



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, and Avaya Session Border Controller for Enterprise 4.0.5, with AT&T IP Flexible Reach - Enhanced Features – Issue 1.0**

### **Abstract**

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and the Avaya Session Border Controller for Enterprise with the AT&T IP Flexible Reach - Enhanced Features service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Session Manager 6.3 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.3 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise 4.0.5 is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach - Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T Flexible Reach 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.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results .....	6
2.2.1.	Known Limitations .....	6
2.3.	Support .....	9
3.	Reference Configuration.....	9
3.1.	Illustrative Configuration Information .....	12
3.2.	AT&T IP Flexible Reach - Enhanced Features Service Call Flows .....	13
3.2.1.	Inbound .....	13
3.2.2.	Outbound.....	14
3.2.3.	Call Forward Re-direction .....	14
3.2.4.	Coverage to Voicemail .....	15
3.3.	AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow .....	16
4.	Equipment and Software Validated .....	17
5.	Configure Avaya Aura® Session Manager .....	18
5.1.	SIP Domain .....	20
5.2.	Locations .....	20
5.2.1.	Location for CPE Equipment.....	20
5.3.	Configure Adaptations .....	21
5.3.1.	Adaptation for calls to Avaya Aura® Communication Manager .....	22
5.3.2.	Adaptation for calls to the AT&T IP Flexible Reach – Enhanced Features Service..	24
5.3.3.	Adaptation for calls to Avaya Aura® Messaging.....	25
5.4.	SIP Entities.....	26
5.4.1.	Avaya Aura® Session Manager SIP Entity .....	27
5.4.2.	Avaya Aura® Communication Manager SIP Entity - Public .....	28
5.4.3.	Avaya Aura® Communication Manager SIP Entity – Local .....	30
5.4.4.	Avaya Session Border Controller for Enterprise SIP Entity.....	31
5.4.5.	Avaya Aura® Messaging SIP Entity .....	32
5.5.	Entity Links .....	32
5.5.1.	Entity Link to Avaya Aura® Communication Manager - Public .....	33
5.5.2.	Entity Link to Avaya Aura® Communication Manager Entity - Local .....	33
5.5.3.	Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE .....	34
5.5.4.	Entity Link to Avaya Aura® Messaging .....	34
5.6.	Time Ranges.....	34
5.7.	Routing Policies .....	35
5.7.1.	Routing Policy for AT&T Routing to Avaya Aura® Communication Manager .....	35
5.7.2.	Routing Policy for Outbound Calls to AT&T .....	37
5.7.3.	Routing Policy for Local Routing to/from Avaya Aura® Communication Manager	38
5.7.4.	Routing Policy for Inbound Routing to Avaya Aura® Messaging.....	39
5.8.	Dial Patterns .....	40
5.8.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager .....	40

5.8.2.	Matching Outbound Calls to AT&T .....	42
5.8.3.	Matching Inbound Calls to Avaya Aura® Messaging Pilot Number via Avaya Aura® Communication Manager.....	43
5.8.4.	Message Wait Indicator (MWI) Notification from Avaya Aura® Messaging to Avaya Aura® Communication Manager, and Routing to SIP Telephones. ....	43
5.8.5.	Matching Outbound Calls from Avaya Aura® Messaging via Avaya Aura® Communication Manager.....	44
6.	Configure Avaya Aura® Communication Manager.....	46
6.1.	System Parameters .....	46
6.2.	Dial Plan.....	48
6.3.	IP Node Names.....	49
6.4.	IP Interface for procr .....	49
6.5.	IP Network Regions .....	50
6.5.1.	IP Network Region 1 – Local Region.....	50
6.5.2.	IP Network Region 2 – AT&T Trunk Region .....	52
6.6.	IP Codec Parameters .....	53
6.6.1.	Codecs for IP Network Region 1 (local calls) .....	53
6.6.2.	Codecs for IP Network Region 2 .....	53
6.7.	SIP Trunks.....	54
6.7.1.	SIP Trunk for AT&T calls .....	54
6.7.2.	Local SIP Trunk (Avaya Aura® Messaging and Avaya SIP Telephones).....	57
6.8.	Private Numbering .....	59
6.9.	Route Patterns .....	60
6.9.1.	Route Pattern for Calls to AT&T.....	60
6.9.2.	Route Pattern for Calls to Aura® Messaging .....	61
6.10.	Automatic Route Selection (ARS) Dialing .....	61
6.11.	Automatic Alternate Routing (AAR) Dialing .....	62
6.12.	Provisioning for Coverage to Aura® Messaging .....	62
6.12.1.	Hunt Group for Station Coverage to Avaya Aura® Messaging .....	62
6.12.2.	Coverage Path for Station Coverage to Avaya Aura® Messaging .....	63
6.12.3.	Station Coverage Path to Avaya Aura® Messaging .....	64
7.	Configure Avaya Session Border Controller for Enterprise .....	65
7.1.	Initial Installation/Provisioning.....	65
7.2.	Log Into Avaya SBCE.....	65
7.3.	Global Profiles.....	66
7.3.1.	Server Interworking – Avaya Side.....	66
7.3.2.	Server Interworking – AT&T Side .....	66
7.3.3.	Routing – Avaya Side .....	67
7.3.4.	Routing – AT&T Side.....	68
7.3.5.	Server Configuration – To Avaya Aura® Session Manager .....	69
7.3.6.	Server Configuration – To AT&T IPFR-EF Border Element .....	70
7.3.7.	Topology Hiding – Avaya Side .....	71
7.3.8.	Topology Hiding – AT&T Side.....	71
7.3.9.	Signaling Manipulation.....	72
7.4.	Domain Policies .....	74

7.4.1.	Application Rules.....	74
7.4.2.	Media Rules .....	75
7.4.3.	Signaling Rules .....	76
7.4.4.	Endpoint Policy Groups – Avaya .....	81
7.4.5.	Endpoint Policy Groups – AT&T .....	81
7.5.	Device Specific Settings.....	82
7.5.1.	Network Management.....	82
7.5.2.	Media Interfaces.....	83
7.5.3.	Signaling Interface .....	83
7.5.4.	Endpoint Flows – To Avaya (Session Manager) .....	84
7.5.5.	Endpoint Flows – To AT&T.....	84
7.6.	Troubleshooting Port Ranges .....	85
8.	Configure Avaya Aura® Messaging.....	86
9.	Verification Steps.....	86
9.1.	AT&T IP Flexible Reach – Enhanced Features .....	86
9.2.	Avaya Aura® Communication Manager .....	86
9.3.	Avaya Aura® Session Manager .....	88
9.3.1.	Call Routing Test .....	89
9.4.	Protocol Traces.....	91
10.	Conclusion .....	94
11.	References.....	95
12.	Addendum 1 – Redundancy to Multiple AT&T Border Elements .....	96
12.1.	Step 1: Configure the Secondary Location in Server Configuration.....	96
12.2.	Step 2: Add Secondary IP Address to Routing.....	97
12.3.	Step 3: Configure End Point Flows – ATT_Secondary .....	98
13.	Addendum 2 – Dedicated SIP Trunk for Blind Transfer (Refer Call Redirection) AT&T IP Flexible Reach - Enhanced Feature .....	99
13.1.	Configure Avaya Session Border Controller for Enterprise.....	99
13.1.1.	Create URI Group .....	99
13.1.2.	Routing.....	100
13.2.	Configure Avaya Aura® Session Manager .....	101
13.2.1.	Adaptation for NCR Trunk .....	101
13.2.2.	SIP Entity for NCR Trunk.....	102
13.2.3.	Entity Link for NCR Trunk.....	103
13.2.4.	Routing Policy for NCR Trunk .....	104
13.2.5.	Dial Pattern for NCR Trunk.....	105
13.3.	Configure Communication Manager .....	106
13.3.1.	SIP Trunk for NCR calls .....	106
13.3.2.	Communication Manager Vector (Refer Generation).....	108

# 1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication Manager 6.3, Avaya Aura® Session Manager 6.3, Avaya Aura® System Manager 6.3, and the Avaya Session Border Controller for Enterprise 4.0.5 (referred to in the remainder of this document as Avaya SBCE), with the AT&T IP Flexible Reach - Enhanced Features service using AVPN or MIS/PNT transport connections.

Avaya Aura® Session Manager is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Avaya SBCE is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach - Enhanced Features service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The AT&T Flexible Reach 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 AVPN<sup>1</sup> or MIS/PNT<sup>2</sup> transport services.

**Note** – The AT&T IP Flexible Reach - Enhanced Features service will be referred to as IPFR-EF in the remainder of this document.

## 2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya System Manager, Session Manager, Communication Manager, Avaya phones, fax machines (Ventafax application), Avaya Session Border Controller for Enterprise, and Avaya Aura® Messaging.
- An IPFR-EF service production circuit, to which the simulated enterprise was connected via AVPN transport.

### 2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Sections 3.2** and **3.3** for examples) between Session Manager, Communication Manager, the Avaya SBCE, and the IPFR-EF service.

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

---

<sup>1</sup> AVPN supports compressed RTP (cRTP).

<sup>2</sup> MIS/PNT does not support cRTP.

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

- SIP trunking.
- Inbound and outbound dialing including international calls.
- Voicemail (leave and retrieve messages).
- 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.
- Avaya Aura® Messaging Reach-Me and Notify-Me outbound calling features.
- 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. The following observations were noted during testing:

### 2.2.1. Known Limitations

1. **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 RecOnly). 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 create two SIP trunks:
    - Create a “general access” SIP trunk, with NCR *disabled*, for inbound and outbound calls (see **Section 6.7**). Note that Meet-Me conference calls must be directed to this “general access” trunk as well (see **item 3**).

- Create an “NCR enabled” SIP trunk used exclusively for customers using the IPFR-EF “Blind Transfer” feature that utilizes Refer, which requires that NCR be enabled (see **Addendum 2**).
2. **Communication Manager station transfer issues 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 station initiated transfers to the PSTN will use Refer signaling (Refer with Replaces) to perform the transfers. *IPFR-EF does not support Refer with Replaces.*
      - The workaround for this issue is the same as for **item 1**. Use a “general access” SIP trunk, with NCR *disabled*, for inbound and outbound calls (see **Section 6.7**).
  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 the same as for **item 1**. Use a “general access” SIP trunk, with NCR *disabled*, for Meet-Me conferences (see **Section 6.7**).
  4. **Codec negotiation with IPFR-EF Simultaneous Ring/Sequential Ring features.** The Enhanced IP Flexible Reach 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 6.7.1**, 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.**
  - Alternatively, an Avaya SBCE SIP header manipulation script may be used, and is documented in **Section 7.3.9**.
- 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 6.7.1, Step 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. **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.
- 8. **Outbound calls from Avaya SIP endpoints may generate SIP Invites with Endpoint-View and AV-Correlation-ID headers.** The Endpoint-View header has been observed to cause issues with the IPFR-EF service (e.g., returning a 408 Request Timeout). The Endpoint-View and AV-Correlation-ID headers also contain local network information. In addition, an “epv” parameter is inserted into the Contact header that also contains local network information.
  - The workaround is to have the Avaya SBCE remove the **Endpoint-View** and **AV-Correlation-ID** headers, as well as the “epv” parameter (see **Sections 7.3.9, 7.4.3.1, and 7.4.3.2**).
- 9. **Some Avaya SIP endpoints may generate three Bandwidth headers; b=TIAS:64000, b=CT:64, and b=AS:64 (others only generate the b=TIAS:64000 header) that may cause issues with the IPFR\_EF service.** It has been observed that sending these Bandwidth headers may cause issues with the IPFR-EF service (specifically with AT&T IP Teleconferencing), therefore an Avaya SBCE Signaling Manipulation Rule is implemented to remove these headers (see **Section 7.3.9**).
  - It was also found that when all three Bandwidth headers are sent to the SBCE, the Avaya SBCE would only pass a single bandwidth header and block the other two.
    - The Avaya SBCE support team has been notified and an MR submitted.
- 10. **Inbound calls from AT&T may include Resource-Priority headers.** During lab testing it was observed that the IPFR-EF test environment generated a Resource-Priority header in initial Invites. Communication Manager does not process this header correctly (known



issue). Currently, the use of this header has not been migrated to the IPFR-EF production environment.

- As a precaution, an Avaya SBCE Signaling Rule is defined to block this header (see **Section 7.4.3.3**).

**11. IPFR-EF Sequential Ring – Loss of connection if Secondary party is busy.** The following AT&T 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.

