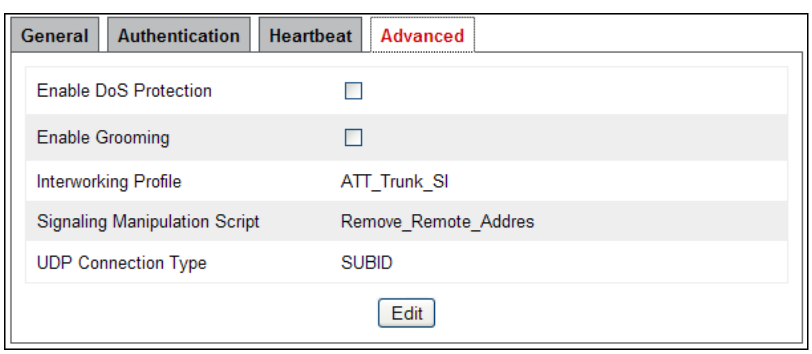
Note – The AT&T IPFR-EF service may provide a Primary and Secondary Border Element. This section describes the connection to a single (Primary) Border Element. See **Addendum 1** for information on configuring two IPFR-EF Border Elements (Primary & Secondary).

Repeat the steps in **Section 7.3.6**, with the following changes. Note that the **Heartbeat** tab is not used here.

1. Enter a Profile Name (e.g., **ATT_Primary_SC**) and select **Next**.
2. The **Add Server Configuration Profile - General** window will open (not shown).
    a. Select Server Type**: Trunk Server**
    b. **IP Address: 10.10.10.10** (AT&T Border Element IP address[10])
    c. **Supported Transports**: Check **UDP**
    d. **UDP Port: 5060**
    e. Select **Next**.
3. The **Add Server Configuration Profile - Advanced** window will open.
    d. Select **ATT_Trunk_SI** (created in **Section 7.3.2**), for **Interworking Profile**.
    e. In the **Signaling Manipulation Script** field select **Remove_Remote_Address** (see **Sestion 2.2.1**, **Item 7**, and **Section 7.3.10**).
    a. Select **Finish**.

The following screen shots show the completed **General** and **Advanced** tabs, that are displayed after **Finish** has been selected for each.



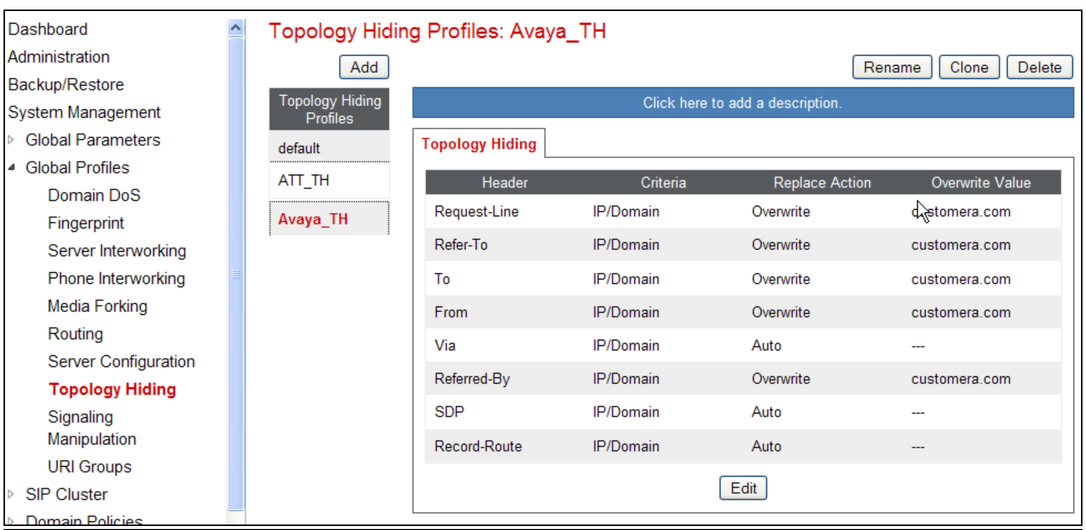


[10] See the note in **Section 3.1**

7.3.8. Topology Hiding – Avaya Side

The **Topology Hiding** hides the topology of the enterprise network from external networks.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Topology Hiding**.
3. Click **default** profile and select **Clone Profile** (not shown).
4. Enter Profile Name: (e.g., **Avaya_TH**)
5. For the Header **To**,
    a. In the **Criteria** column select **IP/Domain**
    b. In the **Replace Action** column select **Overwrite**
    c. In the **Overwrite Value** column enter **customera.com**
6. For the Header **Request Line**,
    a. In the **Criteria** column select **IP/Domain**
    b. In the **Replace Action** column select **Overwrite**
    c. In the **Overwrite Value** column enter **customera.com**
7. For the Header **From**,
    a. In the **Criteria** column select **IP/Domain**
    b. In the **Replace Action** column select **Overwrite**
    c. In the **Overwrite Value** column enter **customera.com**
8. Use default values for rest of the fields.
9. Click **Finish**.



7.3.9. Topology Hiding – AT&T Side

Repeat the steps in **Section 7.3.8,** with the following changes:

- Enter Profile Name: (e.g., **ATT_TH**).

Topology Hiding

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	---

Edit

7.3.10. Signaling Manipulation

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

- To remove a *Remote-Address* header, (see **Section 2.2.1, Item 7**).
- To modify the *Sendonly* parameter sent by Communication Manager, to *SendRecv*, (see **Section 2.2.1, Item 2**).

Note – Use of the Signaling Manipulation scripts demands higher processing requirements on the Avaya SBCE. Therefore, this method of header manipulation should only be used in cases where the use of Signaling Rules (**Section 7.4.3**) does not meet the desired result. Refer to **[9]** for information on the Avaya SBCE scripting language.

7.3.10.1 Remove Remote-Address header

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Signaling Manipulation**.
3. Click **Add Script** (not shown) and the script editor window will open.
4. Enter a name for the script in the **Title** box (e.g., **Remove_Remote_Address**). The following script is defined:

Signaling Manipulation Editor AVAYA

Title Remove_Remote_Addres Save

```
// Remove Remote-Address header added by SBCE

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

5. Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the AT&T Server Configuration in **Section 7.3.7**.

7.3.10.2 Modify SendOnly to SendRecv

1. Select **Global Profiles** →Select **Signaling Manipulation**.
2. Click **Add Script** (not shown) and the script editor window will open.
3. Enter a name for the script in the **Title** box (e.g., **sendonly**) and enter the following:

Title sendonly Save