**12. 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.

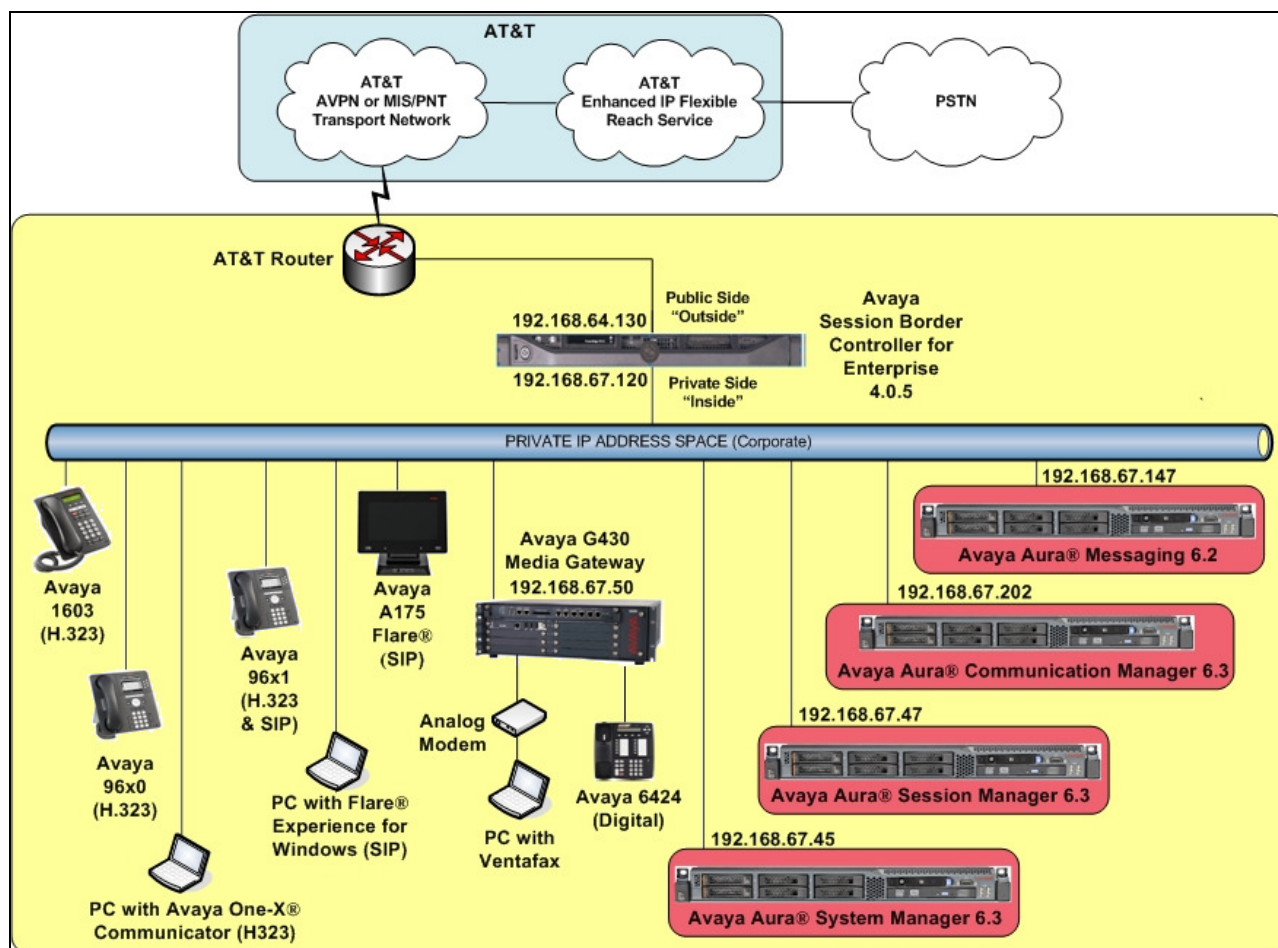
## 3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 1** and consists of the following:

- Avaya Communication Manager 6.3, System Manager 6.3, Session Manager 6.3, and the Avaya SBCE 4.0.5 are used in the reference configuration.

- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications. Avaya SIP endpoints register to Session Manager.
- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager provides the voice communication services for a particular enterprise site. Avaya H.323 endpoints register to Communication Manager.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G430 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya desk telephones used are Avaya 1603 IP Telephone (H.323), 96x1 Series IP Telephones (H.323 and SIP), 96x0 Series IP Telephone (H.323). Avaya A175 (SIP with Flare Experience), Flare Experience for Windows soft phone (SIP), Avaya one-X® Communicator soft phone (H323), as well as 6424 Digital Telephones.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the IPFR-EF service and the enterprise internal network.
- The IPFR-EF service Border Element (BE) uses SIP over UDP to communicate with enterprise edge SIP devices, (e.g., the Avaya SBCE in this sample configuration). Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE, and SIP over TCP and TLS to communicate with Communication Manager. UDP transport protocol is used between the Avaya SBCE and the IPFR-EF service.
- Avaya Aura® Messaging was used in the reference configuration to provide voice messaging capabilities. This solution is extensible to other Avaya Messaging platforms. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Testing was performed using an IPFR-EF service production circuit.

**Note** – Documents used to provision the reference configuration are listed in **Section 11**. Specific references to these documents are indicated in the following sections by the notation [x], where x is the document reference number.



**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
<b>Avaya Aura® System Manager</b>	
IP Address	192.168.67.45
<b>Avaya Aura® Session Manager</b>	
Management IP Address	192.168.67.46
Network IP Address	192.168.67.47
<b>Avaya Aura® Communication Manager</b>	
IP Address	192.168.67.202
Avaya Aura® Communication Manager extensions	19xxx = Stations 4xxxx = VDNs
Voice Messaging Pilot Extension	36000
<b>Avaya Session Border Controller for Enterprise (SBCE)</b>	
IP Address of Outside (Public) Interface (to AT&T IP Flexible Reach-Enhanced Features Service)	192.168.64.130
IP Address of Inside (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.67.120
<b>Avaya Aura Messaging</b>	
IP Address	192.168.67.147
Messaging Mailboxes	19xxx

**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 a placeholder in the following configuration sections, the IP address of **10.10.10.10** and **10.10.10.11** are used to represent the AT&T BE IP addresses.

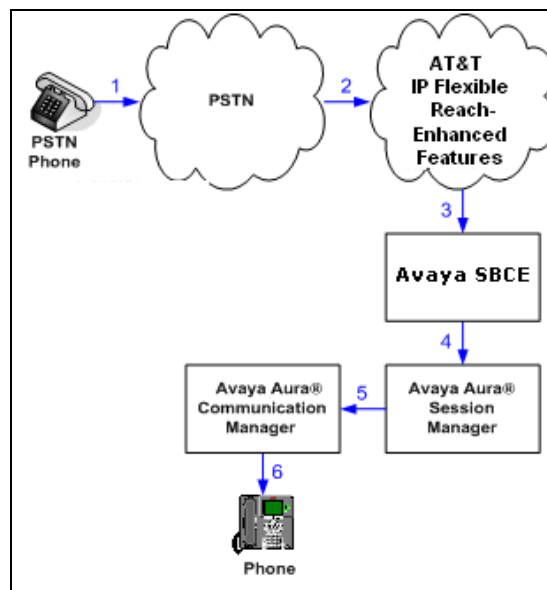
## 3.2. AT&T IP Flexible Reach - Enhanced Features Service Call Flows

To understand how IPFR-EF service calls are handled by the Avaya CPE environment, four 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.

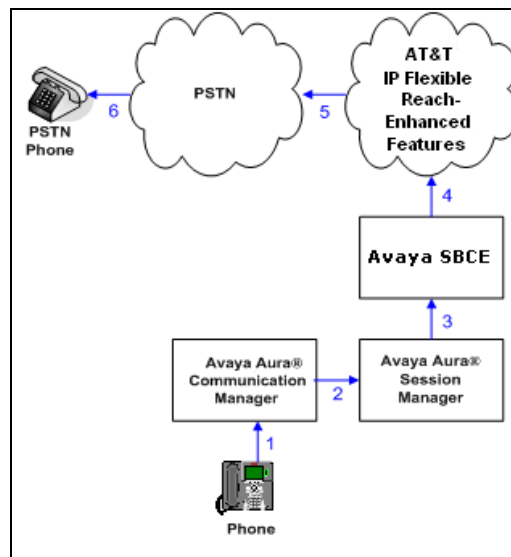


**Figure 2: Inbound IPFR-EF Call**

### 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**

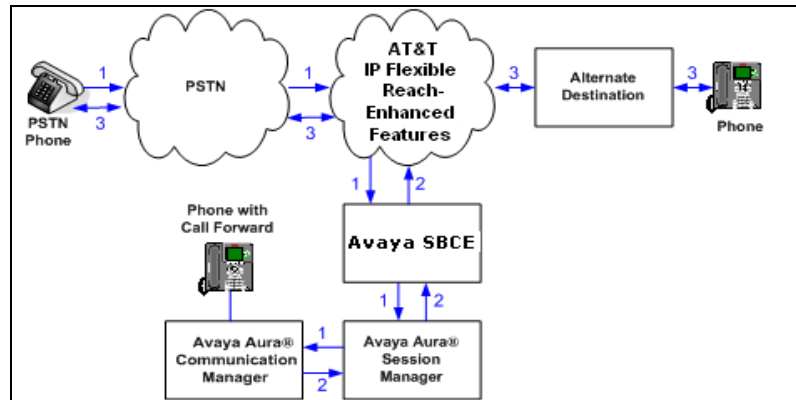
### 3.2.3. Call Forward Re-direction

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 6.7**).

1. Same as the first call scenario in **Section 3.2.1**.

2. 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.
3. The IPFR-EF service places a call to the alternate destination and upon answering; Communication Manager connects the calling party to the target party.

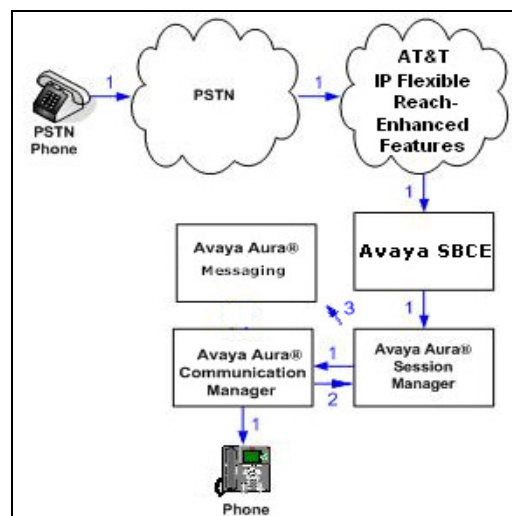


**Figure 4: Station Re-directed (e.g. Call Forward) IPFR-EF Call**

### 3.2.4. Coverage to Voicemail

The call scenario illustrated is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Aura® Messaging system.

1. Same as the first call scenario in **Section 3.2.1**.
2. The called Communication Manager phone does not answer the call, and the call goes to coverage.
3. Communication Manager forwards the call to Avaya Aura® Messaging (via Session Manager). Avaya Aura® Messaging answers the call and connects the caller to the called phone's voice mailbox.



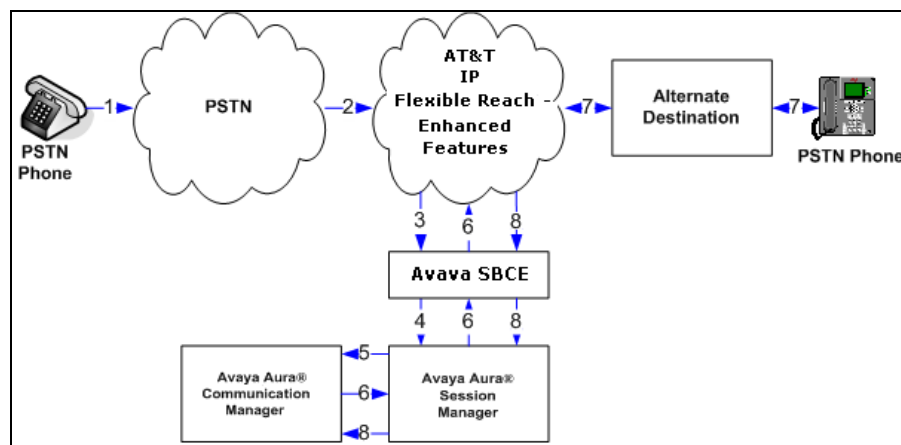
**Figure 5: Coverage to Voicemail**

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

**Note** - For customers requiring the use of the IPFR-EF “Blind Transfer” feature (utilizing Refer), a separate SIP trunk with NCR enabled is required for this use (see **Section 2.2.1, Items 1 through 3** as well as **Addendum 2**).

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)**



## 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 <ul style="list-style-type: none"> <li>System Platform</li> <li>Avaya Aura® System Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3.0.0.18002</li> <li>6.3.2.4 with SP1 (r1212) and patch 2 (r1451)</li> </ul>
IBM 8800 server <ul style="list-style-type: none"> <li>Avaya Aura® Session Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3 SP2 (6.3.2.632023)</li> </ul>
IBM 8800 server <ul style="list-style-type: none"> <li>System Platform</li> <li>Avaya Aura® Communication Manager</li> </ul>	<ul style="list-style-type: none"> <li>6.3.0.0.18002</li> <li>6.3 SP0 (06.3-03.0.124.0-20553)</li> </ul>
Dell R610 <ul style="list-style-type: none"> <li>System Platform</li> <li>Avaya Aura® Messaging</li> </ul>	<ul style="list-style-type: none"> <li>6.2.1.0.9</li> <li>6.2 SP3 (MSG-02.0.823.0-109_0304)</li> </ul>
Avaya G430 Media Gateway <ul style="list-style-type: none"> <li>MM712 Digital card</li> </ul>	33.13.0 <ul style="list-style-type: none"> <li>HW7 FW11</li> </ul>
Dell R310 <ul style="list-style-type: none"> <li>Avaya Session Border Controller for Enterprise</li> </ul>	<ul style="list-style-type: none"> <li>4.0.5 Q19</li> </ul>
Avaya 96x0 IP Telephone	H.323 Version S3.2
Avaya 96x1 IP Telephone	H.323 Version S6.2408 SIP Version 6.2.2.17
Avaya 9601 IP Telephone	SIP Version 6.1.5.12
Avaya one-X® Communicator	H323 6.1 SP8 (6.1.8.06)
Avaya 1603 IP Telephone	H323 (ha1603ua1_3200.bin)
Avaya Flare® Experience for A175	SIP A175-IPT-SIP-R1_1_3-021913
Avaya Flare® Experience for Windows	SIP 1.1.2.11
Avaya 6424 Digital telephone	-
Ventafax Home Version (Windows based Fax device)	6.1.59.144

**Table 2: Equipment and Software Versions**

**Note** - Compliance testing of solutions included the Avaya Session Border Controller for Enterprise (Avaya SBCE) version 4.0.5; also includes those solutions with the Avaya SBCE version 6.2 as well.

## 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] through [4] for further details if necessary.

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunks between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Avaya SBCE. In addition, provisioning for calls to Avaya Aura® Messaging is described.

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as SIP Entities and the connections/trunks between Session Manager and those components are represented as Entity Links. Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates said administration in a central place, namely System Manager.