```
//Replace SendOnly with SendRecv for IPFR
within session "INVITE"
{
  act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
   %BODY[1].regex_replace("a=sendonly","a=sendrecv");
  }
}
```

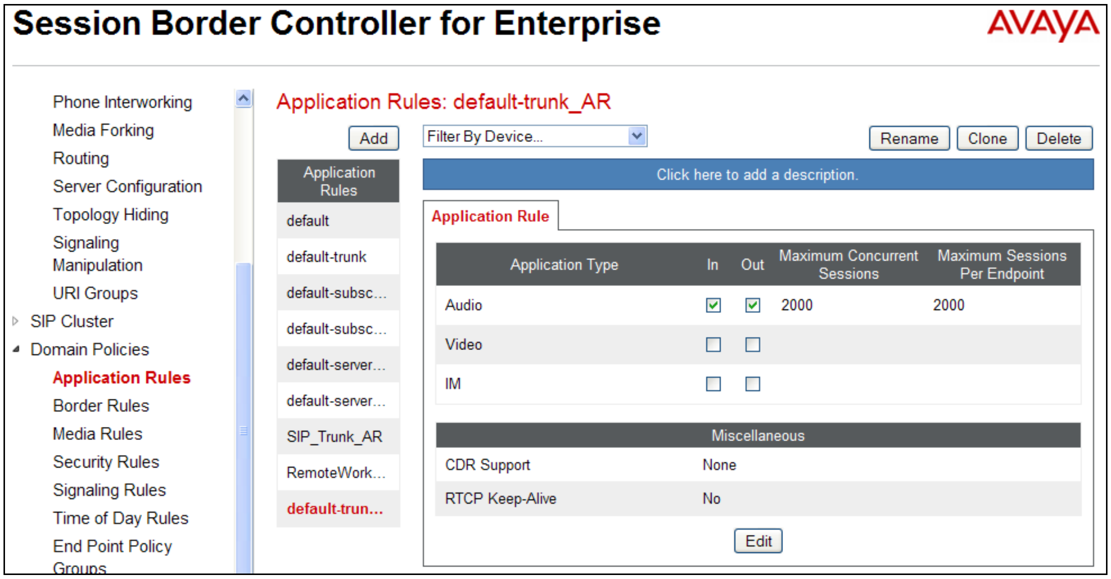
4. Click on **Save**. The script editor will test for any errors, and the window will close. This script is applied to the Avaya Server Configuration in **Sections 7.3.5** and **7.3.6**.

7.4. 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.

7.4.1. Application Rules

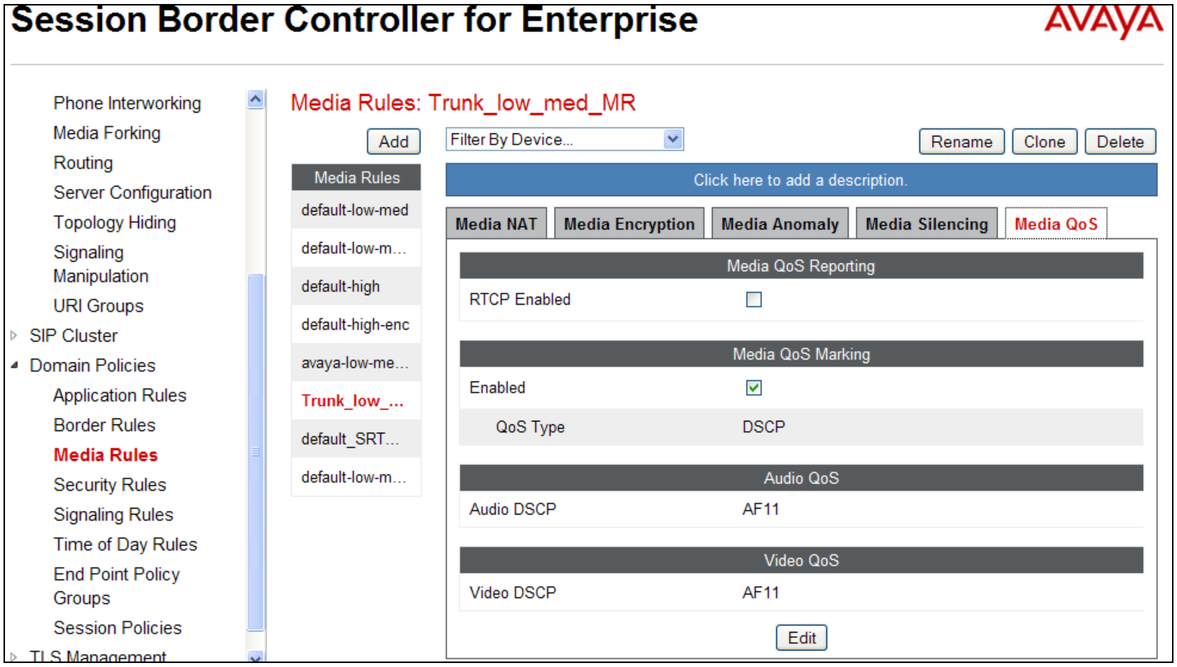
1. Select **Domain Policies** from the menu on the left-hand side (not shown).
2. Select the **Application Rules** (not shown).
3. Select the **default** Rule (not shown).
4. Select the **Clone** button (not shown), and the **Clone Rule** window will open.
   a. In the **Clone Name** field enter **default-trunk_AR**
   b. Click **Finish.**
5. Select the **default-trunk** rule just created (not shown).
   a. Click the **Edit** button. The **Editing Rule** screen will be displayed.
   b. In the **Voice** row:
      i. Change the **Maximum Concurrent Sessions** to **2000**
      ii. Change the **Maximum Sessions per Endpoint** to **2000**
   c. Click on **Finish.**



7.4.2. Media Rules

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

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Media Rules** (not shown).
3. The Media Rules window will open (not shown). From the Media Rules menu, select the **default-low-med** rule
4. Select **Clone** button (not shown), and the **Clone Rule** window will open.
    a. In the **Clone Name** field enter **Trunk-low-med_MR**
    b. Click **Finish.** The newly created rule will be displayed.
5. Highlight the **Trunk-low-med_MR** rule just created (not shown):
    a. Select the **Media QOS** tab.
    b. Click the **Edit** button and the **Media QOS** window will open.
    c. Check the **Media QOS Marking** field is **Enabled.**
    d. Select the **DSCP** box.
    e. **Audio**: Select **AF11** from the drop-down.
    f. **Video**: Select **AF11** from the drop-down.
6. Click **Finish.** The completed **Media Rules** screen is shown below.



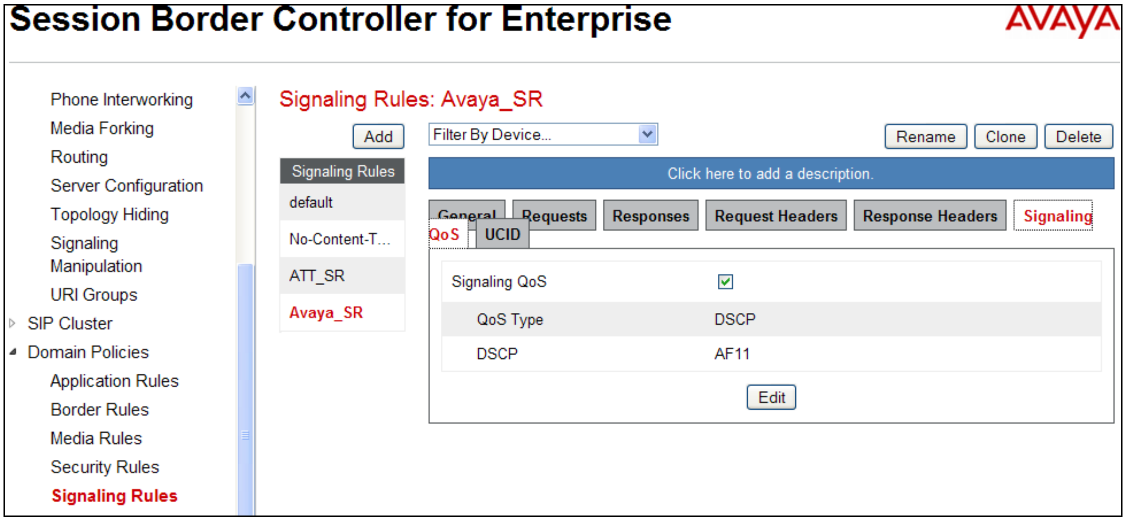
7.4.3. Signaling Rules

In the reference configuration, Signaling Rules are used to define QOS parameters, as well as block various SIP headers.

Note – SIP headers may also be blocked by the Signaling Manipulation function (see **Section 7.3.10**). However, Signaling Rules are a more efficient use of Avaya SBCE resources.

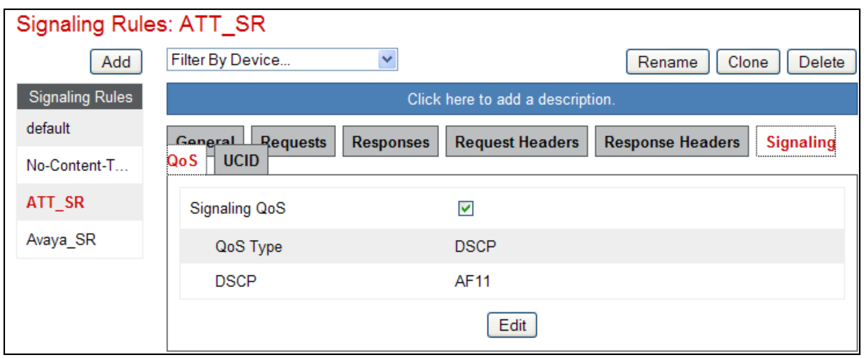
7.4.3.1 Avaya – Signaling QOS

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. 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.
5. 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**.
6. Click **Finish.** The completed **Signaling Rules** screen is shown below.



7.4.3.2 AT&T – Signaling QOS Tab

1. Repeat the steps in **Section 7.4.3.1**, with the following changes:
   - Clone the **default** rule button and name the rule**: ATT_SR**
   - Specify the same parameters used in **Section 7.4.3.1**.



7.4.3.3 Avaya – Request Headers Tab

The following Signaling Rules remove SIP headers sent by Communication Manager SIP requests that are either not supported or required by AT&T or headers that may contain internal CPE information.

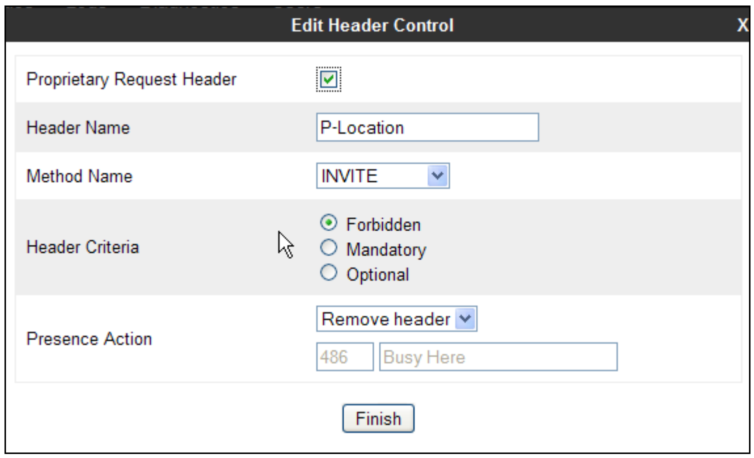
Note – In configurations that include Avaya Aura® Session Manager, the History-Info header is removed by Session Manager (see **Section 5.3.2**). Alternatively it may be removed by Communication Manager (see **Section 6.8.1**).

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

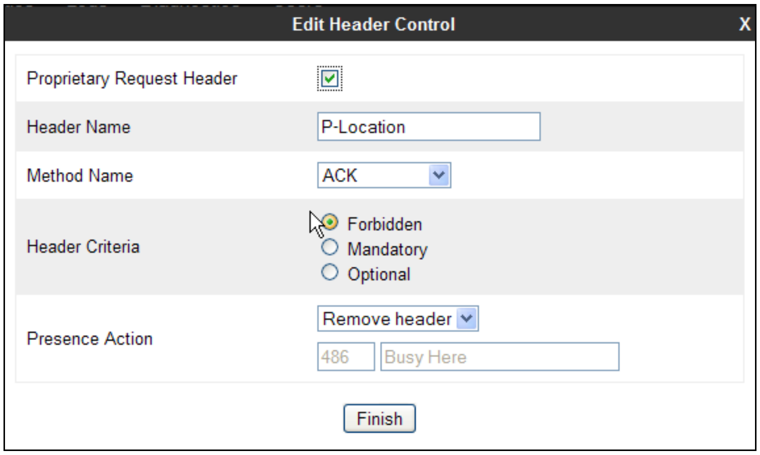
1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select **Signaling Rules** (not shown).
3. From the Signaling Rules menu, select the **default** rule.
4. Select **Clone Rule** button

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

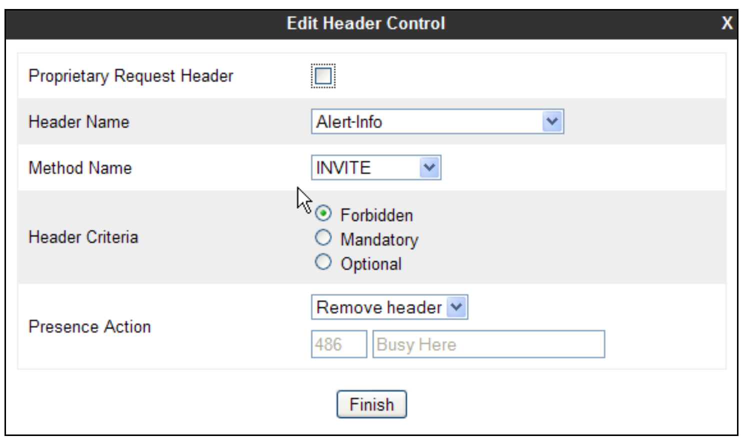
5. Highlight and edit the **Avaya_SR** rule created in **Step 4** and enter the following:
   - Select the **Add In Header Control** button (not shown). The Add Header Control window will open.
   - Select the **Request Headers** tab (not shown).
   - Click the **Edit** button and the **Edit Header Control** 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**.
6. Click **Finish**



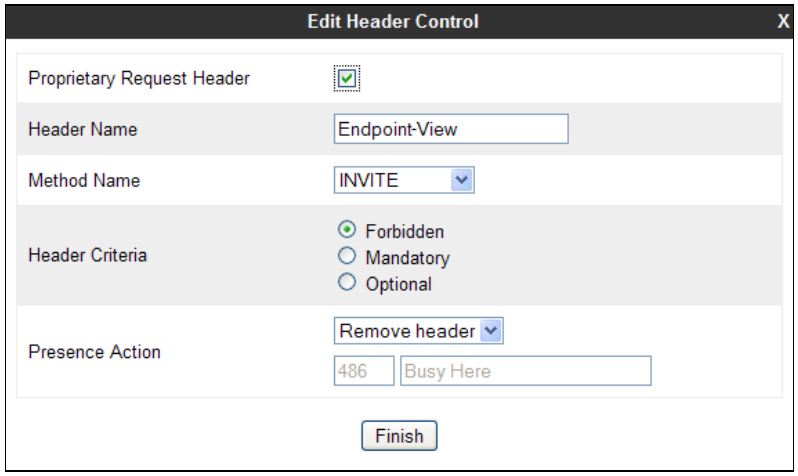
7. Repeat **Steps 5** through **6** to create a rule to remove the **P-Location** header from ACKs.
   - Click the **Edit** button and the **Edit Header Control** window will open.
   - Verify the **Proprietary Request Header** box is *unchecked*.
   - From the **Header Name** menu select **Alert-Info**
   - From the **Method Name** menu select **Invite**.
   - For **Header Criteria** select **Forbidden**
   - From the **Presence Action** menu select **Remove Header**.
8. Click **Finish**



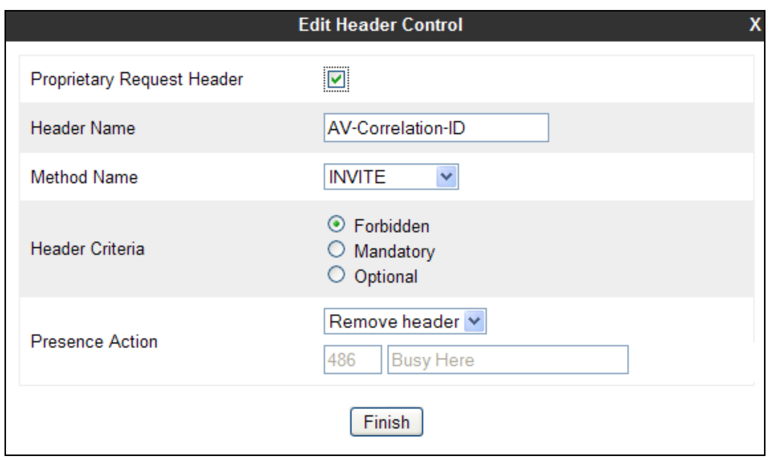
9. Repeat **Steps 5** through **6** to create a rule to remove the **Alert-Info** header.
   - Click the **Edit** button and the **Edit Header Control** window will open.
   - Verify the **Proprietary Request Header** box is *unchecked*.
   - From the **Header Name** menu select **Alert-Info**
   - From the **Method Name** menu select **Invite**.
   - For **Header Criteria** select **Forbidden**
   - From the **Presence Action** menu select **Remove Header**.
10. Click **Finish**



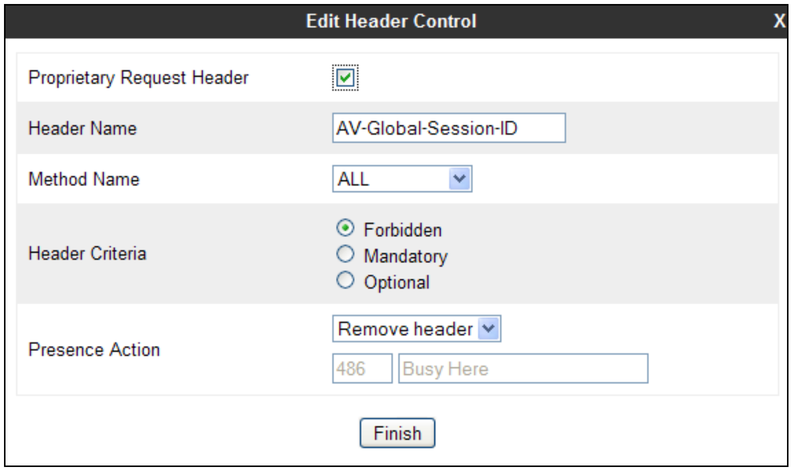
11. Repeat **Steps 5** through **6** to create a rule to remove the **Endpoint-View** header.
    - Click the **Edit** button and the **Edit Header Control** window will open.
    - Check the **Proprietary Request Header** box.
    - In the **Header Name** field, enter **Endpoint-View.**
    - From the **Method Name** menu select **Invite**.
    - For **Header Criteria** select **Forbidden**
    - From the **Presence Action** menu select **Remove Header**.
12. Click **Finish**



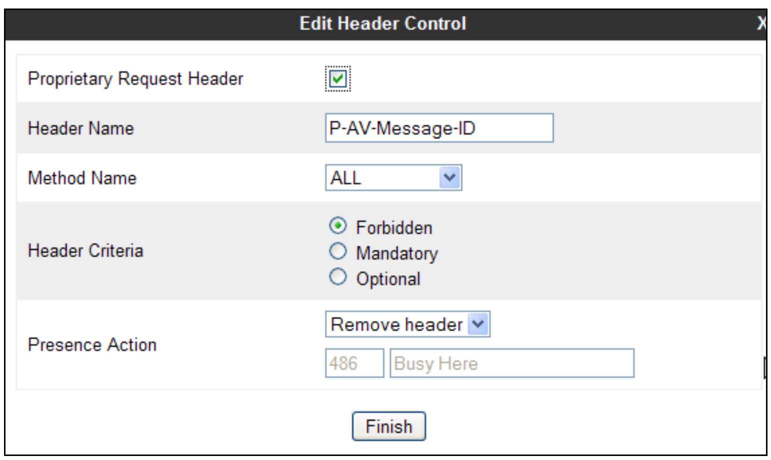
13. Repeat **Steps 5** through **6** to create a rule to remove the **AV-Correlation-ID** header.
    - Click the **Edit** button and the **Edit Header Control** window will open.
    - Check the **Proprietary Request Header** box.
    - In the **Header Name** field enter **AV-Correlation-ID**.
    - From the **Method Name** menu select **Invite**.
    - For **Header Criteria** select **Forbidden**
    - From the **Presence Action** menu select **Remove Header**.
14. Click **Finish**



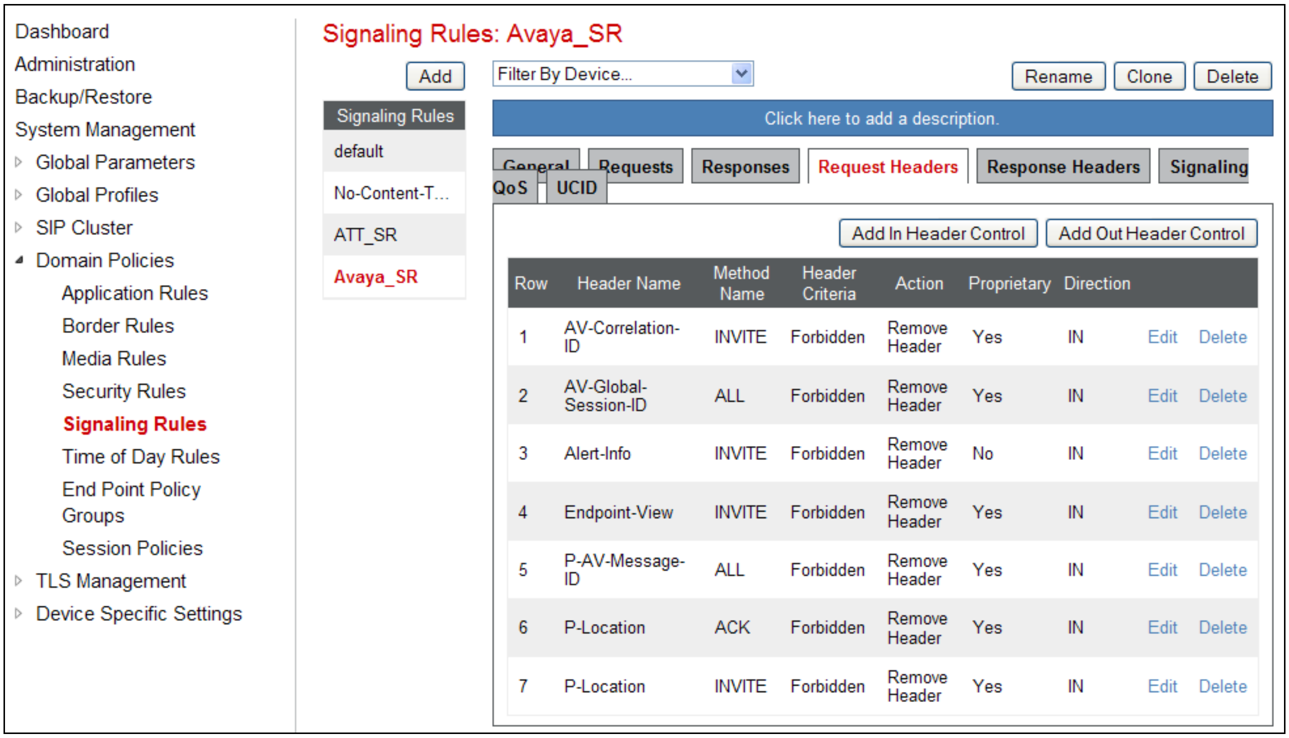
15. Repeat **Steps 5** through **6** to create a rule to remove the **AV-Global-Session-ID** header.
    - Click the **Edit** button and the **Edit Header Control** window will open.
    - Check the **Proprietary Request Header** box.
    - In the **Header Name** field enter **AV-Global-Session-ID**
    - From the **Method Name** menu select **ALL**.
    - For **Header Criteria** select **Forbidden**
    - From the **Presence Action** menu select **Remove Header**.
16. Click **Finish**



17. Repeat **Steps 5** through **6** to create a rule to remove the P-**AV-Message-ID** header.
    - 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-**AV-Message-ID**
    - From the **Method Name** menu select **ALL**.
    - For **Header Criteria** select **Forbidden**
    - From the **Presence Action** menu select **Remove Header**.
18. Click **Finish**



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



7.4.3.4 Avaya – Response Headers Tab

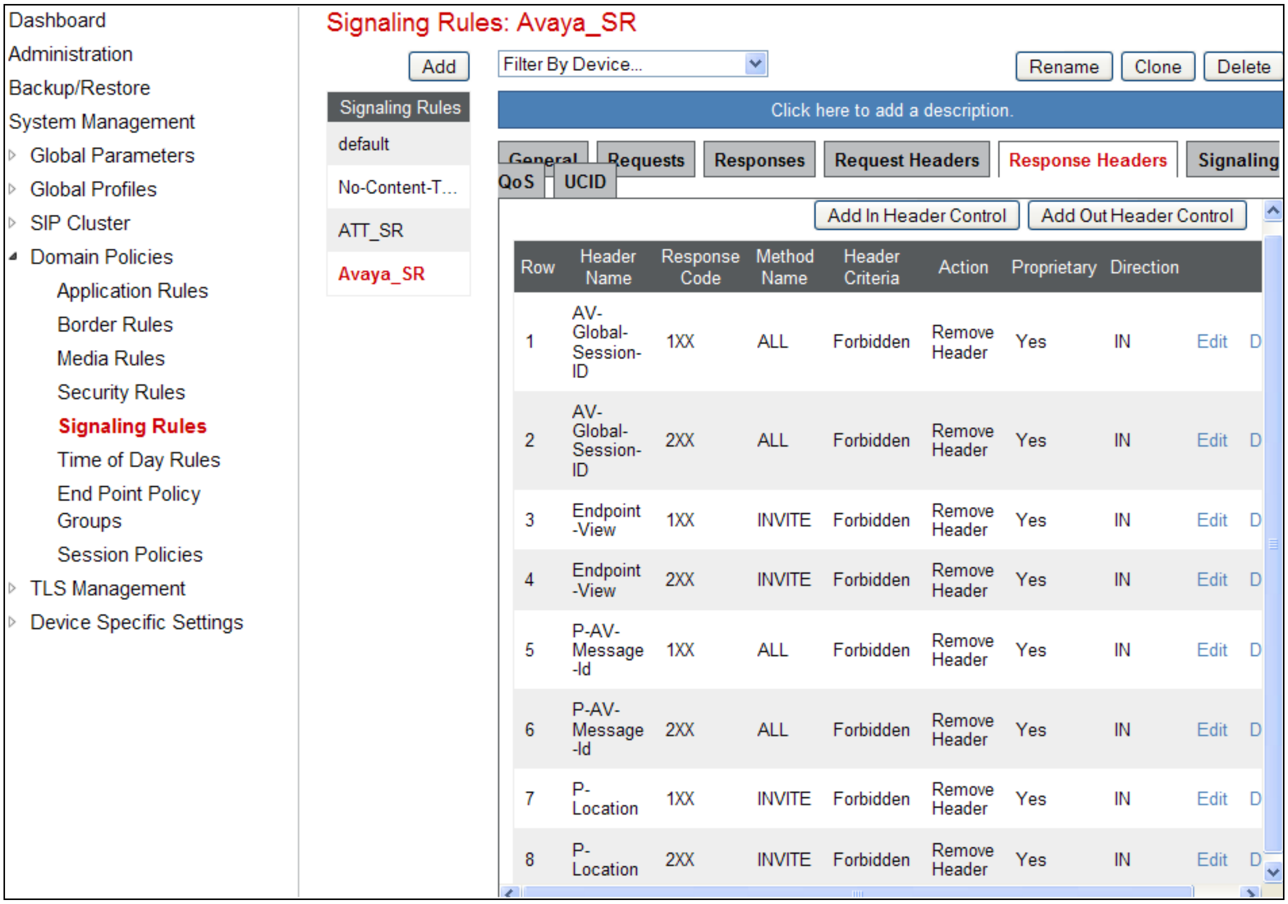
The following Signaling Rules remove headers sent by Communication Manager SIP responses (e.g., 1xx and/or 200OK) that are either not supported or required by AT&T or headers that may contain internal CPE information.

1. Highlight the **Avaya_SR** rule created in **Section 7.4.3.1**, and using the same procedures shown in **Section 7.4.3.3**, remove the **P-Location** header from **1xx** responses:
    - Select the **Response 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 **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**
2. Repeat **Step 1** to create a rule to remove the **P-Location** header from **2xx** responses.