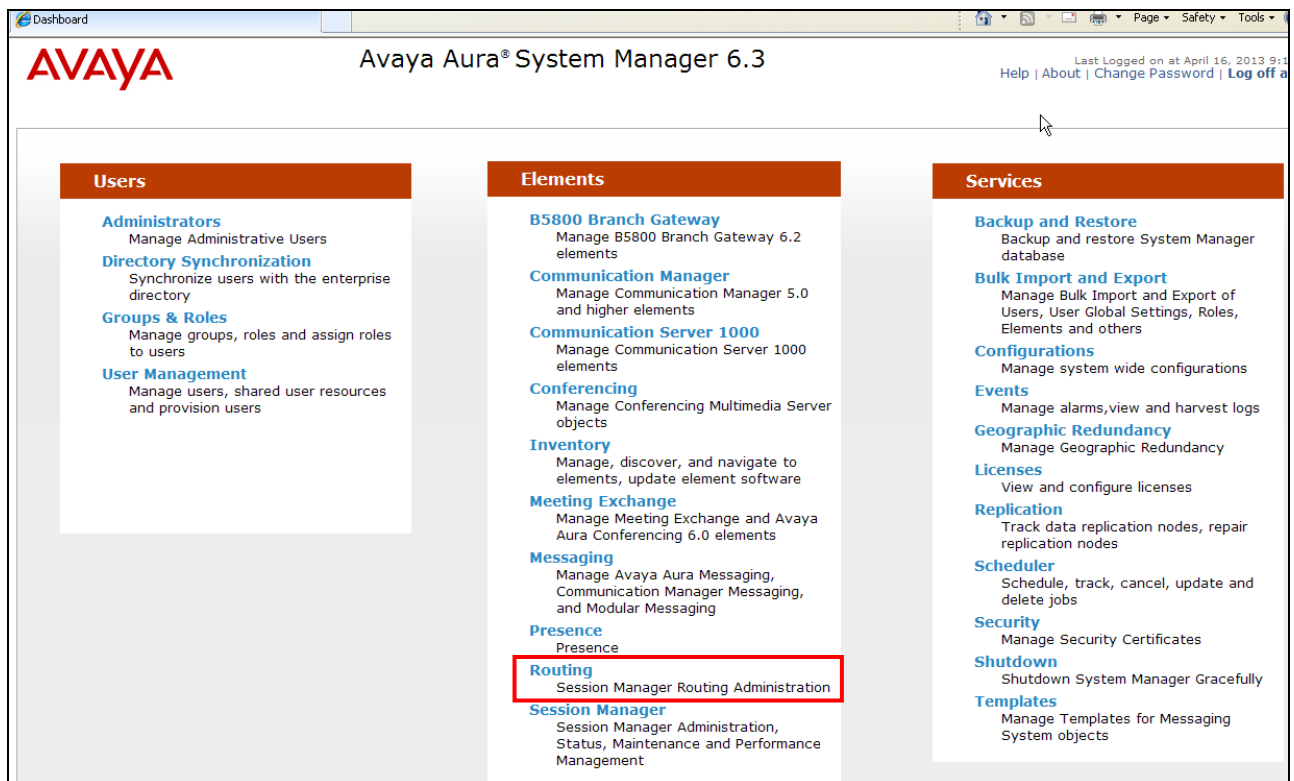
When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as Adaptations, are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of normalizing the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed Dial Patterns, and determines the destination SIP Entities based on Routing Policies specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

The following administration activities will be described:

- Define SIP Domain(s)
- Define a Location for Customer Premises Equipment (CPE), including Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Define SIP Entities corresponding to Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Define Entity Links describing the SIP trunks between Communication Manager and Session Manager, the SIP trunk between Session Manager and the Avaya SBCE, and the SIP trunk between Session Manager and Avaya Aura® Messaging.
- Define Routing Policies associated with Communication Manager, the Avaya SBCE and Avaya Aura® Messaging.
- Define Dial Patterns, which govern which Routing Policy will be selected for call routing.

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager.

In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



## 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. [Optional]

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

Avaya Aura® System Manager 6.3

Last Logged on at April 16, 2013 9:14 AM  
Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Domains

Domain Management

Commit Cancel

1 Item Refresh Filter: Enable

Name	Type	Notes
customera.com	sip	

Commit Cancel

**Note** – Multiple SIP Domains may be defined if required.

## 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, the Location "**Main**" was defined for the entire Customer Premises Equipment (CPE) using subnet **192.168.67.\***.

### 5.2.1. Location for CPE Equipment

The Location **Main** is used for the CPE Avaya equipment (e.g., Communication Manager, Session Manager, Avaya SBCE, and Avaya Aura® Messaging).

**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. [Optional]

**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. [Optional]

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

**AVAYA** Avaya Aura® System Manager 6.3 Help

Home / Elements / Routing / Locations

**Location Details** Commit Cancel

**General**

\* Name:

Notes:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

**Per-Call Bandwidth Parameters**

Maximum Multimedia Bandwidth (Intra-Location):  Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):  Kbit/Sec

\* Minimum Multimedia Bandwidth:  Kbit/Sec

\* Default Audio Bandwidth:  Kbit/sec

**Alarm Threshold**

Overall Alarm Threshold:  %

Multimedia Alarm Threshold:  %

\* Latency before Overall Alarm Trigger:  Minutes

\* Latency before Multimedia Alarm Trigger:  Minutes

**Location Pattern**

Add Remove

1 Item Refresh

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*192.168.67.*	

Select : All, None

Commit Cancel

### 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.

- 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**) is replaced with **customera.com** for source domain.
- The AT&T called number digit strings in the Request URI are replaced with their associated Communication Manager extensions/VDNs.
- Calls to AT&T (**Section 5.3.2**) - Modification of SIP messages sent by Communication Manager.
  - The domain of Session Manager (**customera.com**) is replaced with the AT&T BE IP address (**10.10.10.10**) in the destination headers (see the note in **Section 3.1**).
  - The domain of Session Manager (**customera.com**) is replaced with the Avaya SBCE private IP address (**192.168.67.120**) in the origination headers.
  - The History-Info header is removed automatically by the ATAdapter.
- Calls to Avaya Aura® Messaging from AT&T/PSTN (**Section 5.3.3**)
  - The AT&T called number digit strings in the Request URI are replaced with the Avaya Aura® Messaging pilot number.

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

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager from AT&T, and to direct incoming calls to their associated Communication Manager extensions.

**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**).
3. In the **Module parameter** field enter **odstd=customera.com osrcd=customera.com**. The **odstd** parameter will replace the IP address of Session Manager (**192.168.67.47**) with **customera.com** in the *inbound* Request URI, and the **osrcd** parameter will replace the AT&T Border Element IP address (**10.10.10.10**) with **customera.com**, when Session Manager sends the Invite to Communication Manager (see the note in **Section 3.1**).

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations (highlighted), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area is titled 'Home / Elements / Routing / Adaptations' and 'Adaptation Details'. It includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible:
 

- \* Adaptation name: ACM63\_public
- Module name: DigitConversionAdapter (dropdown menu)
- Module parameter: odstd=customera.com osrcd=cus
- Egress URI Parameters: (empty text box)
- Notes: (empty text box)

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

- Example: 5553161 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Communication Manager extension 19001.
  - 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.

**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 Incoming Calls to SM

Add

Remove

0 Items

Refresh

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
--	------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

Digit Conversion for Outgoing Calls from SM

Add

Remove

9 Items

Refresh

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*5553161	*7	*7		*7	19001	destination		sequential ring
<input type="checkbox"/>	*5553162	*7	*7		*7	19023	destination		sequential ring
<input type="checkbox"/>	*5553163	*7	*7		*7	19021	destination		Call Forward
<input type="checkbox"/>	*5553164	*7	*7		*7	19002	destination		Call Forward
<input type="checkbox"/>	*5553165	*7	*7		*7	19002	destination		simultaneous ring
<input type="checkbox"/>	*5553166	*7	*7		*7	19001	destination		simultaneous ring
<input type="checkbox"/>	*5553171	*7	*7		*7	40010	destination		VDN
<input type="checkbox"/>	*5553172	*7	*7		*7	40020	destination		VDN
<input type="checkbox"/>	*5553173	*7	*7		*7	40030	destination		VDN

Select : All, None

Commit

Cancel

### 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.

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

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

- A descriptive **Name**, (e.g., **ATT**).
- 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), if sent by Communication Manager (see **Section 6.7.1**).
- In the **Module parameter** field enter **odstd=<AT&T border Element IP address>** **osrcd=<Avaya SBCE public IP address>**. For example:

*odstd= 10.10.10.10 osrcd=192.168.64.130*

**Step 3** - Click on **Commit**.

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



Avaya Aura® System Manager 6.3

Last Logged on at April 16, 2013 9:15 AM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) × [Home](#)

Home / Elements / Routing / Adaptations

**Adaptation Details** [Commit](#) [Cancel](#)

**General**

\* Adaptation name:

Module name:

Module parameter:

Egress URI Parameters:

Notes:

**Digit Conversion for Incoming Calls to SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

**Digit Conversion for Outgoing Calls from SM**

[Add](#) [Remove](#)

0 Items [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
--------------------------	------------------	-----	-----	---------------	---------------	---------------	-------------------	-----------------	-------

[Commit](#) [Cancel](#)

### 5.3.3. Adaptation for calls to Avaya Aura® Messaging

The Adaptation administered in this section is used for modification of SIP messages from AT&T to Avaya Aura® Messaging.

**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:

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

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

- Example: 5553170 is a DNIS string sent in the Request URI by the IPFR-EF service that is associated with Avaya Aura® Messaging pilot number 36000.
  - Enter **5553170** in the **Matching Pattern** column.
  - Enter **7** in the **Min/Max** columns.
  - Enter **7** in the **Delete Digits** column.
  - Enter **36000** in the **Insert Digits** column.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

**Step 4** - Click on **Commit**.

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

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and user information. A left sidebar lists various configuration categories under 'Routing'. The main content area is titled 'Home / Elements / Routing / Adaptations' and shows the 'Adaptation Details' for an adaptation named 'AAM\_Digits'. The 'General' tab is active, showing fields for 'Adaptation name', 'Module name' (set to 'DigitConversionAdapter'), 'Module parameter', 'Egress URI Parameters', and 'Notes'. Below the general settings, there are two sections for digit conversion: 'Digit Conversion for Incoming Calls to SM' (currently showing 0 items) and 'Digit Conversion for Outgoing Calls from SM' (showing 1 item). The outgoing conversion table has columns for Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. The single entry shows a matching pattern of '\*5553170' and a delete digit of '10'.

## 5.4. SIP Entities

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

- Session Manager (**Section 5.4.1**).
- Communication Manager for AT&T access (**Section 5.4.2**) – 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.
- Communication Manager for local access (**Section 5.4.3**) – This entity, and its associated Entity Link (using TLS with port 5061), is primarily for traffic between Avaya SIP telephones and Communication Manager.
- Avaya SBCE (**Section 5.4.4**) - 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.
- Avaya Aura® Messaging (**Section 5.4.5**) – This entity, and its associated Entity Link (using TCP and port 5060), is for traffic from Avaya Aura® Messaging to Communication Manager.

**Note** – In the reference configuration, only the “Local” trunk defined between Session Manager and Communication Manager used TLS (port 5061). TCP is used as the transport protocol between Session Manager and the Communication Manager “Public” trunk (port 5062), the Avaya SBCE (port 5060), and Avaya Aura® Messaging (port 5060). This was done to facilitate protocol trace analysis. In addition TCP and port 5080 is used for the dedicated “NCR enabled” trunk (see **Addendum 2**). Avaya best practices call for TLS (port 5061) to be used as the transport protocol whenever possible.

### 5.4.1. Avaya Aura® Session Manager SIP Entity

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

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

- **Name** – Enter a descriptive name for Session Manager (e.g., **sm63**).
- **FQDN or IP Address** – Enter the IP address of the 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.

AVAYA Avaya Aura® System Manager 6.3

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

\* Name: sm63

\* FQDN or IP Address: 192.168.67.47

Type: Session Manager

Notes:

Location: Main

Outbound Proxy:

Time Zone: America/New\_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

**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** (see note above).
- **Protocol** – Select **TCP** (see note above).
- **Default Domain** – Select a SIP domain administered in **Section 5.1** for the selected **Default Domain** field (e.g., **customer.com**)

This is for connections to Avaya SBCE and Avaya Aura® Messaging.

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

- **5062** for **Port** and **TCP** for **Protocol**. This is for public traffic between the Communication Manager and the Avaya SBCE/AT&T.
- **5080** for **Port** and **TCP** for **Protocol** (see **Addendum 2**).

- **5061** for **Port** and **TLS** for **Protocol**. This is for the “Local” trunk between Session Manager and Communication Manager.

**Port**

TCP Failover port:

TLS Failover port:

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5061	TLS	customera.com	Local traffic
<input type="checkbox"/>	5062	TCP	customera.com	Public traffic
<input type="checkbox"/>	5080	TCP	customera.com	NCR trunk

Select : All, None

Filter: Enable

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

**Step 7** - Click on **Commit** (not shown).

**Note** – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.

**Note** – The **SIP Responses to an OPTIONS Request** section of the form (not shown) is not used in the reference configuration.

#### 5.4.2. Avaya Aura® Communication Manager SIP Entity - Public

**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 Communication Manager Processor Ethernet (procr) described in **Section 6.3** (e.g. **192.168.67.202**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation 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).

**SIP Entity Details**
Commit Cancel

**General**

\* **Name:**

\* **FQDN or IP Address:**

**Type:**

**Notes:**

**Adaptation:**

**Location:**

**Time Zone:**

**Override Port & Transport with DNS SRV:** ☐

\* **SIP Timer B/F (in seconds):**

**Credential name:**

**Call Detail Recording:**

**SIP Link Monitoring**

**SIP Link Monitoring:**

**Supports Call Admission Control:** ☐

**Shared Bandwidth Manager:** ☐

**Primary Session Manager Bandwidth Association:**

**Backup Session Manager Bandwidth Association:**

**Note** – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.

**Note** – The **SIP Responses to an OPTIONS Request** section of the form (not shown) is not used in the reference configuration.

### 5.4.3. Avaya Aura® Communication Manager SIP Entity – Local

To configure the Communication Manager Local trunk SIP Entity, repeat the steps in **Section 5.4.2**. The **FQDN or IP Address** field is populated with the IP address of Communication Manager and the **Type** field is set to **CM**. See the figure below for the values used in the reference configuration.

The screenshot shows the 'SIP Entity Details' configuration window. At the top right are 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

- Name:** ACM63\_local
- \* FQDN or IP Address:** 192.168.67.202
- Type:** CM (dropdown menu)
- Notes:** (empty text field)
- Adaptation:** (empty dropdown menu)
- Location:** Main (dropdown menu)
- Time Zone:** America/New\_York (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- \* SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown menu)

The 'SIP Link Monitoring' section is expanded, showing:

- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty dropdown menu)
- Backup Session Manager Bandwidth Association:** (empty dropdown menu)

#### 5.4.4. Avaya Session Border Controller for Enterprise SIP Entity

To configure the Avaya SBCE SIP Entity, repeat the steps in **Section 5.4.2**. The **FQDN or IP Address** field is populated with the IP address of the inside interface of the Avaya SBCE and the **Type** field is set to **SIP Trunk**. See the figure below for the values used in the reference configuration.

**SIP Entity Details**CommitCancel

**General**

\*

Name:

A-SBCE

\*

FQDN or IP Address:

192.168.67.120

Type:

SIP Trunk

Notes:

Adaptation:

ATT\_Production\_via\_SBCE

Location:

Main

Time Zone:

America/New\_York

Override Port & Transport with DNS SRV:

☐

\*

SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

CommProfile Type Preference:

**SIP Link Monitoring**

SIP Link Monitoring:

Link Monitoring Enabled

\*

Proactive Monitoring Interval (in seconds):

120

\*

Reactive Monitoring Interval (in seconds):

60

\*

Number of Retries:

1

Supports Call Admission Control:

☐

Shared Bandwidth Manager:

☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

### 5.4.5. Avaya Aura® Messaging SIP Entity

To configure the Avaya Aura® Messaging SIP Entity, repeat the steps in **Section 5.4.2**. The **FQDN or IP Address** field is populated with the IP address of the Avaya Aura® Messaging Application and the **Type** field is set to **Modular Messaging** (note: use this type even with Avaya Aura® Messaging). See the figure below for the values used in the reference configuration.

The screenshot shows the 'SIP Entity Details' configuration window. The 'General' tab is active. The 'Name' field is 'AA-M'. The 'FQDN or IP Address' field is '192.168.67.147'. The 'Type' dropdown is set to 'Modular Messaging'. The 'Notes' field is empty. The 'Adaptation' dropdown is 'AAM\_Digits'. The 'Location' dropdown is 'Main'. The 'Time Zone' dropdown is 'America/New\_York'. The 'Override Port & Transport with DNS SRV' checkbox is unchecked. The 'SIP Timer B/F (in seconds)' field is '4'. The 'Credential name' field is empty. The 'Call Detail Recording' dropdown is 'none'. The 'SIP Link Monitoring' section has a dropdown set to 'Use Session Manager Configuration'. The 'Supports Call Admission Control' and 'Shared Bandwidth Manager' checkboxes are unchecked. The 'Primary Session Manager Bandwidth Association' and 'Backup Session Manager Bandwidth Association' dropdowns are empty. The 'Commit' and 'Cancel' buttons are in the top right corner.

SIP Entity Details		Commit	Cancel
<b>General</b>			
* Name:	AA-M		
* FQDN or IP Address:	192.168.67.147		
Type:	Modular Messaging		
Notes:			
Adaptation:	AAM_Digits		
Location:	Main		
Time Zone:	America/New_York		
Override Port & Transport with DNS SRV:	<input type="checkbox"/>		
* SIP Timer B/F (in seconds):	4		
Credential name:			
Call Detail Recording:	none		
<b>SIP Link Monitoring</b>			
SIP Link Monitoring:	Use Session Manager Configuration		
Supports Call Admission Control:	<input type="checkbox"/>		
Shared Bandwidth Manager:	<input type="checkbox"/>		
Primary Session Manager Bandwidth Association:			
Backup Session Manager Bandwidth Association:			

## 5.5. Entity Links

In this section, Entity Links are administered between Session Manager and the following SIP Entities:

- Avaya Aura® Communication Manager – Public (**Section 5.5.1**).
- Avaya Aura® Communication Manager – Local (**Section 5.5.2**).
- Avaya SBCE (**Section 5.5.3**).
- Avaya Aura® Messaging (**Section 5.5.4**).

**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. Entity Link to Avaya Aura® Communication Manager - Public

**Step 1** - In the left pane under **Routing**, click on **Entity Links**. In the **Entity Links** page, 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., **ACM63\_public**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager. SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter **5062** (see **Section 5.4.1**).
- **Protocol** – Select **TCP**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity (e.g., **ACM63\_public**).
- **SIP Entity 2 Port** - Enter **5062**.
- **Connection Policy** – Select **Trusted**.

**Step 3** - Click on **Commit**.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
*ACM63_public	*sm63	TCP	*5062	*ACM63_public	*5062	Trusted	<input type="checkbox"/>	

### 5.5.2. Entity Link to Avaya Aura® Communication Manager Entity - Local

To configure this Entity Link, repeat the steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.3** for the Communication Manager local Entity (e.g., **ACM63\_Local**). The **Protocol** is **TLS** and the **Port** is **5061**. See the figure below for the values used in the reference configuration.

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
*ACM63_Local	*sm63	TLS	*5061	*ACM63_local	*5061	Trusted	<input type="checkbox"/>	

### 5.5.3. 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 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.4** for the Avaya SBCE. The **Protocol** is **TCP** and the **Port** is **5060**. See the figure below for the values used in the reference configuration.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
*A-SBCE	sm63	TCP	*5060	*A-SBCE	*5060	Trusted	<input type="checkbox"/>	

### 5.5.4. Entity Link to Avaya Aura® Messaging

To configure this Entity Link, repeat the steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.5**. The **Protocol** is **TCP** and the **Port** is **5060**. See the figure below for the values used in the reference configuration.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
*AA-M	sm63	TCP	*5060	*AA-M	*5060	Trusted	<input type="checkbox"/>	

## 5.6. Time Ranges

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

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

**Step 3** - Click on **Commit**.

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

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

## 5.7. Routing Policies

In this section, the following Routing Policies are administered:

- Calls to Communication Manager from AT&T (**Section 5.7.1**).
- Calls to AT&T (**Section 5.7.2**).
- Avaya Aura® Messaging Message Wait Indicator (MWI) notification to Communication Manager, Avaya Aura® Messaging outbound dialing, and access to/from SIP phones (**Section 5.7.3**).
- Communication Manager call coverage to Avaya Aura® Messaging (**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.

**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.

Routing Policy Details

Commit Cancel

General

\* Name:

Disabled: ☐

\* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
------	--------------------	------	-------

**Step 4** - In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**ACM63\_Public**), and click on **Select** (not shown).

SIP Entities			
6 Items Refresh			
	Name	FQDN or IP Address	Type
<input type="radio"/>	AA-M	192.168.67.147	Modular Messaging
<input type="radio"/>	ACM63_local	192.168.67.202	CM
<input checked="" type="radio"/>	ACM63_public	192.168.67.202	CM
<input type="radio"/>	A-SBCE	192.168.67.120	Other
<input type="radio"/>	sm63	192.168.67.47	Session Manager
Select : None			

- 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**.

Routing Policy Details
Commit Cancel

General

\* Name:

Disabled: ☐

\* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM63_public	192.168.67.202	CM	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	1	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Select : All, None

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

Commit Cancel

## 5.7.2. 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 5.4.4** 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.

Routing Policy Details

Commit

Cancel

General

\* Name:

A-SBCE\_to\_ATT

Disabled:

☐

\* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
A-SBCE	192.168.67.120	Other	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add

Remove

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Select : All, None

Regular Expressions

Add

Remove

0 Items

Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

### 5.7.3. Routing Policy for Local Routing to/from Avaya Aura® Communication Manager

This Routing Policy is used for Avaya Aura® Messaging Message Wait Indicator (MWI) notification to Communication Manager, Avaya Aura® Messaging outbound dialing, and access to/from SIP phones. 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 local calls to Communication Manager (e.g. **ACM63\_Local**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.3** for the Communication Manager local SIP Entity (e.g. **ACM63\_Local**).
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Routing Policy Details

CommitCancel

General

\* Name:

ACM63\_Local

Disabled:

☐

\* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM63_Local	192.168.67.202	CM	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: Enable

<input type="checkbox"/>	Ranking	1	Name	2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0		24/7		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

AddRemove

2 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Select : All, None

Regular Expressions

AddRemove

0 Items RefreshFilter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

#### 5.7.4. Routing Policy for Inbound Routing to Avaya Aura® Messaging

This Routing Policy is used for Call Coverage from Communication Manager to Avaya Aura® Messaging, as well as inbound calls to Avaya Aura® Messaging, for message retrieval. Repeat **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 Avaya Aura® Messaging (e.g. **To\_AAM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.5** for Avaya Aura® Messaging (e.g. **AA-M**), and click on **Select**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Routing Policy Details

CommitCancel

General

\* Name: To\_AAM

Disabled: ☐

\* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AA-M	192.168.67.147	Modular Messaging	

Time of Day

AddRemoveView Gaps/Overlaps

1 Item Refresh

Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

AddRemove

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
--------------------------	---------	-----	-----	----------------	------------	----------------------	-------

Select : All, None

Regular Expressions

AddRemove

0 Items Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

## 5.8. Dial Patterns

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

- Inbound PSTN calls via the IPFR-EF service to Communication Manager.
- Inbound PSTN message retrieval to the Avaya Aura® Messaging pilot number.
- Outbound calls to AT&T.
- Local Call Coverage/retrieval to Avaya Aura® Messaging from Communication Manager to the Avaya Aura® Messaging pilot number.
- Avaya Aura® Messaging MWI notifications to Communication Manager extensions.
- Outbound calls from Avaya Aura® Messaging (Reach-Me, Notify-Me) to the PSTN via Communication Manager for message notification.

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

In the reference configuration inbound calls from the IPFR-EF service used the 7 digit pattern 555xxxx 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 the SIP Domain defined in **Section 5.1** or **-ALL-**, to select all of the administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if **-ALL-** is selected) can match this Dial Pattern.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

\* Pattern: 555

\* Min: 7

\* Max: 7

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: ATT Production inbound 7 digits



**Step 3** – Scrolling down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on **Add**.

**Step 4** - In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to the Location **Main** see **Section 5.2.1**). Note that only those calls that originate from the selected Location(s), or all administered Locations if the option **Apply The Selected Routing Policies to All Originating Locations** is checked, can match this Dial Pattern.

**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**).

**Originating Location**

☐ Apply The Selected Routing Policies to All Originating Locations

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	Main	

Select : All, None

**Routing Policies**

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ACM63_Local	<input type="checkbox"/>	ACM63_local	
<input type="checkbox"/>	ACM63_NCR	<input type="checkbox"/>	ACM63_NCR	IPFR Call Forward with Refer
<input checked="" type="checkbox"/>	ACM63_Public	<input type="checkbox"/>	ACM63_public	from AT&T
<input type="checkbox"/>	A-SBCE_to_ATT	<input type="checkbox"/>	A-SBCE	
<input type="checkbox"/>	To_AAM	<input type="checkbox"/>	AA-M	

Select : All, None

Select Cancel

**Step 6** - In the **Originating Location** page, click on **Select**.

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

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		ACM63_Public	1	<input type="checkbox"/>	ACM63_public	from AT&T

Select : All, None

**Denied Originating Locations**

Add Remove

0 Items Refresh

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

Commit Cancel

**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 1xxxxyyxxxx, x11 (411, 911), and 011 international calls were verified. In addition, IPFR-EF Call Forward feature access codes (e.g., \*7xyyyzzzxxxx) were verified.

**Step 1** - Following the steps shown in **Section 5.8.1**, enter the following:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to AT&T (e.g. **1732**).
- Enter a **Min** and **Max** pattern of **11**.
- In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to “**Main**”.
- 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 5.7.2** (e.g., **A-SBCE\_to\_ATT**).

**Avaya Aura® System Manager 6.3**

Last Logged on at April 17, 2013 5:03 PM  
Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Dial Patterns

**Dial Pattern Details** [Commit] [Cancel] Help ?

**General**

\* Pattern: 1732

\* Min: 11

\* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- [v]

Notes:

**Originating Locations and Routing Policies**

[Add] [Remove]

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		A-SBCE_to_ATT	0	<input type="checkbox"/>	A-SBCE	

Select : All, None

**Denied Originating Locations**

[Add] [Remove]

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

**Step 2** - Repeat **Step 1** to add patterns for IPFR-EF Call Forward codes of **\*7** and **\*9** (Min/Max=13).

**Step 3** - Repeat **Step 1** to add any additional outbound patterns.

### 5.8.3. Matching Inbound Calls to Avaya Aura® Messaging Pilot Number via Avaya Aura® Communication Manager

Communication Manager stations cover to the Avaya Aura® Messaging pilot extension (36000 in the reference configuration). Additionally, stations may dial this pilot extension to retrieve messages or modify mailbox settings. Repeat **Section 5.8.1** with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter a dial pattern for routing calls to Avaya Aura® Messaging (e.g. **36000**).
- Enter a **Min** and **Max** pattern of **5**.
- In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to “**Main**”.
- 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 Avaya Aura® Messaging in **Section 5.7.4** (e.g., **To\_AAM**).

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

\* Pattern: 36000

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: A-MM Pilot number

Originating Locations and Routing Policies

Add Remove

2 Items Refresh

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		To_AAM	0	<input type="checkbox"/>	AA-M	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

### 5.8.4. Message Wait Indicator (MWI) Notification from Avaya Aura® Messaging to Avaya Aura® Communication Manager, and Routing to SIP Telephones.

Avaya Aura® Messaging signals MWI by sending a SIP Notify message to the associated Communication Manager extension. In addition, this entry covers routing of calls to Avaya SIP endpoints. Repeat **Section 5.8.1** with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter the Communication Manager extension pattern based on the 5 digit dial plan defined in **Section 6.2**. In the reference configuration, station extensions used the pattern **19xxx**.
- Enter a **Min** and **Max** pattern of **5**.

- In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to the Avaya Aura® Messaging Location defined in **Section 5.2.1** (e.g., **Main**).
- 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 Communication Manager local trunk in **Section 5.7.3** (e.g., **ACM63\_Local**).