    - From the **Response Code** menu select **2xx**.
    - Click **Finish**.
3. Repeat **Step 1** to create a rule to remove the **Endpoint-View** header from **1xx** responses.
    - Select the **Response 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 **Endpoint-View**.
- 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**

4. Repeat **Step 3** to remove **Endpoint-View** headers from **2xx** responses.
    - From the **Response Code** menu select **1xx**.
    - Click **Finish**
5. Repeat **Step 1** to create a rule to remove the P-**AV-Message-ID** header from **1xx** responses.
    - Select the **Response 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 **Endpoint-View**.
    - From the **Response Code** menu select **1xx**.
    - From the **Method Name** menu select **ALL**.
    - For **Header Criteria** select **Forbidden**.
    - From the **Presence Action** menu select **Remove Header**.
    - Click **Finish**
6. Repeat **Step 3** to remove P-**AV-Message-ID** headers from **2xx** responses.
    - From the **Response Code** menu select **1xx**.
    - Click **Finish**
7. Repeat **Step 1** to create a rule to remove the **AV-Global-Session-ID** header from **1xx** responses.
    - Select the **Response 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 **Endpoint-View**.
    - From the **Response Code** menu select **1xx**.
    - From the **Method Name** menu select **ALL**.
    - For **Header Criteria** select **Forbidden**.
    - From the **Presence Action** menu select **Remove Header**.
    - Click **Finish**
8. Repeat **Step 3** to remove **AV-Global-Session-ID** headers from **2xx** responses.
    - From the **Response Code** menu select **1xx**.
    - Click **Finish**
9. Click **Finish**

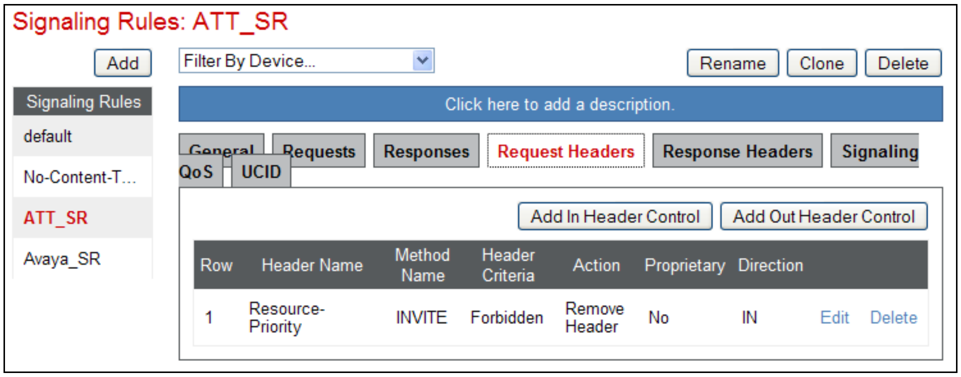
The completed Response Headers form is shown below. Note that the Direction column says “IN”.



7.4.3.5 AT&T – Request Headers Tab

Use the following steps to remove the **Resource-Priority** header:

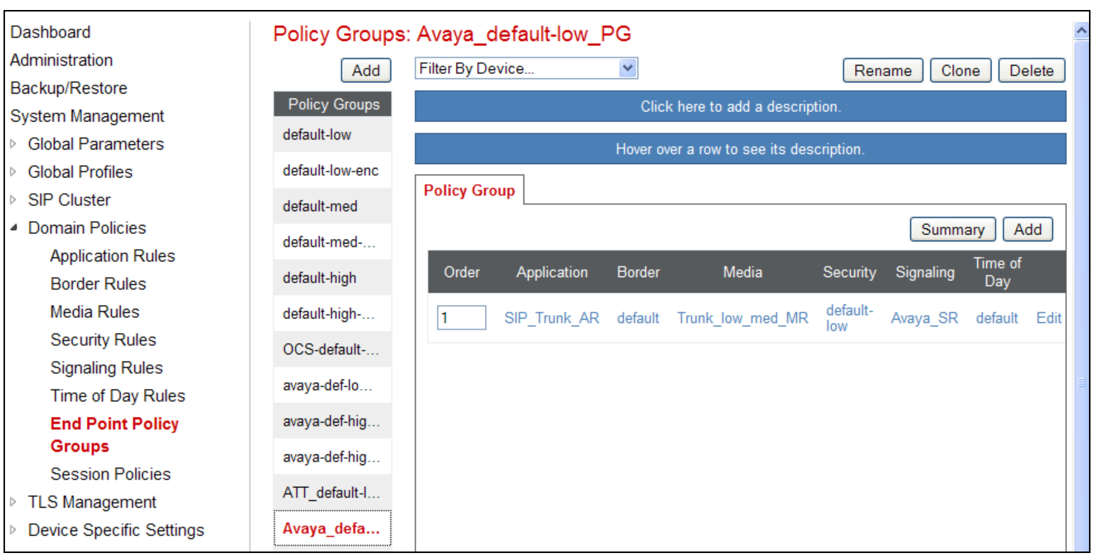
1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select **Signaling Rules** (not shown).
3. From the Signaling Rules menu, select the **default** rule.
4. Select **Clone Rule** button
   - Enter a name**: ATT_SR**
5. Click **Finish**
6. Highlight and edit the **ATT_SR** rule created in **Step 4**, enter the following:
   - Select the **Add In Header Control** button (not shown).
   - Select the **Request Headers** tab (not shown).
   - Click the **Edit** button and the **Edit Header Control** window will open.
   - From the **Header Name** menu select **Resource-Priority**.
   - From the **Method Name** menu select **Invite**.
   - For **Header Criteria** select **Forbidden**.
   - From the **Presence Action** menu select **Remove Header**.
7. Click **Finish.** The completed Request Headers form is shown below.
   Note that the Direction column says "IN", and that no Response
   Header manipulation is required.



7.4.4. Endpoint Policy Groups – Avaya Connection

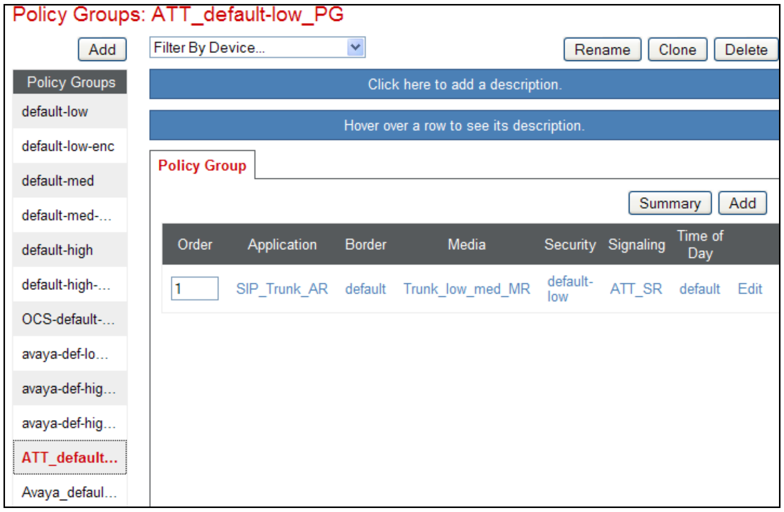
1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
   a) **Name**: **Avaya_default-low_PG**
   b) **Application Rule**: **SIP_Trunk_AR** (created in **Section 7.4.1**)
   c) **Border Rule**: **default**
   d) **Media Rule**: **Trunk_low_med_MR** (created in **Section 7.4.2**)
   e) **Security Rule**: **default-low**
   f) **Signaling Rule**: **Avaya_SR** (created in **Section 7.4.3**)
   g) **Time of Day**: **default**
4. Select **Finish** (not shown)

The completed **Policy Groups** screen is shown below.



7.4.5. Endpoint Policy Groups – AT&T Connection

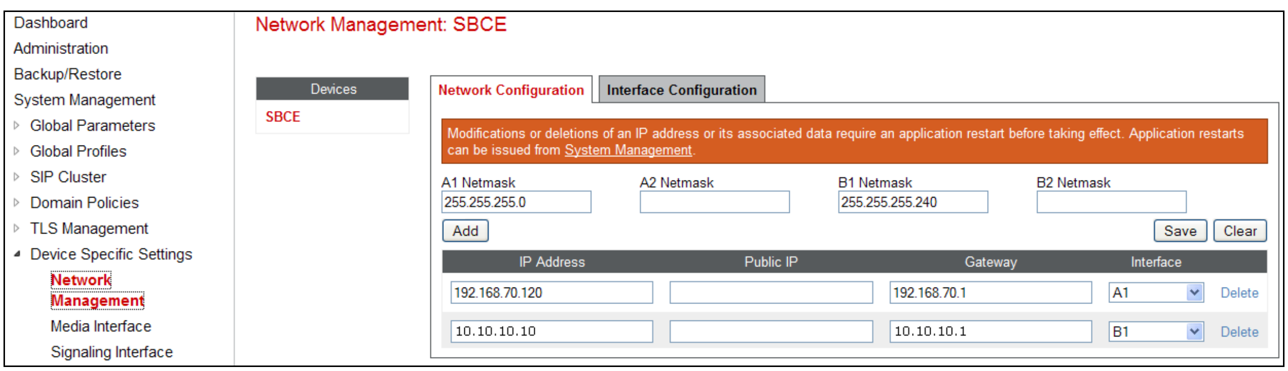
1. Repeat steps **1** through **4** from **Section 7.4.4** with the following changes:
    a. **Group Name**: **ATT_default-low_PG**
    b. **Signaling Rule**: **ATT_SR** (created in **Section 7.4.3)**
2. **Select Finish** (not shown)



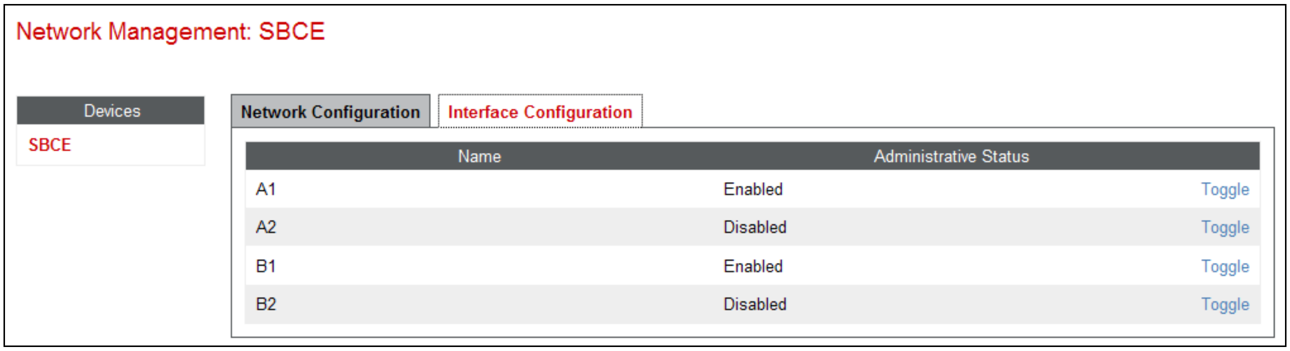
7.5. Device Specific Settings

7.5.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**
    a) The network interfaces are defined during installation. However if these values need to be modified, do so via this tab.