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

\* Pattern: 19

\* Min: 5

\* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: Station MWI and SIP phones

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		ACM63_Local	0	<input type="checkbox"/>	ACM63_local	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

### 5.8.5. Matching Outbound Calls from Avaya Aura® Messaging via Avaya Aura® Communication Manager

Avaya Aura® Messaging supports Reach-Me and Notify-Me outbound calling features. In the reference configuration, Avaya Aura® Messaging generates the outbound call using a 9 prefix, (this matches the Communication ARS dial access code used in the reference configuration and defined in **Section 6.2**), followed by the United States dialing code (**1**), and the 10 digit number. These outbound calls are routed by Session Manager to Communication Manager (to initiate an outbound ARS call), and then Communication Manager sends the call out to AT&T using the routing previously defined in **Section 5.8.2**. Repeat **Section 5.8.1** with the following differences:

- In the **General** section of the **Dial Pattern Details** page, enter the Communication Manager ARS access code prefix that Avaya Aura® Messaging inserts for Reach-Me and Notify-Me calls Messaging (e.g. **91**).
- Enter a **Min** and **Max** pattern of **12** (the ARS code 9 plus an 11 digit outbound number, e.g., 91xxxxxyyxxxx).
- In the **Originating Location** section of the **Originating Locations and Routing Policies** page, check the checkbox corresponding to the Avaya Aura® Messaging Location defined in **Section 5.2.1** (e.g., **Main**).

- 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 Communication Manager local trunk in **Section 5.7.3** (e.g., **ACM63\_local**).

**AVAYA** Avaya Aura® System Manager 6.3 Last Logged on at April 19, 2013 7:54 AM  
Help | About | Change Password | Log off admin

[Routing](#) [Home](#)

Home / Elements / Routing / Dial Patterns [Help ?](#)

**Dial Pattern Details** [Commit](#) [Cancel](#)

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

[Add](#) [Remove](#) Filter: Enable

1 Item [Refresh](#)

<input type="checkbox"/>	Originating Location Name <sup>1</sup>	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup>	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		ACM63_Local	0	<input type="checkbox"/>	ACM63_local	

Select : All, None

**Denied Originating Locations**

[Add](#) [Remove](#) Filter: Enable

0 Items [Refresh](#)

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

## 6. Configure Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult [5] and [6] for further details if necessary.

**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

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 **system-parameters customer-options** 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		
<b>Maximum Administered SIP Trunks:</b>		<b>24000</b>	<b>30</b>		
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 System-Parameters Customer-options 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	
<b>ARS? y</b>	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	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? y		
(NOTE: You must logoff & login to effect the permission changes.)		

**Step 3 - On Page 4 of the system-parameters customer-options form:**  
Verify that the **Enhanced EC500?**, **IP Stations?**, **ISDN-PRI?**, **IP Trunks?**, and **ISDN/SIP Network Call Redirection?** fields are set to y.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	<b>IP Stations? y</b>	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
<b>Enhanced EC500? y</b>	<b>ISDN/SIP Network Call Redirection? y</b>	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	<b>ISDN-PRI? y</b>	
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	
<b>IP Trunks? y</b>		
IP Attendant Consoles? y		
(NOTE: You must logoff & login to effect the permission changes.)		

**Step 5** - On **Page 5** of the **system-parameters customer-options** 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		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? y	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
<b>Private Networking? y</b>	Usage Allocation Enhancements? y	
Processor and System MSP? y		
<b>Processor Ethernet? y</b>	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. 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:
  1. The digit **1** for Communication Manager stations (the pattern 19xxx was used for stations, with the pattern 1902x reserved for SIP stations).
  2. The digit **3** for Avaya Aura® Messaging pilot number (36000).
  3. The digit **4** for Communication Manager VDNs and announcements (4xxxx).
- 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 6.7**.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**), e.g., access code **8** for Automatic Alternate Routing dialing, see **Section 6.11**.
- 1-digit facilities access code (indicated with a **Call Type** of **fac**), e.g., access code **9** for outbound Automatic Route Selection dialing, see **Section 6.10**.



## DIAL PLAN ANALYSIS TABLE

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

### 6.3. 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. The Processor Ethernet node name and IP Address (**procr** & **192.168.67.202**) appear automatically based on the address defined during installation (as does the **default** and **procr6** entries). The 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:

- Session Manager signaling interface (e.g., **SM63** and **192.168.67.47**).
- Avaya Aura® Messaging (**AAM** and **192.168.67.147**).
- Avaya SBCE private network interface (**A-SBCE** and **192.168.67.120**).

## change node-names ip

## IP NODE NAMES

Name	IP Address
<b>A-SBCE</b>	<b>192.168.67.120</b>
<b>AAM</b>	<b>192.168.67.147</b>
<b>SM63</b>	<b>192.168.67.47</b>
<b>default</b>	<b>0.0.0.0</b>
<b>procr</b>	<b>192.168.67.202</b>
<b>procr6</b>	<b>::</b>

### 6.4. IP Interface for procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (procr) parameters. 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**.
- Assign a **Network Region** (e.g., **1**).
- Use default values for the remaining parameters.

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

## 6.5. 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, two network regions are used, one for local calls and one for AT&T calls.

### 6.5.1. IP Network Region 1 – Local Region

In the reference configuration, local Communication Manager elements (e.g., procr) as well as other local Avaya devices (e.g., SIP and H.323 IP telephones, Avaya Aura® Messaging) are assigned to **ip-network-region 1**.

**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., **Local**).
  - 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**).

<b>change ip-network-region 1</b>		<b>Page 1 of 20</b>
IP NETWORK REGION		
Region: 1		
Location: 1	<b>Authoritative Domain: customera.com</b>	
<b>Name: Local</b>		
MEDIA PARAMETERS		
<b>Codec Set: 1</b>	<b>Intra-region IP-IP Direct Audio: yes</b>	
<b>UDP Port Min: 16384</b>	<b>Inter-region IP-IP Direct Audio: yes</b>	
<b>UDP Port Max: 32767</b>	IP Audio Hairpinning? n	
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		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y		RSVP Enabled? n
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.

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

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

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

<b>change ip-network-region 1</b>		<b>Page 4 of 20</b>	
Source Region: 1      Inter Network Region Connection Management			
		I	M
		G	A
		A	G
		R	L
		all	e
		n	t

<b>dst rgn</b>	<b>codec set</b>	direct	WAN	Units	WAN-BW-limits	Video	Intervening	Dyn	CAC
<b>1</b>	<b>1</b>								
<b>2</b>	<b>2</b>	<b>y</b>		<b>NoLimit</b>					
<b>3</b>									



## 6.6. IP Codec Parameters

### 6.6.1. Codecs for IP Network Region 1 (local calls)

In the reference configuration, IP Network Region 1 uses codec set 1.

**Step 1** - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls (e.g., 1). 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				
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>				
Modem	off	0				
TDD/TTY	off	0				
Clear-channel	n	0				

### 6.6.2. Codecs for IP Network Region 2

In the reference configuration IP Network Region 2 uses codec set 2 for calls 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 if desired. For G729B and G729A set **3** for the **Frames Per Pkt**. This will automatically populate **30** for the Packet Size (ms). Let G711MU default to **20**.

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	20			

**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
<b>FAX</b>	<b>t.38-standard</b>	<b>0</b>
Modem	off	0
TDD/TTY	off	0
Clear-channel	n	0

## 6.7. SIP Trunks

Two 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**.
- Local for Avaya Aura® Messaging and Avaya SIP telephone access – SIP Trunk 1
  - Note that this trunk will use TLS port 5061 as described in **Section 5.5.2**.

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

**Note** – Although TCP and TLS are 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.

### 6.7.1. SIP Trunk for AT&T calls

This section describes the steps for administering the SIP trunk to Session Manager used for IPFR-EF calls. This trunk corresponds to the **ACM63\_Public** SIP Entity defined in **Section 5.4.2**.

**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 6.3**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (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 6.5.2**.
- **Far-end Domain** – Enter **customer.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**.

<b>add signaling-group 2</b>		<b>Page 1 of 1</b>
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		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	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**).

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

**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.

<b>add trunk-group 2</b>		<b>Page 2 of 21</b>
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
	Redirect On OPTIM Failure: 6000	
SCCAN? n	Digital Loss Group: 18	
<b>Preferred Minimum Session Refresh Interval(sec): 900</b>		
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 **Numbering 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.

<b>add trunk-group 2</b>		<b>Page 3 of 21</b>
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
<b>Numbering Format: private</b>		
	UII 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 **n** (default). See **Addendum 2** regarding the use of Network Call Redirection (NCR) with the IPFR-EF service.
- 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** – The 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.

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

### 6.7.2. Local SIP Trunk (Avaya Aura® Messaging and Avaya SIP Telephones)

This section describes the steps for administering the local SIP trunk to Session Manager. This trunk is used for Avaya Aura® Messaging and Avaya SIP station calls. This trunk corresponds to the **ACM63\_Local** 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., **1**), and repeat the steps in **Section 6.7.1** with the following changes:

- **Transport Method** – Set to **tls** (see the note at the beginning of this section).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5061** (see the note at the beginning of this section).
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.5.1**.

add signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority Video? y	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM63	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: customera.com	Far-end Secondary Node Name:	
	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

**Step 2** - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., 1). On **Page 1** of the **trunk-group** form, repeat the steps in **Section 6.7.1** 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 6.7.1**.

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

- Same as **Section 6.7.1**.

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

- Set **Telephone Event Payload Type** to the RTP payload type required by the IPFR-EF service (e.g., **100**).
- Use default for all other values.

## 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. Private Numbering

In the reference configuration, the private-numbering form 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.
- Define local extension ranges to facilitate call coverage to Avaya Aura® Messaging via the local trunk.

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

- Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- Ext Code** – Enter the Communication Manager extension assigned to the Avaya Aura® Messaging coverage hunt group defined in **Section 6.12.1** (e.g., **36000**).
- Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

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

- Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- Ext Code** – Enter the Communication Manager extension patterns defined in the Dial Plan in **Section 6.2** (e.g., **1** and **4**).
- Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

**Step 3** – Add a Communication Manager extension and its corresponding IPFR-EF DNIS number (for the public trunk):

- Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- Ext Code** – Enter the Communication Manager 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., **7325553163**).
- 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 Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
5	1	1		5	Total Administered: 11
5	36000	1		5	Maximum Entries: 540
5	4	1		5	
5	19001	2	7327373163	10	
5	19002	2	7327373164	10	
5	19003	2	7327373165	10	
5	19004	2	7327373166	10	
5	19005	2	7327373170	10	
5	19020	2	7327373171	10	
5	19021	2	7327373168	10	
5	19022	2	7327373169	10	

## 6.9. Route Patterns

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

### 6.9.1. 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 6.10** (e.g., calls to AT&T).

**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**.

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

## 6.9.2. Route Pattern for Calls to Aura® Messaging

This form defines the local SIP trunk, based on the route-pattern selected by the AAR table in **Section 6.11** (e.g., calls to the Avaya Aura® Messaging pilot number 36000).

**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

## 6.10. Automatic Route Selection (ARS) Dialing

The ARS table is selected based on the caller dialing the ARS access code (e.g., **9**) as defined in **Section 6.2**. The access code is removed and the ARS table matches the remaining dialed digits and sends them to the designated route-pattern (see **Section 6.9.1**).

**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 17xxxxxxxx.
- 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, but calls to 1900xxxxxxx will be denied.

## ARS DIGIT ANALYSIS TABLE

Location: all

Percent Full: 1

Dialed String	Total Min Max	Route Pattern	Call Type	Node Num	ANI Reqd
1732	11 11	2	hnpa		n
1800	11 11	2	hnpa		n
1900	11 11	deny	fnpa		n

## 6.11. Automatic Alternate Routing (AAR) Dialing

AAR is used to direct coverage calls for Avaya Aura® Messaging (36000) to the route-pattern defined in **Section 6.9.2**.

**Step 1** – Enter the following:

- **Dialed String**
  - Avaya Aura® Messaging Pilot Number, enter **36000**.
  - SIP telephone extension range (see **Section 6.2**), enter **1902** (to match 1902x).
- **Min & Max** – Enter **5**.
- **Route Pattern** – Enter **1**.
- **Call Type** – Enter **aar**.

## AAR DIGIT ANALYSIS TABLE

Location: all

Percent Full: 1

Dialed String	Total Min Max	Route Pattern	Call Type	Node Num	ANI Reqd
1902	5 5	1	aar		n
36000	5 5	1	aar		n

## 6.12. Provisioning for Coverage to Aura® Messaging

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

### 6.12.1. Hunt Group for Station Coverage to Avaya Aura® Messaging

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

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

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

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

- **Message Center** – Enter **sip-adjunct**.
- **Voice Mail Number** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Voice Mail Handle** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Routing Digits** – Enter the AAR access code defined in **Section 6.2** (e.g., **8**).

<b>change hunt-group 1</b>	<b>Page 2 of 60</b>
HUNT GROUP	
<b>Message Center: sip-adjunct</b>	
<b>Voice Mail Number</b>	<b>Voice Mail Handle</b>
36000	36000
<b>Routing Digits</b> (e.g., AAR/ARS Access Code) <b>8</b>	

### 6.12.2. Coverage Path for Station Coverage to Avaya Aura® Messaging

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

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

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

<b>add coverage path 1</b>	<b>Page 1 of 1</b>
COVERAGE PATH	
Coverage Path Number: 1	
Cvg Enabled for VDN Route-To Party? n	Hunt after Coverage? n
Next Path Number:	Linkage
<b>COVERAGE CRITERIA</b>	
Station/Group Status	Inside Call      Outside Call
Active?	n      n
Busy?	Y      Y
Don't Answer?	Y      Y      Number of Rings: 4
All?	n      n
DND/SAC/Goto Cover?	Y      Y
Holiday Coverage?	n      n
<b>COVERAGE POINTS</b>	
Terminate to Coverage Pts. with Bridged Appearances? n	
<b>Point1: h1</b>	<b>Rng: 4</b> Point2:
Point3:	Point4:
Point5:	Point6:

### 6.12.3. Station Coverage Path to Avaya Aura® Messaging

The coverage path configured in the previous section is then defined on the stations.

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

- **Coverage path** – Specify the coverage path defined in **Section 6.12.2**. Note that the coverage path field will appear at different positions on the form depending on whether agent or station extensions are being provisioned.