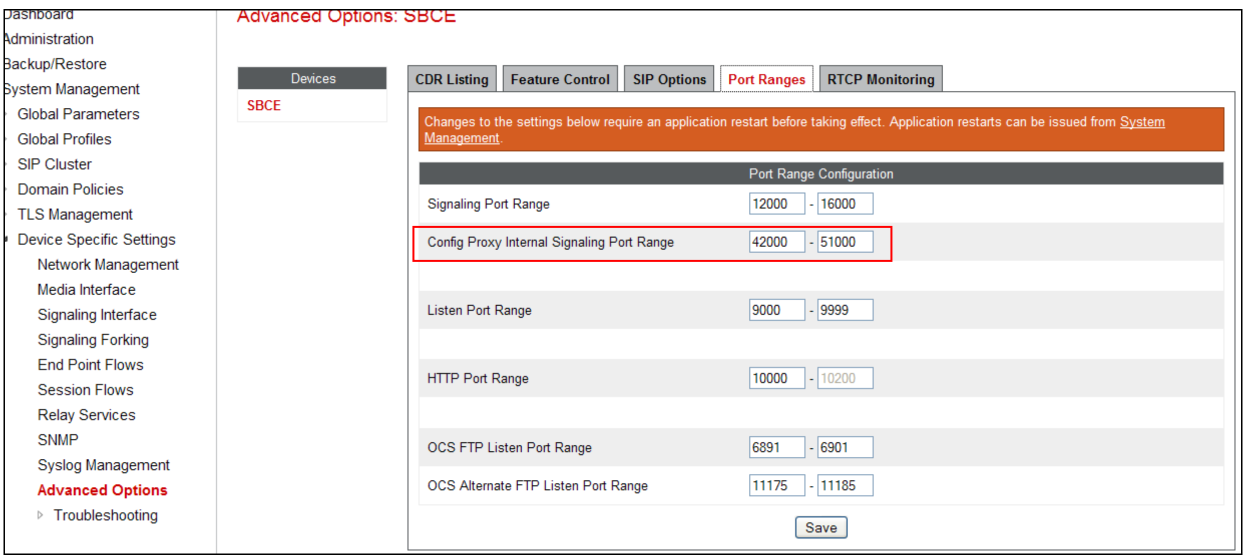
3. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab (note that the A2 and B2 interfaces are not supported at this time).



7.5.2. Advanced Options

In **Section 7.5.3**, 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.

1. Select **Device Specific Settings → Advanced Options** from the menu on the left-hand side.
2. Select the **Port Ranges** tab.
3. In the **Config Proxy Internal Signaling Port Range** row, change the range to **42000 – 51000**.
4. Scroll to the bottom of the window and select **Save** (not shown).



7.5.3. 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.

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface.**
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

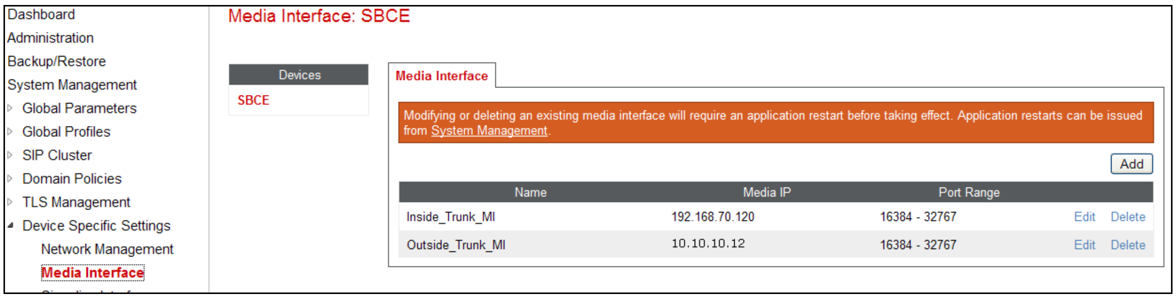
a) **Name**: **Inside_Trunk_MI**
b) **IP Adrress**: **192.168.42.20** (Avaya SBCE A1 address)
c) **Port Range**: **16384 - 32767**

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

a) **Name**: **Outside_Trunk_MI**
b) **IP Address**: **10.10.10.12**[11] (Avaya SBCE B1 address)
c) **Port Range**: **16384 - 32767**

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

The completed **Media Interface** screen is shown below.



7.5.4. Signaling Interface

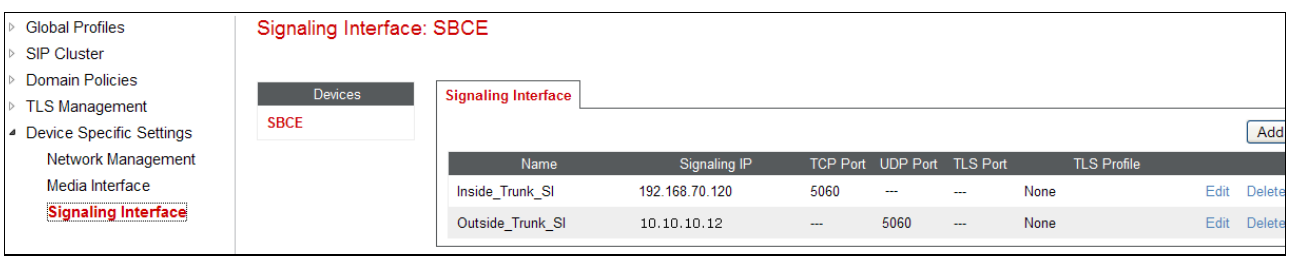
1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:

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

4. lick **Finish** (not shown).
5. Select **Add** again, and enter the following:

a) **Name**: **Outside_Trunk_SI**
d) **IP Address**: **10.10.10.12**[12] (Avaya SBCE B1 address)
b) **UDP Port**: **5060**

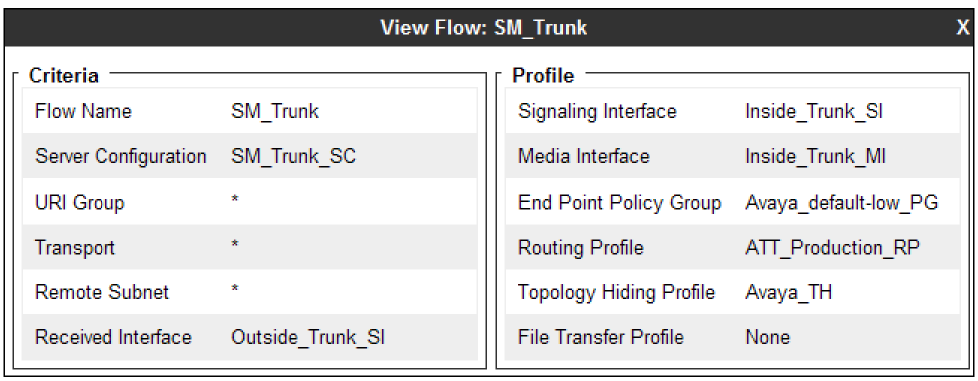
6. Click **Finish** (not shown).



[11] See the note in **Section 3.1**
[12] See the note in **Section 3.1**

7.5.5. Endpoint Flows – Main Site

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Endpoint Flows** (not shown).
3. Select the **Server Flows** tab (not shown).
4. Select **Add**, (not shown) and enter the following:
   a) **Name**: **SM_Trunk**
   b) **Server Configuration**: **SM_Trunk_SC** (**Section 7.3.5**)
   c) **URI Group**: *****
   d) **Transport**: *****
   e) **Remote Subnet**: *****
   f) **Received Interface**: **Outside_Trunk_SI (Section 7.5.4)**
   g) **Signaling Interface**: **Inside_Trunk_SI** (**Section 7.5.4**)
   h) **Media Interface**: **Inside_Trunk_MI** (**Section 7.5.3**)
   i) **End Point Policy Group**: **Avaya_default-low_PG** (**Section 7.4.4**)
   j) **Routing Profile**: **To_ATT_Production_RP** (**Section 7.3.4**)
   k) **Topology Hiding Profile**: **Avaya_TH** (**Section 7.3.8**)
   l) **File Transfer Profile**: **None**
5. Click **Finish**.



7.5.6. Endpoint Flows – Branch Site

1. Repeat steps **1** through **4** from **Section 7.5.5**, with the following changes:
   a) **Name**: **BSM_Trunk**
   b) **Server Configuration**: B**SM_Trunk_SC** (**Section 7.3.6**)
   c) **URI Group**: *****
   d) **Transport**: *****
   e) **Remote Subnet**: *****
   f) **Received Interface**: **Outside_Trunk_SI (Section 7.5.4)**
   g) **Signaling Interface**: **Inside_Trunk_SI** (**Section 7.5.4**)
   h) **Media Interface**: **Inside_Trunk_MI** (**Section 7.5.3**)
   i) **End Point Policy Group**: **Avaya_default-low_PG** (**Section 7.4.4**)
   j) **Routing Profile**: **To_ATT_Production_RP** (**Section 7.3.4**)
   k) **Topology Hiding Profile**: **Avaya_TH** (**Section 7.3.8**)
   l) **File Transfer Profile**: **None**
2. Click **Finish**.

View Flow: BSM_Trunk

Criteria		Profile	
Flow Name	BSM_Trunk	Signaling Interface	Inside_Trunk_SI
Server Configuration	BSM_Trunk_SC	Media Interface	Inside_Trunk_MI
URI Group	*	End Point Policy Group	Avaya_default-low_PG
Transport	*	Routing Profile	ATT_Production_RP
Remote Subnet	*	Topology Hiding Profile	Avaya_TH
Received Interface	Outside_Trunk_SI	File Transfer Profile	None

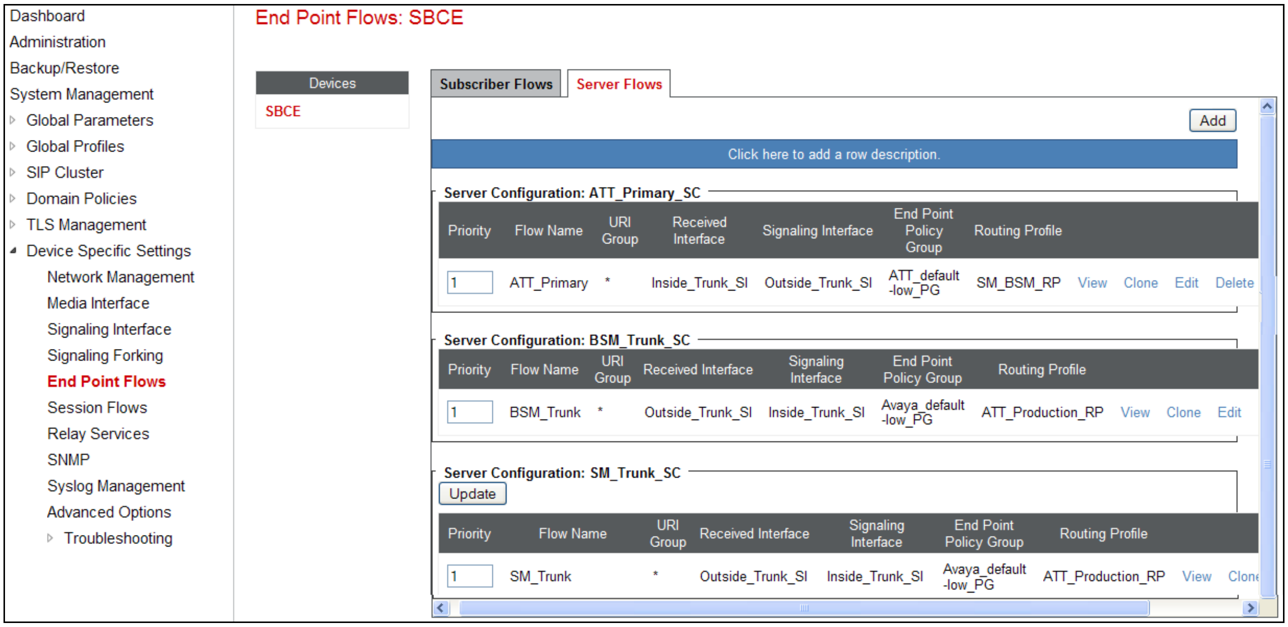
7.5.7. Endpoint Flows – AT&T

1. Repeat steps **1** through **4** from **Section 7.5.5**, with the following changes:
   a) **Name**: **ATT_Primary**
   b) **Server Configuration**: **ATT_Primary_SC** (**Section 7.3.7**).
   c) **URI Group**: *
   d) **Transport**: *
   e) **Remote Subnet**: *
   f) **Received Interface**: **Inside_Trunk_SI** (**Section 7.5.4**).
   g) **Signaling Interface**: **Outside_Trunk_SI (Section 7.5.4**).
   h) **Media Interface**: **Outside_Trunk_MI** (**Section 7.5.3**).
   i) **End Point Policy Group**: **ATT_default-low_PG** (**Section 7.4.5**).
   j) **Routing Profile**: **SM_BSM_RP (Section 7.3.3**).
   k) **Topology Hiding Profile**: **ATT_TH** (**Section 7.3.9**).
   l) **File Transfer Profile**: **None**
2. Click **Finish**.

View Flow: ATT_Primary

Criteria		Profile	
Flow Name	ATT_Primary	Signaling Interface	Outside_Trunk_SI
Server Configuration	ATT_Primary_SC	Media Interface	Outside_Trunk_MI
URI Group	*	End Point Policy Group	ATT_default-low_PG
Transport	*	Routing Profile	SM_BSM_RP
Remote Subnet	*	Topology Hiding Profile	ATT_TH
Received Interface	Inside_Trunk_SI	File Transfer Profile	None

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


Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
TLS Management
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
End Point Flows
Session Flows
Relay Services
SNMP
Syslog Management
Advanced Options
Troubleshooting
End Point Flows: SBCE
Devices
SBCE
Subscriber Flows
Server Flows
Add
Click here to add a row description.
Server Configuration: ATT_Primary_SC
Priority
Flow Name
URI Group
Received Interface
Signaling Interface
End Point Policy Group
Routing Profile
1
ATT_Primary
*
Inside_Trunk_SI
Outside_Trunk_SI
ATT_default -low_PG
SM_BSM_RP
View
Clone
Edit
Delete
Server Configuration: BSM_Trunk_SC
Priority
Flow Name
URI Group
Received Interface
Signaling Interface
End Point Policy Group
Routing Profile
1
BSM_Trunk
*
Outside_Trunk_SI
Inside_Trunk_SI
Avaya_default -low_PG
ATT_Production_RP
View
Clone
Edit
Server Configuration: SM_Trunk_SC
Update
Priority
Flow Name
URI Group
Received Interface
Signaling Interface
End Point Policy Group
Routing Profile
1
SM_Trunk
*
Outside_Trunk_SI
Inside_Trunk_SI
Avaya_default -low_PG
ATT_Production_RP
View

8. Verification Steps

The following steps may be used to verify the configuration:

8.1. Normal Operations

Under normal operations, the Session Manager and Communication Manager located in the Main site will be in control of inbound and outbound calls, as well as performing registrar functionality for the SIP and H.323 telephones. The Avaya SBCE (located in the Common site) will direct inbound calls to the Main Session Manager, as well as receiving outbound calls from the Main Session Manager. The Branch Session Manager and Branch Communication Manager will remain idle.

1. Place inbound and outbound calls (including IPFR-EF features), answer the calls, and verify that two-way talk path exists. Verify that the calls remain stable for several minutes and disconnect properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

8.2. Fail-Over Operations

During a failure (connections to the Main Session Manager and Communication Manager is lost), the Branch Session Manager and Branch Communication Manager located in the Branch site will activate. SIP and H.323 phones located in the Branch site will reregister to the Branch Session Manager and Branch Communication Manager. The Avaya SBCE will detect the loss of connectivity to the Main Session Manager, and will redirect inbound calls to the Branch Session Manager, as well as receiving outbound calls from the Branch Session Manager.

1. Place inbound and outbound calls (including IPFR-EF features), answer the calls, and verify that two-way talk path exists. Verify that the calls remain stable for several minutes and disconnect properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

8.3. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See **[4]** for more information.

- Tracing a SIP trunk.
    1. 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).

  Note that in the trace shown below, Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 19001, before sending the INVITE to Communication Manager.