<b>change station 19001</b>	<b>Page 1 of 5</b>
STATION	
Extension: 19001	Lock Messages? n
Type: 9630	Security Code:
Port: S00000	<b>Coverage Path 1: 1</b>
Name: 9630 H323	Coverage Path 2:
	Hunt-to Station:
STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
Speakerphone: 2-way	Personalized Ringing Pattern: 1
Display Language: english	Message Lamp Ext: 19001
Survivable GK Node Name:	Mute Button Enabled? y
Survivable COR: internal	Button Modules: 0
Survivable Trunk Dest? y	Media Complex Ext:
	IP SoftPhone? n
	IP Video? n
	Short/Prefixed Registration Allowed: default
	Customizable Labels? y



## 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.

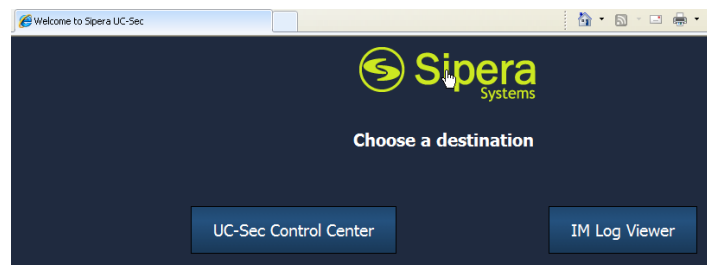
**IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition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

In the reference configuration, the Avaya SBCE interface B1 (192.168.64.130) was used for the public interface (toward AT&T), and interface A1 (192.168.67.120) was the private interface.

### 7.2. Log Into Avaya SBCE

The follow provisioning is performed via the Avaya SBCE GUI interface.

- 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. Select **UC-SEC Control Center**.



- C. Enter the login ID and password.

A screenshot of a "Sign in" form. The form has a light gray background. At the top, the text "Sign in" is displayed in a large, bold, sans-serif font. Below this, there are two input fields: "Login ID" and "Password". The "Login ID" field is highlighted with a red border. Below the input fields is a yellow button with the text "Sign in" in black.

## 7.3. Global Profiles

Global Profiles allow for configuration of parameters across all UC-Sec appliances.

### 7.3.1. Server Interworking – Avaya Side

Server Interworking is used to configure and manage various SIP call server-specific capabilities such as call hold and T.38.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Interworking**.
3. Select the default profile **avaya-ru** and select the **Clone Profile** button. The **Clone Profile** name window will open (not shown). Enter a profile name (e.g., **Avaya\_SI**).
4. Select the **General** Tab, and click on **Edit** (not shown):
  - a. Check **T38 Support** → **Yes**
  - b. All other options on the General Tab can be left at default
  - c. Select **Next**

Editing Profile: Avaya_SI	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<input type="button" value="Next"/>	

5. On the **Privacy** window (not shown), select **Next** to accept default values.
6. On the **SIP Timers** window (not shown), select **Next** to accept default values.
7. On the **Advanced Settings** window (not shown), select **Next** to accept default values.
8. Click **Finish** (not shown).

### 7.3.2. Server Interworking – AT&T Side

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

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:
  - a. Enter a profile name: (e.g., **ATT\_SI**)
  - b. Check **T38 Support**
  - c. All other options on the General Tab can be left at default
  - d. Select **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 **Advanced** Tab (not shown), enter the following:
  - a. Set **Avaya Extensions** to **No**
  - b. Select **Next** to accept remaining default values.
8. Click **Finish**. The completed form is shown below.

The screenshot shows the UC-Sec Control Center interface. On the left is a navigation tree with categories like Administration, System Management, Global Parameters, Global Profiles, and Server Interworking. Under Global Profiles, the 'Server Interworking' section is expanded, and the 'ATT\_SI' profile is selected and highlighted with a red box. The main panel displays the configuration for the 'ATT\_SI' profile. At the top, there are buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. Below these is a tabbed interface with 'General', 'Timers', 'URI Manipulation', 'Header Manipulation', and 'Advanced' tabs. The 'General' tab is active, showing a table of settings. The 'Privacy' and 'DTMF' sections are also visible.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
DTMF Support	None

An 'Edit' button is located at the bottom right of the configuration panel.

### 7.3.3. Routing – Avaya Side

The Routing Profile is used to manage parameters related to routing SIP signaling messages.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Routing** (not shown).
3. Select **Add Profile** (not shown).
4. Enter Profile Name: (e.g., **To\_Avaya**).
5. Click **Next** and enter:
  - a. **Next Hop Server 1: 192.168.67.47** (Session Manager IP address)
  - b. Select **Routing Priority Based on Next Hop Server**
  - c. **Outgoing Transport: TCP**
6. Click **Finish**.

### 7.3.4. Routing – AT&T Side

Repeat the steps in **Section 7.3.3** to add a Routing Profile for the AT&T connection. Note that the AT&T IPFR-EF service provides a Primary and a Secondary Border Element.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Routing**.
3. Select **Add Profile**.
4. Enter Profile Name: (e.g., **ATT\_Production**).
5. Click **Next**, then enter the following:
  - a. **Next Hop Server 1: 10.10.10.10** (Primary AT&T Border Element IP address)
  - b. Select **Routing Priority Based on Next Hop Server**
  - c. **Outgoing Transport: UDP**
6. Click **Finish**.

### 7.3.5. Server Configuration – To Avaya Aura® Session Manager

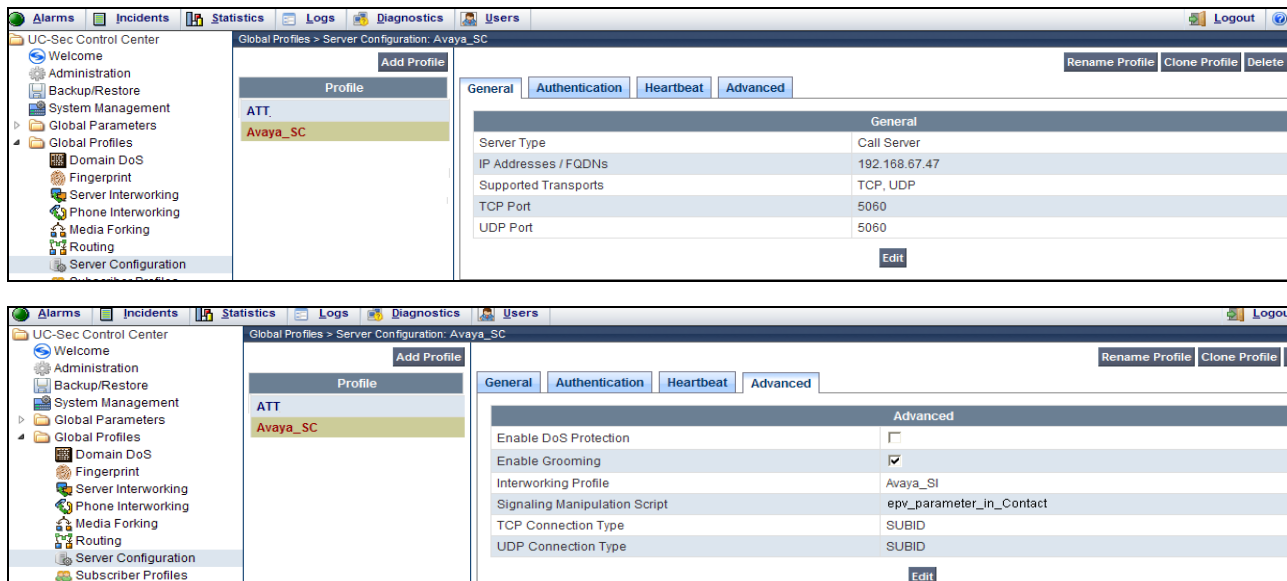
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**, and select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **Avaya\_SC**) and select **Next**.
3. The **Add Server Configuration Profile - General** window will open (not shown).
  - a. Select **Server Type: Call Server**
  - b. **IP Address: 192.168.67.47** (Session Manager IP Address)
  - c. **Supported Transports:** Check **UDP** and **TCP**
  - d. **TCP Port: 5060**
  - e. **UDP Port: 5060**
  - f. Select **Next**
4. The **Add Server Configuration Profile - Authentication** window will open (not shown).
  - a. Select **Next** to accept default values.
5. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
  - a. Select **Next** to accept remaining default values.
6. The **Add Server Configuration Profile - Advanced** window will open.
  - a. For **Interworking Profile** select **Avaya\_SI** created in **Section 7.3.1**.
  - b. For the **Signaling Manipulation Script** select the **epv\_parameter\_in\_Contact** script defined in **Section 7.3.9.1**.

**Note** - See **section 7.3.9.2** for a possible modification to this script.

  - c. Select **Finish**, accepting remaining default values.

The following screen shots show the completed **General** and **Advanced** tabs.

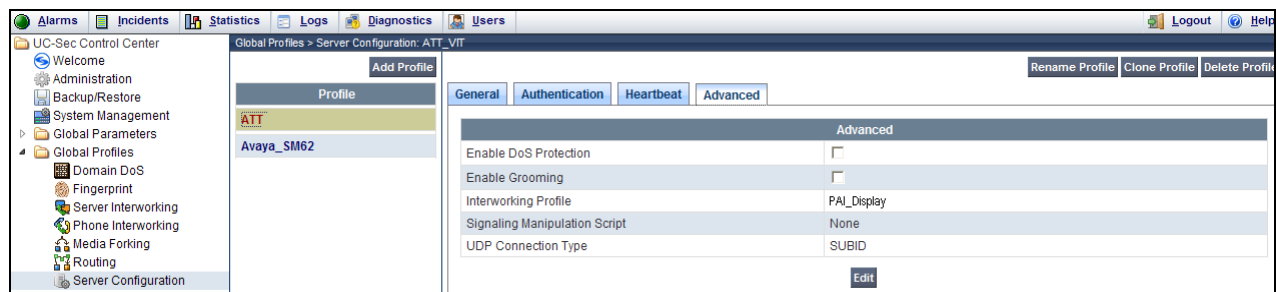
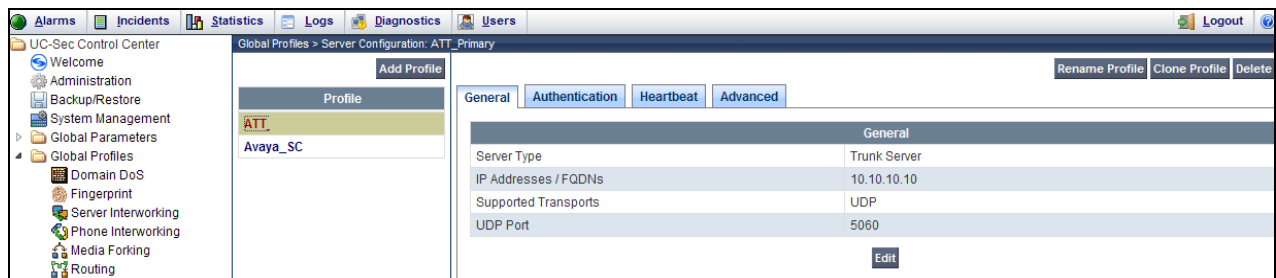


### 7.3.6. Server Configuration – To AT&T IPFR-EF Border Element

Repeat the steps in **Section 7.3.5** to create a Server Configuration for the connection to AT&T.

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., **ATT**) and select **Next**.
4. The **Add Server Configuration Profile - General** window will open (not shown).
  - a. Select Server Type: **Trunk Server**
  - b. **IP Address: 10.10.10.10** (IPFR-EF Border Element IP Address, see **Section 3.1**).
  - c. **Supported Transports**: Check **UDP**
  - d. **UDP 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. Select **Next** to accept default values.
7. The **Add Server Configuration Profile - Advanced** window will open.
  - d. Select **ATT\_SI** for **Interworking Profile** (created in **Section 7.3.2**).
  - a. Select **Finish**.

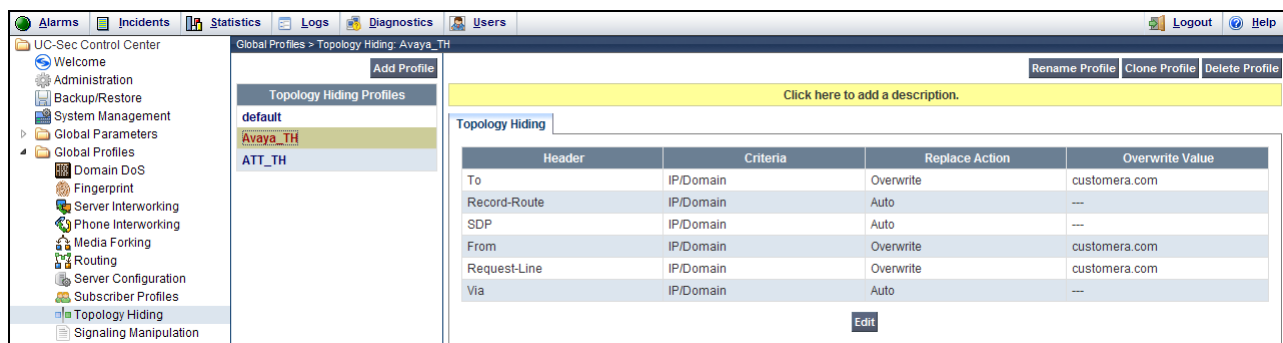
The following screen shots show the completed **General** and **Advanced** tabs.



### 7.3.7. Topology Hiding – Avaya Side

The **Topology Hiding** configuration is used to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

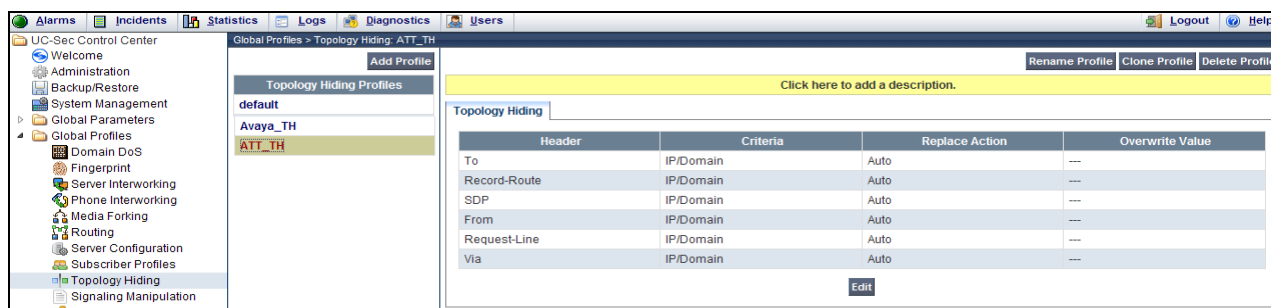
1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Topology Hiding**.
3. Click **default** profile and select **Clone Profile**.
4. Enter Profile Name: (e.g., **Avaya\_TH**).
5. For the Header **To**,
  - a. In the **Criteria** column select **IP/Domain**
  - b. In the **Replace Action** column select: **Overwrite**
  - c. In the **Overwrite Value** column: **customerera.com**
6. 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: **customerera.com**
7. 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: **customerera.com**
8. Click **Finish** (not shown).