```
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 [192.168.70.120]: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     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:18     7ok0
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<P/2.0
15:55:18     Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg
15:55:18     7ok0
```

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

Step 2 – To verify when the Branch Communication Manager has last received translations (see **Section 6.17**), enter the command **list survivable-processor**, and verify that the **Translations Updated** information approximately reflects the time/date when the **save translation all** command was issued. Note that this command also can be used to verify the node name (**Section 6.4)**, the assigned network region (**Section 6.6.3**), as well as whether the LSP is registered.

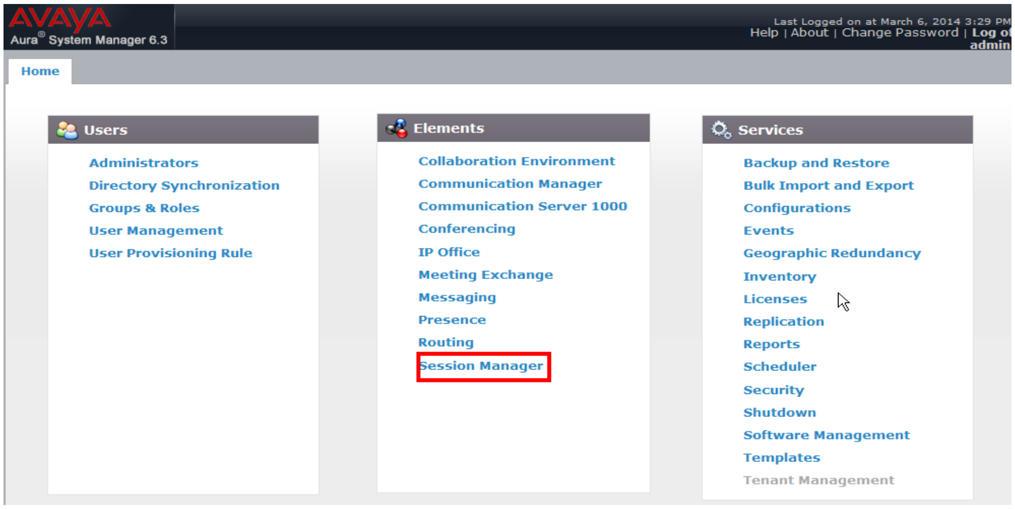
```
list survivable-processor
                             SURVIVABLE PROCESSORS
 Record Name/               Type         Reg Act          Translations      Net
 Number  IP Address                                       Updated           Rgn
  1     S8300D              LSP           y   n           14:55 3/13/2014   3
         192.168.69.12
        No V6 Entry
```

8.4. Avaya Aura® Session Manager Status

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

8.4.1. Normal Operations

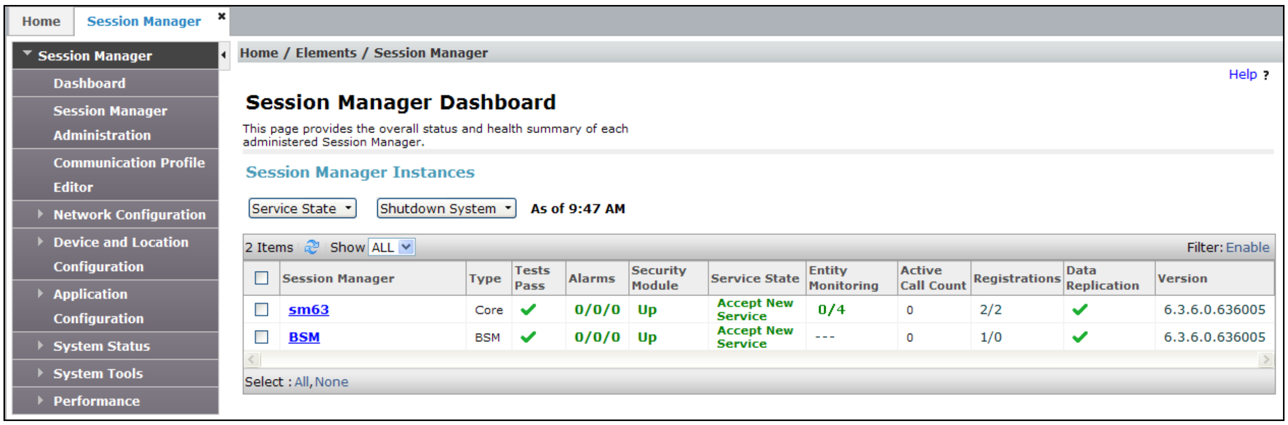
Step 1 – Using the procedures described in **Section 5**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



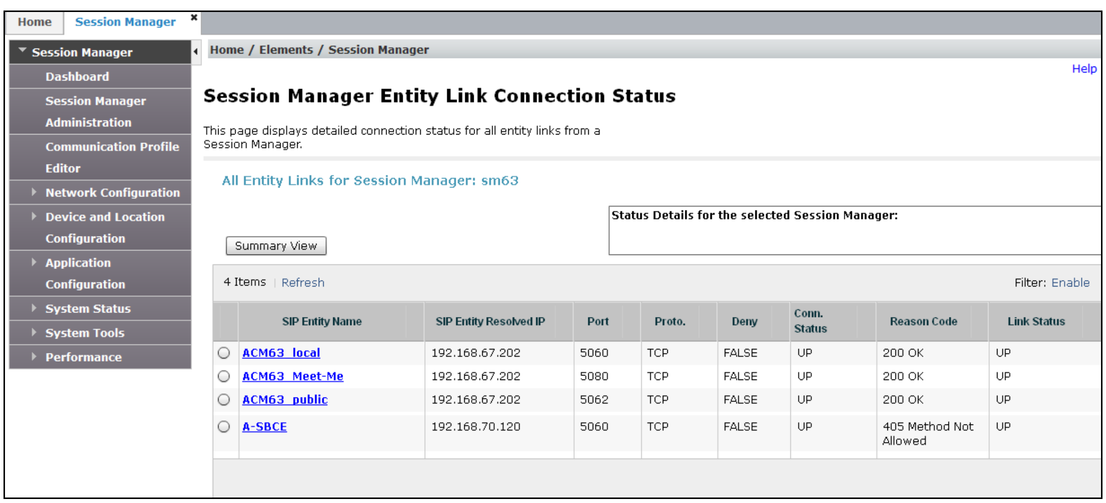
Step 2 – The Session Manager Dashboard is displayed. In the example below, both the Main Session Manager (**sm63**) and the Branch Session Manager (**BSM**) are displayed.

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

In the **Entity Monitoring Column**, the Main Session Manager shows that there are **0** (zero) alarms out of the **4** Entities defined. Also note that this column shows no entries for the **BSM** Session Manager. This is because the BSM is idle and not in control of the Entities.



Step 3 - Clicking on the **0/4** entry in the **Entity Monitoring** column for Session Manager **sm63**, results in the following display.



Note the **A-SBCE** Entity from the list of monitored entities above. The **Reason Code** column indicates that Session Manager has received a SIP **405 Method Not Allowed** response to the SIP OPTIONS it generated. This response is sufficient for SIP Link Monitoring to consider the link up. Also note that the Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T IPFR-EF Border Element, and it is the AT&T Border Element that is generating the 405, and the Avaya SBCE sends it back to Session Manager.

Step 4 – Returning to the screen shown in **Step 2** above, clicking on the **---** entry in the **Entity Monitoring** column for Session Manager **BSM**, results in the following display. Note that only the connection to the Avaya SBCE show up. This is because the connection between the Avaya SBCE and the Branch Session Manager is independent from the connection between the Avaya SBCE and the Main Session Manager, and is under the Branch Session Manager's control. The other Entities resolve to the IP address of the Branch Communication Manager (192.168.69.12) which is inactive.

Also note the Entity **avaya-lsp-fs**. This Entity is automatically created as a logical connection to the Branch Communication Manager when the Branch Session Manager is installed. It is through this logical connection that Communication Manager provisioning specifying the Main Session Manager (e.g., SIP trunks), can be "retasked" to communicate with the Branch Session Manager, when the Branch Communication Manager activates.

All Entity Links for Session Manager: BSM

Status Details for the selected Session Manager:

Summary View

4 Items | Refresh Filter: Enable

SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
A-SBCE	192.168.70.120	5060	TCP	FALSE	UP	405 Method Not Allowed	UP
LSP_Meet-Me	192.168.69.12	5080	TCP	FALSE	DOWN	408 Request Timeout	DOWN
avaya-lsp-fs	192.168.69.12	5060	TCP	FALSE	DOWN	408 Request Timeout	DOWN
ACM63_public	192.168.69.12	5062	TCP	FALSE	DOWN	408 Request Timeout	DOWN

8.4.2. Fail-over Operations

When connections to the Main site fail, the procedure shown in **Step 2** of **Section 8.4.1** will result in the following display:

Session Manager Instances

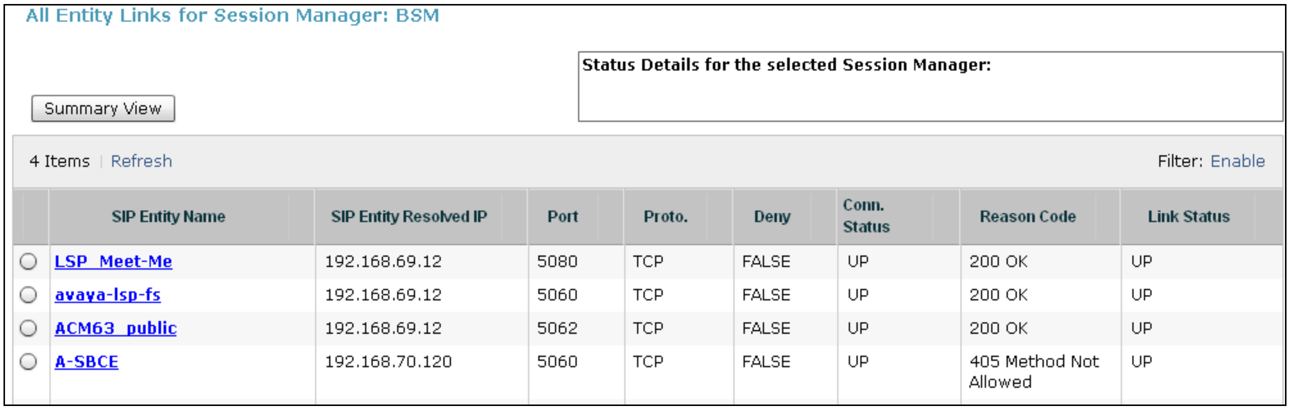
Service State | Shutdown System | As of 10:43 AM

2 Items | Show ALL Filter: Enable

Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
sm63	Core	No Connection	---	---	---	---	---	---	---	---
BSM	BSM	✔	0/0/0	Up	Accept New Service	---	0	1/0	✔	6.3.6.0.636005

Select : All, None

The procedure shown in **Step 4** of **Section 8.4.1** will result in the following display for the BSM Entities:



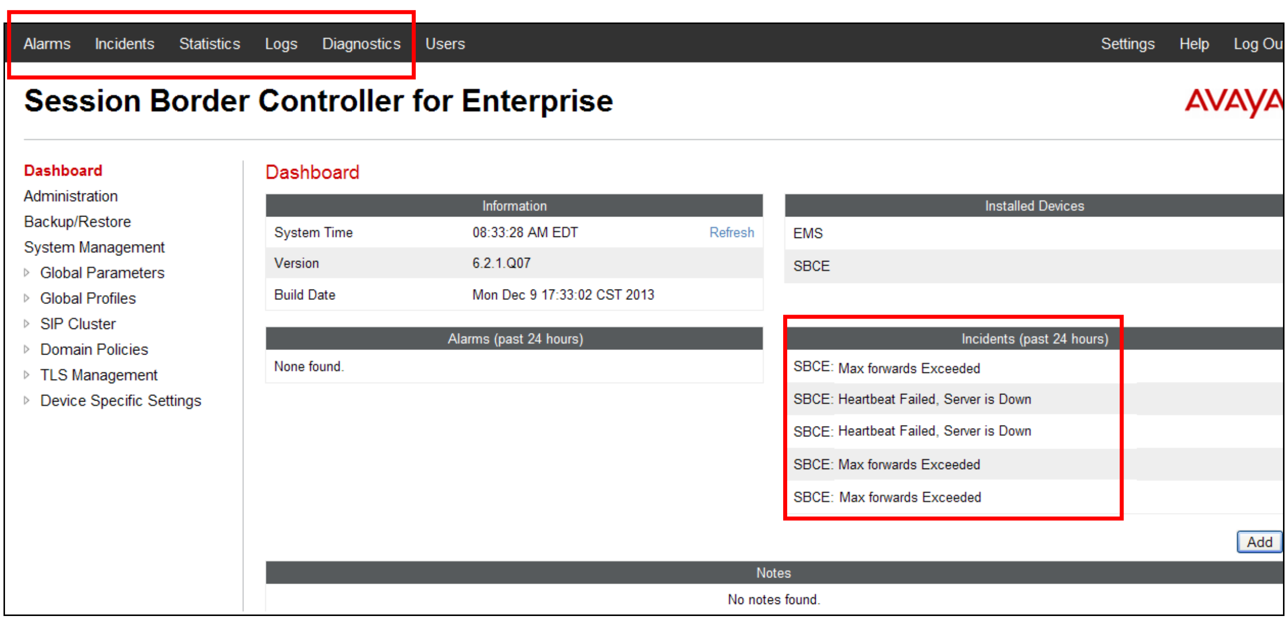
SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