### 7.3.8. Topology Hiding – AT&T Side

Repeat the steps in **Section 7.3.7** to create a Topology Hiding Profile for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Topology Hiding**.
3. Click **default** profile and select **Clone Profile**.
4. Enter Profile Name: (e.g., **ATT\_TH**).
5. Set all **Replace Action** to **Auto**.
6. Click **Finish**.



### 7.3.9. Signaling Manipulation

The Avaya SBCE can manipulate inbound and outbound SIP headers. In the reference configuration, only one signaling manipulation script was used (**Section 7.3.9.1**), however an possible modification to that script is also described in **Section 7.3.9.2**.

**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.

**Step 1** - As described in **Section 2.2.1, Item 8**, Avaya SIP endpoints may send requests with Endpoint-View headers containing private network information. These are removed in **Section 8.4.3**. However an “epv” parameter is also inserted into the Contact header of these requests. This parameter also contains private network information. The following signaling manipulation is used to remove this “epv” parameter from the Contact header.

#### 7.3.9.1 Remove “epv” Parameter from Contact Header as well as Bandwidth Headers Sent by Avaya SIP Endpoints.

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., **epv\_parameter\_bandwidth**). The following script is defined:

Title 
Save

```

1 // Remove epv paramater from Contact in SIP endpoint Invite
2
3 within session "INVITE"
4 {
5     act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
6     {
7         remove (%HEADERS["Contact"] [1].URI.PARAMS["epv"]);
8     }
9 }
10

```



**Step 2** - As described in **Section 2.2.1, Item 9**, some Avaya SIP endpoints may send Bandwidth headers that may cause issues with the AT&T network. The following signaling manipulation script is added to the script defined in **Step 1** above, to remove these Bandwidth headers.

Title  Save

```
1 // Remove epv paramater from Contact in SIP endpoint Invite
2
3 within session "INVITE"
4 {
5   act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
6   {
7     remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
8   }
9 }
10
11 // Remove Bandwidth Headers to AT&T
12
13 within session "ALL"
14 {
15   act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
16   {
17     %BODY[1].regex_replace("b=AS:64\r\n", "");
18     %BODY[1].regex_replace("b=CT:64\r\n", "");
19     %BODY[1].regex_replace("b=TIAS:64000\r\n", "");
20   }
21 }
22
```

5. 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 **Section 7.3.5, Step 6**.

### 7.3.9.2 Alternative Method to Alleviate Simultaneous Ring and Sequential Ring Display Issue.

As described in **Section 2.2.1, Item 5**, a display issue was found with the IPFR-EF Simultaneous Ring and Sequential Ring features. The recommended workaround is to modify the Communication Manager trunk configuration (see **Section 6.7.1, Step 5**). For versions of Communication Manager earlier than 6.x (e.g., 5.2.1), the following script modification is used instead.

1. Select the script **epv\_parameter\_in\_Contact** created in **Section 7.3.9.1**, and click on the **Edit** button (not shown).
2. Enter the additional parameters shown below, then click on **Save**.

Title epv\_parameter\_bandwidth

```
1 // Remove epv parameter from Contact in SIP endpoint Invite
2 within session "INVITE"
3 {
4     act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
5     {
6         remove(%HEADERS["Contact"][1].URI.PARAMS["epv"]);
7     }
8 }
9 // Remove Bandwidth Headers to AT&T
10
11 within session "ALL"
12 {
13     act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
14     {
15         %BODY[1].regex_replace("b=AS:64\r\n", "");
16         %BODY[1].regex_replace("b=CT:64\r\n", "");
17         %BODY[1].regex_replace("b=TIAS:64000\r\n", "");
18     }
19 }
20 //Fix for EIPFR Simultaneous and Sequential Ring display issue (ACM 521 only)
21
22 within session "Invite"
23 {
24     act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
25     {
26         if (exists(%HEADERS["P-Asserted-Identity"][1])) then
27         {
28             %var1 = %HEADERS["P-Asserted-Identity"][1];
29         }
30         else
31         {
32             %HEADERS["P-Asserted-Identity"][1] = %var1;
33         }
34     }
35 }
```

As stated in **Section 7.3.9.1**, this script is applied to the Avaya Server Configuration in **Section 7.3.5, Step 6**.

## 7.4. Domain Policies

The Domain Policies are used to configure, apply, and manage various rule sets (policies) to control communications based upon various criteria of 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
2. Select **Application Rules**
3. Select the **default** Rule
4. Select **Clone Rule** button
  - a. Name: **new-default**
  - b. Click **Finish**
5. Highlight the rule just created: **new-default**
  - a. Click the **Edit** button

- b. In the **Voice** row:
  - i. Change the **Maximum Concurrent Sessions** to an appropriate amount (e.g., **1000**)
  - ii. Change the **Maximum Sessions per Endpoint** to an appropriate amount (e.g., **1000**)

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	None
IM Logging	No
RTCP Keep-Alive	No

## 7.4.2. Media Rules

This Media Rule will be applied to both directions and therefore, only one rule is needed.

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select **Media Rules** (not shown).
3. From the Media Rules menu, select the **default-low-med** rule
4. Select **Clone Rule** button
  - a. Name: **default-low-med-QOS**
  - b. Click **Finish**
5. Highlight the rule just created from the Media Rules menu: **default-low-med-QOS**
  - a. Select the **Media QoS** tab (not shown).
  - b. Click the **Edit** button and the **Media QoS** window will open.
  - c. Check the **Media QoS Marking - 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 screen shot below shows the completed **Media Rules** window.

Domain Policies > Media Rules: default-low-med-QOS

Media Rules

default-low-med

default-low-med-enc

default-high

default-high-enc

avaya-low-med-enc

**default-low-med-QOS**

Media QoS

Media QoS Reporting

RTCP Enabled ☐

Media QoS Marking

Enabled ☒

QoS Type DSCP

Audio QoS

Audio DSCP AF11

Video QoS

Video DSCP AF11

Edit

### 7.4.3. Signaling Rules

Signaling Rules may be used to remove or block various SIP headers.

**Note** – SIP headers may be changed by the Signaling Manipulation function (see **Section 7.3.9**). However, Signaling Rules are a more efficient use of Avaya SBCE resources.

#### 7.4.3.1 Avaya - Requests

The following Signaling Rules remove SIP headers sent by Communication Manager SIP requests that are either not supported by AT&T, (History-Info,), or headers that contain internal CPE information (Alert-Info, Endpoint View, AV-Correlation-ID and P-Location).

**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 6.7.1, Step 5**).

Use the following steps to remove the **P-Location** 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: **Avaya\_SR\_with\_SM**
  - Click **Finish**
5. Highlight and edit the **Avaya\_SR\_with\_SM** 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**

Edit Header Control	
Proprietary Request Header?	<input checked="" type="checkbox"/>
Header Name	<input type="text" value="P-Location"/>
Method Name	<input type="text" value="INVITE"/>
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional
Presence Action	<input type="text" value="Remove header"/> <input type="button" value="488"/> <input type="button" value="Busy Here"/>
<input type="button" value="Finish"/>	

7. 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**.
8. Click **Finish**

9. 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**.
10. Click **Finish**

11. 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**.
12. Click **Finish**

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

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	AV-Correlation-ID	INVITE	Forbidden	Remove Header	Yes	IN
2	Alert-Info	INVITE	Forbidden	Remove Header	No	IN
3	Endpoint-View	INVITE	Forbidden	Remove Header	Yes	IN
4	P-Location	INVITE	Forbidden	Remove Header	Yes	IN

### 7.4.3.2 Avaya - Responses

The following Signaling Rules remove **P-Location** and **Endpoint-View** headers sent by Communication Manager SIP responses (e.g., 1xx and/or 200OK).

- Using the same procedures shown in **Section 7.4.3.1**, the following steps remove the **P-Location** header from **1xx** responses. Highlight the **Avaya\_SR\_with\_SM** rule created in **Section 7.4.3.1** and enter the following:
  - 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**
- Repeat **Step 1** to create a rule to remove the **P-Location** header from **200** 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.
  - From the **Header Name** menu enter **P-Location**.
  - From the **Response Code** menu select **200**.
  - From the **Method Name** menu select **Invite**.
  - For **Header Criteria** select **Forbidden**.

- From the **Presence Action** menu select **Remove Header**.
  - Click **Finish**.
3. Repeat **Step 1** to create a rule to remove the **Endpoint-View** header from **200** 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 **200**.
    - From the **Method Name** menu select **All**.
    - For **Header Criteria** select **Forbidden**.
    - From the **Presence Action** menu select **Remove Header**.
  4. Repeat **Step 3** to remove **Endpoint-View** headers from **1xx** responses.
    - From the **Response Code** menu select **1xx**.
  5. Click **Finish**

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

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	✎ ✕
2	Endpoint-View	200	ALL	Forbidden	Remove Header	Yes	IN	✎ ✕
3	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	✎ ✕
4	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN	✎ ✕

### 7.4.3.3 AT&T - Requests

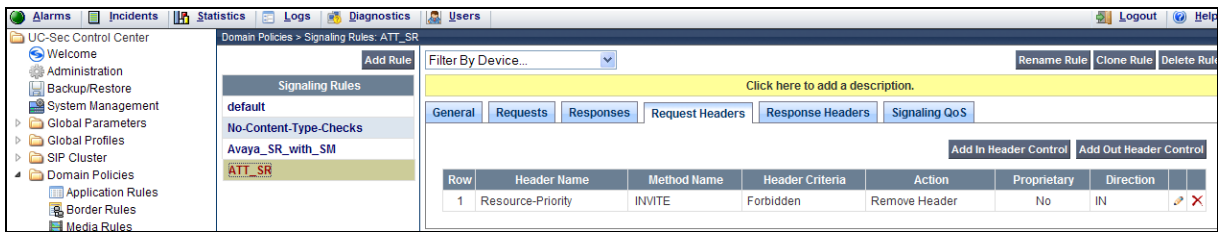
The following Signaling Rule removes the **Resource-Priority** SIP header that may be sent by the AT&T IPFR-EF service (see **Section 2.2.1, Item 10**).

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**.

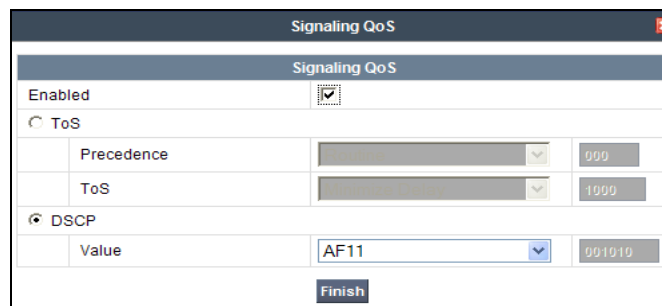


- Click **Finish**. The completed Request Headers form is shown below.  
Note that the Direction column says “IN”, and that no Response Header manipulation is required.



#### 7.4.3.4 Avaya – Signaling QoS

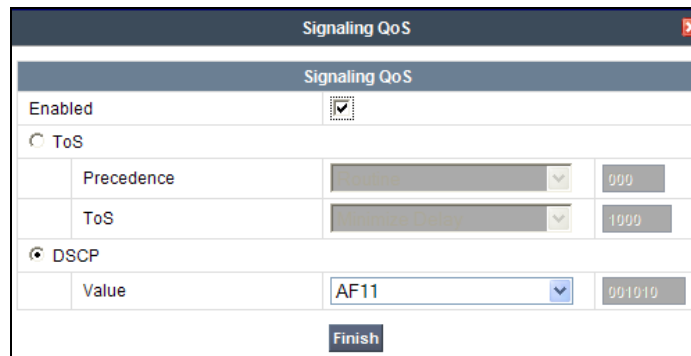
- Highlight the **Avaya\_SR\_with\_SM** rule created in **Section 7.4.3.1** and enter the following:
  - Select the **Signaling QoS** tab (not shown).
  - Click the **Edit** button and the **Signaling QoS** window will open.
  - Verify that the **Enabled** option is checked.
  - Select **DCSP**.
  - Select **Value = AF11**.
- Click **Finish**



#### 7.4.3.5 AT&T – Signaling QoS

- Highlight the **ATT\_SR** rule created in **Section 7.4.3.3** and enter the following:
  - Select the **Signaling QoS** tab (not shown).
  - Click the **Edit** button and the **Signaling QoS** window will open.
  - Verify that the **Enabled** option is checked.
  - Select **DCSP**.
  - Select **Value = AF11**.
- Click **Finish**

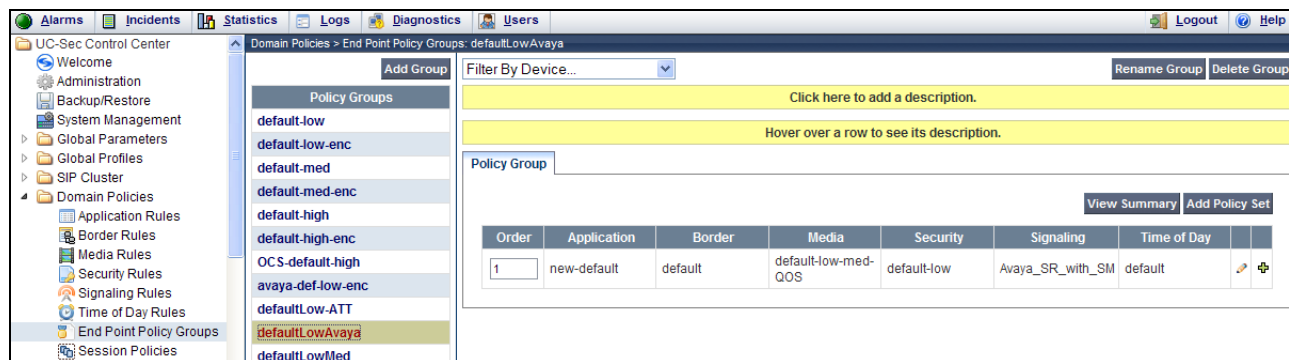




The image shows a 'Signaling QoS' configuration window. It has a title bar with the text 'Signaling QoS' and a close button. Inside, there's a section titled 'Signaling QoS' with a sub-section 'Enabled' containing a checked checkbox. Below this, there are two radio buttons: 'ToS' (selected) and 'DSCP'. Under 'ToS', there are two rows: 'Precedence' with a dropdown menu showing '000' and a text box with '000', and 'ToS' with a dropdown menu showing '1000' and a text box with '1000'. Under 'DSCP', there's a row 'Value' with a dropdown menu showing 'AF11' and a text box with '001010'. At the bottom right is a 'Finish' button.