LSP_Meet-Me	192.168.69.12	5080	TCP	FALSE	UP	200 OK	UP
avaya-lsp-fs	192.168.69.12	5060	TCP	FALSE	UP	200 OK	UP
ACM63_public	192.168.69.12	5062	TCP	FALSE	UP	200 OK	UP
A-SBCE	192.168.70.120	5060	TCP	FALSE	UP	405 Method Not Allowed	UP

8.5. Avaya Session Border Controller for Enterprise Verification

8.5.1. 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 7.2**. 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.



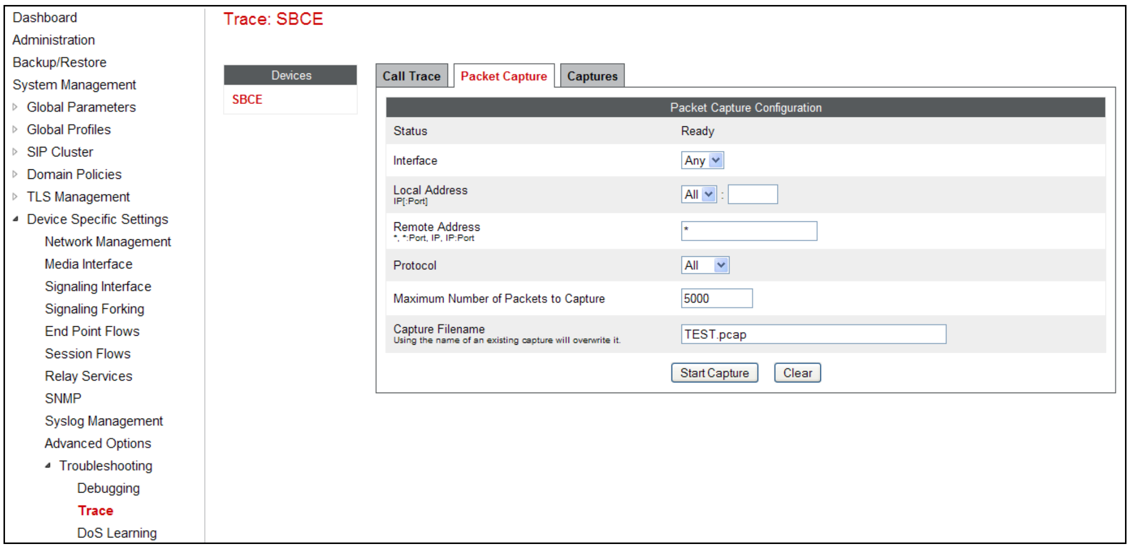
8.5.2. Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

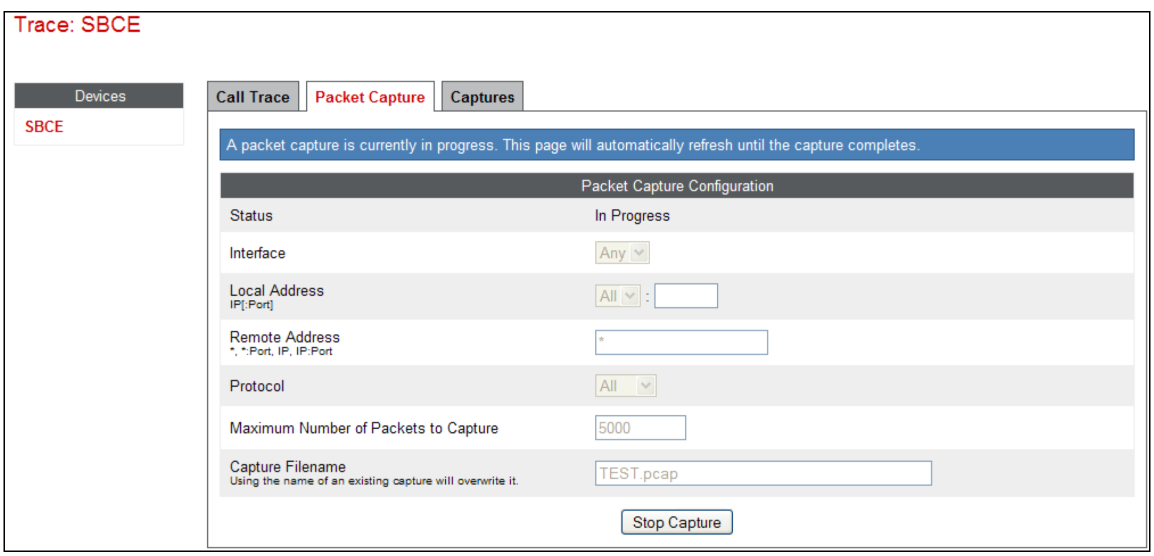
Step 1 - Navigate to UC-Sec Control Centre → Troubleshooting → Trace Settings

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

- Select the desired Interface from the drop down menu (e.g., **B1**, the interface to AT&T)
- Specify the Maximum Number of Packets to Capture (e.g., **1000**)
- Specify a Capture Filename.
- Click **Start Capture** to begin the trace.



The capture process will initialize and then display the following status window:

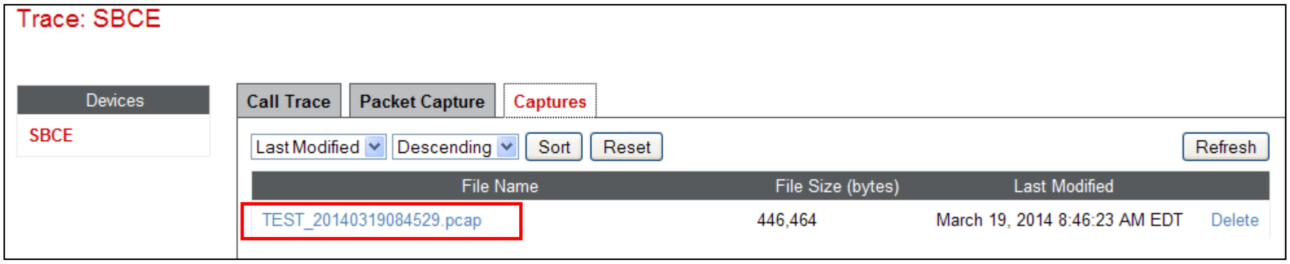


Step 3 – Run the test.

Step 4 - Select **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.



9. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager 6.3, Avaya Aura® Communication Manager 6.3, and the Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2.1, can be configured to interoperate successfully with the AT&T IP Flexible Reach – Enhanced Features service, within the constraints described in **Section 2.2.1.**

In addition, failover functionality (within the constraints of the reference configuration), of the Local Survivable Processor (containing Branch Session Manager 6.3 and the Communication Manager 6.3), in conjunction with the Avaya Session Border Controller for Enterprise 6.2.1, successfully restored SIP trunk capabilities with the AT&T IP Flexible Reach – Enhanced Features service.

Testing was performed on a production AT&T IP Flexible Reach – Enhanced Features service circuit. The reference configuration shown in these Application Notes is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

10. References

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

Avaya Aura® Session Manager/System Manager

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

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

[3] **Deploying Avaya Aura Branch Session Manager,** Release 6.3, Issue 2, March 2014

Avaya Aura® Communication Manager

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

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

[6] **Administering Avaya G430 Branch Gateway,** Release 6.3, 03-603228, Issue 5, October 2013

[7] **Administering Avaya G450 Branch Gateway,** Release 6.3, 03-602055, Issue 7, October 2013

Avaya Session Border Controller for Enterprise

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

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

AT&T IP Flexible Reach - Enhanced Features Service:

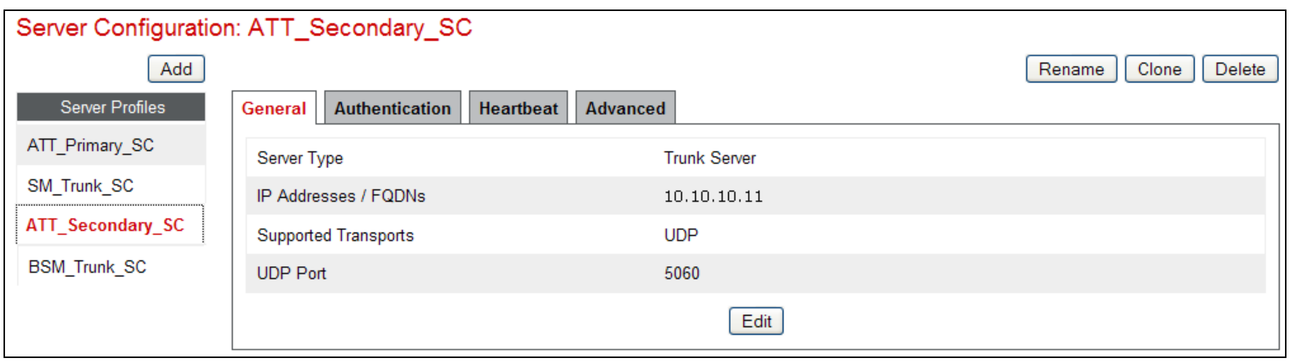
[10] AT&T IP Flexible Reach - Enhanced Features Service description - http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/

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

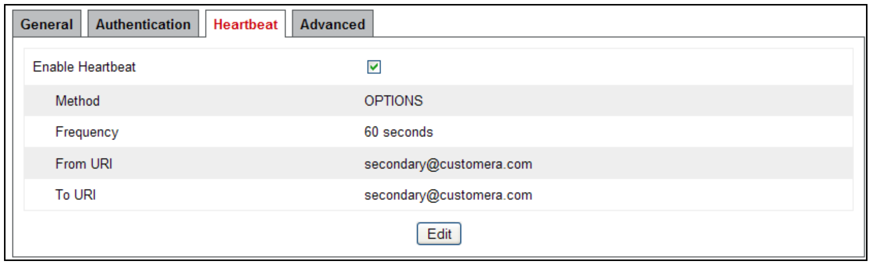
The AT&T IPFR-EF service may provide multiple network Border Elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration. Given two AT&T Border Elements **10.10.10.10** and **10.10.10.11** (see the note in **Section 3.1**) the Avaya SBCE is provisioned 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 7.3.7**).

11.1. Configure the Secondary Location in Server Configuration

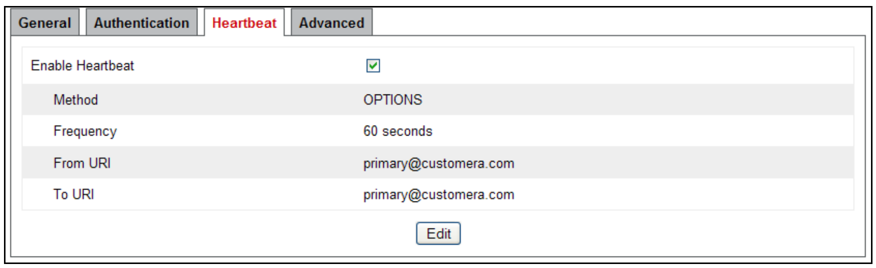
1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Server Configuration**
3. Select **Add Profile**
   a) **Name: ATT_Secondary_SC**
4. On the **Add Server Configuration Profile – General** tab:
   a) Select **Server Type: Trunk Server**
   b) **IP Address: 10.10.10.11** (sample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



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

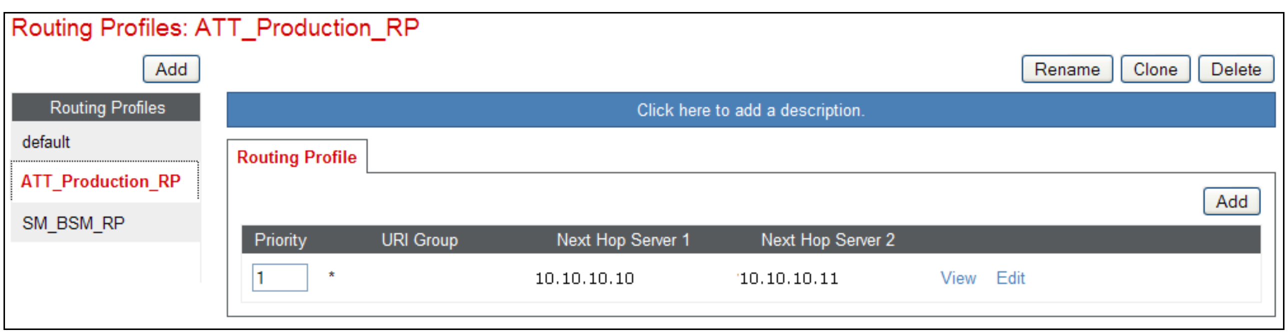


8. Select the **Server Configuration** created in **Section 7.3.7** (e.g., **ATT_Primary_SC**)
9. Select the **Heartbeat Tab**
10. Select **Edit**
11. Repeat **Steps 6 – 7,** using the information shown below, and then click **Finish** (not shown).



11.2. 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 7.3.4** (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).

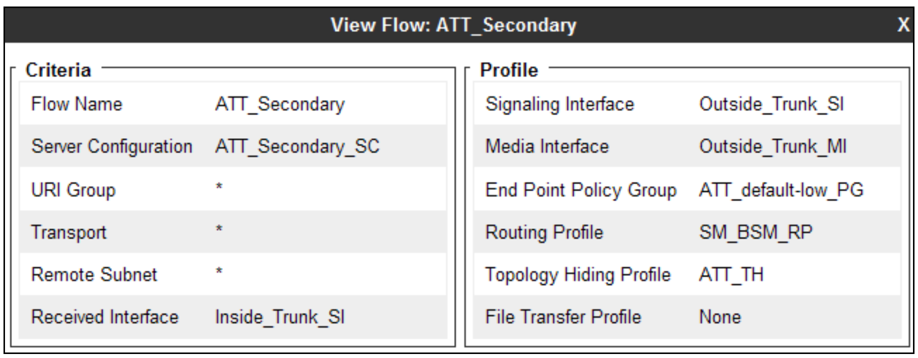


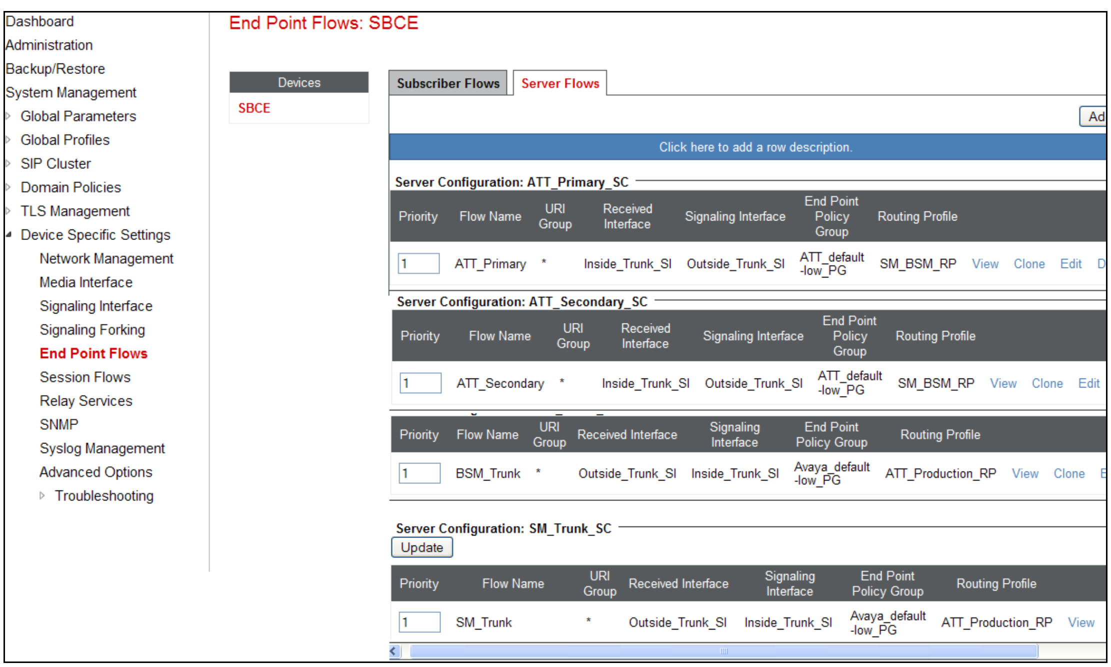
11.3. Configure End Point Flows – Server Flow - ATT_Secondary

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 7.5.4**).
g) **Signaling Interface: Outside_Trunk_ SI (Section 7.5.4**).
h) **Media Interface: Outside_trunk_MI** (**Section 7.5.3**).
i) **End Point Policy Group**: **ATT_default-low_PG** (**Section 7.4.5**).
j) **Routing Profile: SM_BSM_RP** (**Section 7.3.3**).
k) **Topology Hiding Profile: ATT_TH** (**Section 7.3.9**).
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.