#### 7.4.4. Endpoint Policy Groups – Avaya

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
  - a) **Name:** defaultLowAvaya
  - b) **Application Rule:** new-default
  - c) **Border Rule:** default
  - d) **Media Rule:** default-low-med-QOS
  - e) **Security Rule:** default-low
  - f) **Signaling Rule:** Avaya\_SR\_with\_SM
  - g) **Time of Day:** default
4. Select **Finish** (not shown)

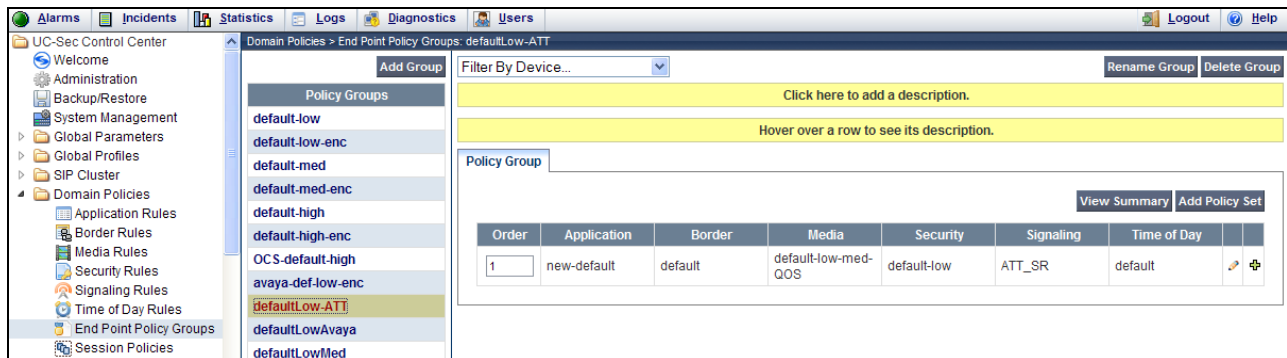


The image shows the UC-Sec Control Center interface. The left-hand menu has 'Domain Policies' expanded, showing 'End Point Policy Groups' selected. The main area shows a list of policy groups: default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, OCS-default-high, avaya-def-low-enc, defaultLow-ATT, defaultLowAvaya (highlighted), and defaultLowMed. Below the list is a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and an icon column. The table has one row with values: 1, new-default, default, default-low-med-QOS, default-low, Avaya\_SR\_with\_SM, default. Above the table are buttons for 'Add Group', 'Filter By Device...', 'Rename Group', and 'Delete Group'. Below the table are buttons for 'View Summary' and 'Add Policy Set'.

#### 7.4.5. Endpoint Policy Groups – AT&T

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
  - a. **Name:** defaultLow-ATT
  - b. **Application Rule:** new-default
  - c. **Border Rule:** default
  - d. **Media Rule:** default-low-med-QOS
  - e. **Security Rule:** default-low
  - f. **Signaling Rule:** ATT\_SR

- g. **Time of Day: default**
4. Select Finish (not shown)

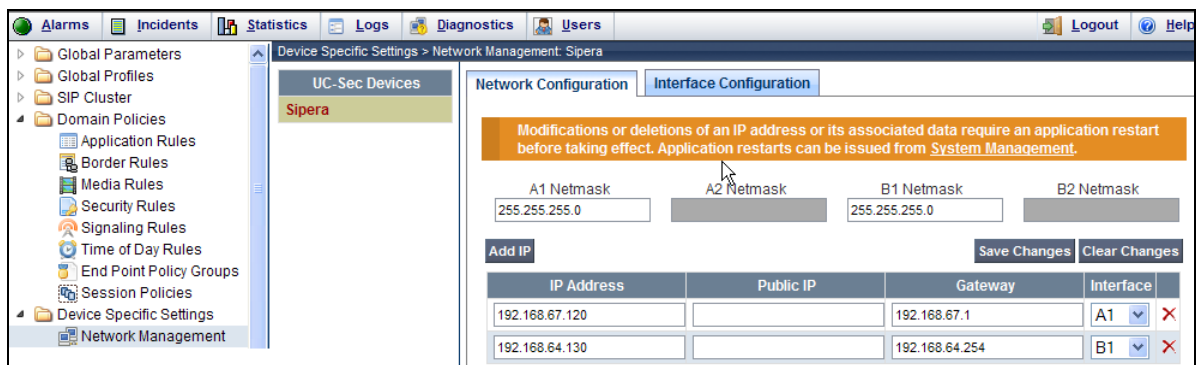


## 7.5. Device Specific Settings

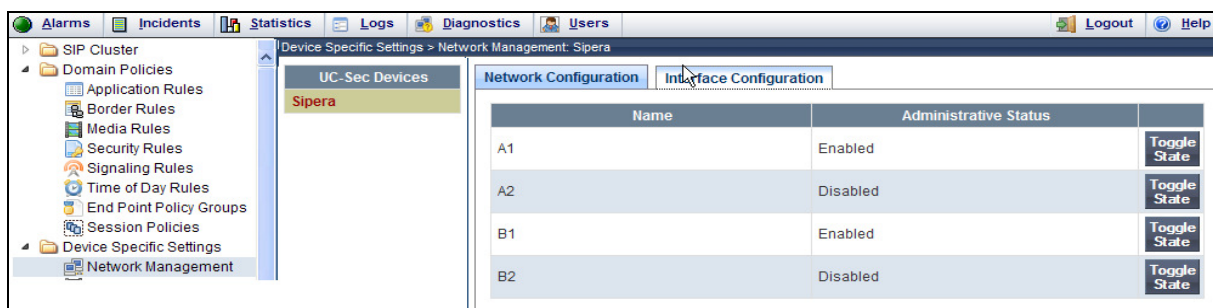
The **Device Specific Settings** configuration is used to view system information, and manage various device-specific network parameters. Specifically, it provides ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows, and Network Management.

### 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 were provisioned during installation. However if these values need to be modified, do so via this tab.



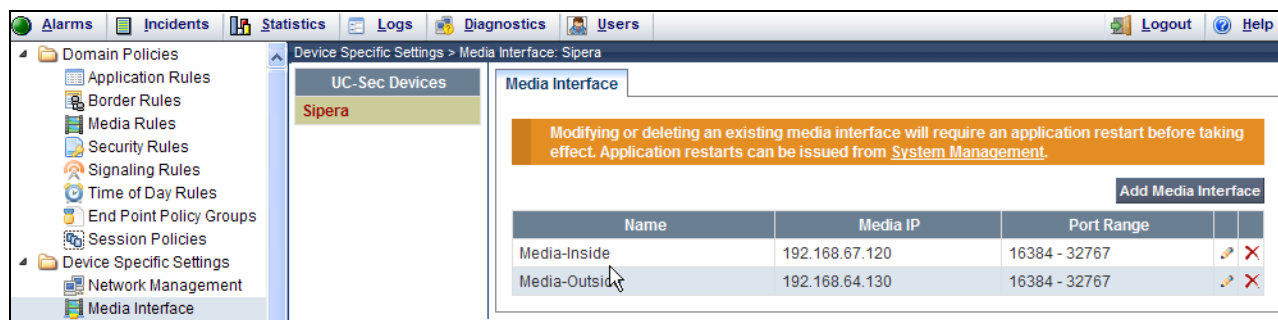
3. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration** tab.
  - a) Toggle the State of the physical interfaces being used.



## 7.5.2. Media Interfaces

AT&T requires customers to use RTP ports in the range of 16384 – 32767. Both inside and outside ports have been changed but only the outside is recommended by AT&T.

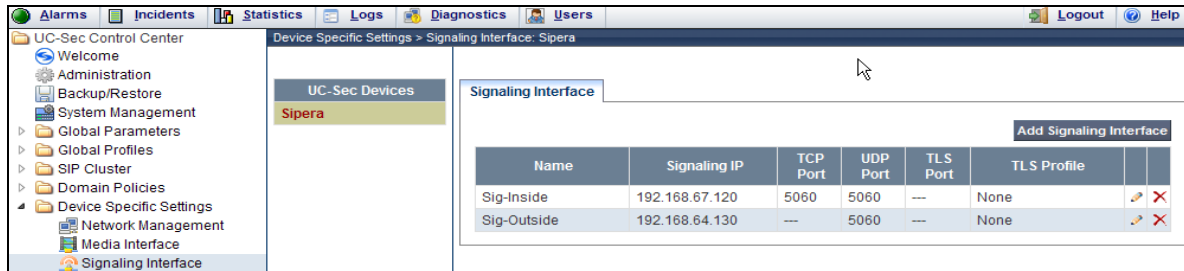
1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Media Interface**
3. Select **Add Media Interface**
  - a) **Name: Media-Inside**
  - b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Session Manager)
  - c) **Port Range: 16384 - 32767**
4. Click **Finish** (not shown)
5. Select **Add Media Interface**
  - a) **Name: Media-Outside**
  - b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
  - c) **Port Range: 16384 - 32767**
6. Click **Finish** (not shown)



## 7.5.3. Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Signaling Interface**
3. Select **Add Signaling Interface**
  - a) **Name: Sig-Inside**
  - b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Session Manager)
  - c) **TCP Port: 5060**
  - d) **UDP Port: 5060**
4. Click **Finish**

5. Select **Add Media Interface**
  - a) **Name: Sig-Outside**
  - b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
  - c) **UDP Port: 5060**
6. Click **Finish**



#### 7.5.4. Endpoint Flows – To Avaya (Session Manager)

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**, and enter the following:
  - a) **Name: Avaya**
  - b) **Server Configuration: Avaya\_SC** (Section 7.3.5)
  - c) **URI Group: \***
  - d) **Transport: \***
  - e) **Remote Subnet: \***
  - f) **Received Interface: Sig-Outside**
  - g) **Signaling Interface: Sig-Inside**
  - h) **Media Interface: Media-Inside**
  - i) **End Point Policy Group: defaultLowAvaya** (Section 7.4.4)
  - j) **Routing Profile: ATT\_Production** (Section 7.3.4)
  - k) **Topology Hiding Profile: Avaya\_TH** (Section 7.3.7)
  - l) **File Transfer Profile: None**
5. Click **Finish** (not shown)

#### 7.5.5. Endpoint Flows – To AT&T

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**, and enter the following:
  - a) **Name: ATT**
  - b) **Server Configuration: ATT** (Section 7.3.6)
  - c) **URI Group: \***
  - d) **Transport: \***
  - e) **Remote Subnet: \***
  - f) **Received Interface: Sig-Inside**

- g) **Signaling Interface: Sig-Outside**
  - h) **Media Interface: Media-Outside**
  - i) **End Point Policy Group: defaultLow-ATT (Section 7.4.5)**
  - j) **Routing Profile: To\_Avaya (Section 7.3.3)**
  - k) **Topology Hiding Profile: ATT\_TH (Section 7.3.8)**
  - l) **File Transfer Profile: None**
5. Click **Finish** (not shown)

The completed Server flow form is shown below.

The screenshot shows the 'Device Specific Settings > End Point Flows: A-SBCE' window. The 'Server Flows' tab is active, displaying two configurations:

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	ATT	*	*	*	Sig-Inside	Sig-Outside	Media-Outside	defaultLow-ATT	To_Avaya	ATT_TH	None			

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Avaya	*	*	*	Sig-Outside	Sig-Inside	Media-Inside	defaultLowAvaya	ATT_Production	Avaya_TH	None			

## 7.6. Troubleshooting Port Ranges

The default port range in this section needs to be changed to exclude the AT&T RTP port range of 16384 – 32767 (Section 7.5.2).

1. Select **Troubleshooting** from the menu on the left-hand side
2. Select **Advanced Options**
3. Select **Sipera** in the list of UC-Sec devices
4. Select the **Port Ranges** Tab
  - a) **Signaling Port Range: 12000 – 16000**
  - b) **Config Proxy Internal Signaling Port Range: 42000 – 51000** (or a range not being used)
5. Click **Save**

The screenshot shows the 'Troubleshooting > Advanced Options: Sipera' window. The 'Port Ranges' tab is active, displaying the following configuration:

Port Range Configuration	
Signaling Port Range	12000 - 16000
Config Proxy Internal Signaling Port Range	42000 - 51000
Listen Port Range	9000 - 9999
HTTP Port Range	10000 - 10200
OCS FTP Listen Port Range	6891 - 6901
OCS Alternate FTP Listen Port Range	11175 - 11185

A 'Save' button is located at the bottom right of the configuration area.

## 8. Configure Avaya Aura® Messaging

In this reference configuration, Avaya Aura® Messaging is used to verify DTMF, Message Waiting Indicator (MWI), as well as basic call coverage functionality. The administration for Avaya Aura® Messaging is beyond the scope of these Application Notes. Consult [7] for further details.

## 9. Verification Steps

The following steps may be used to verify the configuration:

### 9.1. AT&T IP Flexible Reach – Enhanced Features

1. Place inbound and outbound calls, 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.
4. Place an inbound call to an enterprise station, but do not answer the call. Verify that the call covers to Avaya Aura® Messaging voicemail. Retrieve the message from Avaya Aura® Messaging either locally or from PSTN.
5. Using the appropriate IPFR-EF access numbers and codes, verify that the following features are successful:
  - a. Network based Simultaneous Ring – The “primary” and “secondary” endpoints ring, and either may be answered.
  - b. Network based Sequential Ring (Locate Me) – Verify that after the “primary” endpoint rings for the designated time, the “secondary” endpoint rings and may be answered.
  - c. Network Based Blind Transfer (using Communication Manager vector generated REFER) – Verify that the redirection destination rings and may be answered.
  - d. Verify that the Communication Manager Call Forward feature generates Diversion Header in the forward Invite message.
  - e. 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) – Verify that based on each feature criteria, calls are successfully redirected and may be answered.

### 9.2. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See [5] 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.

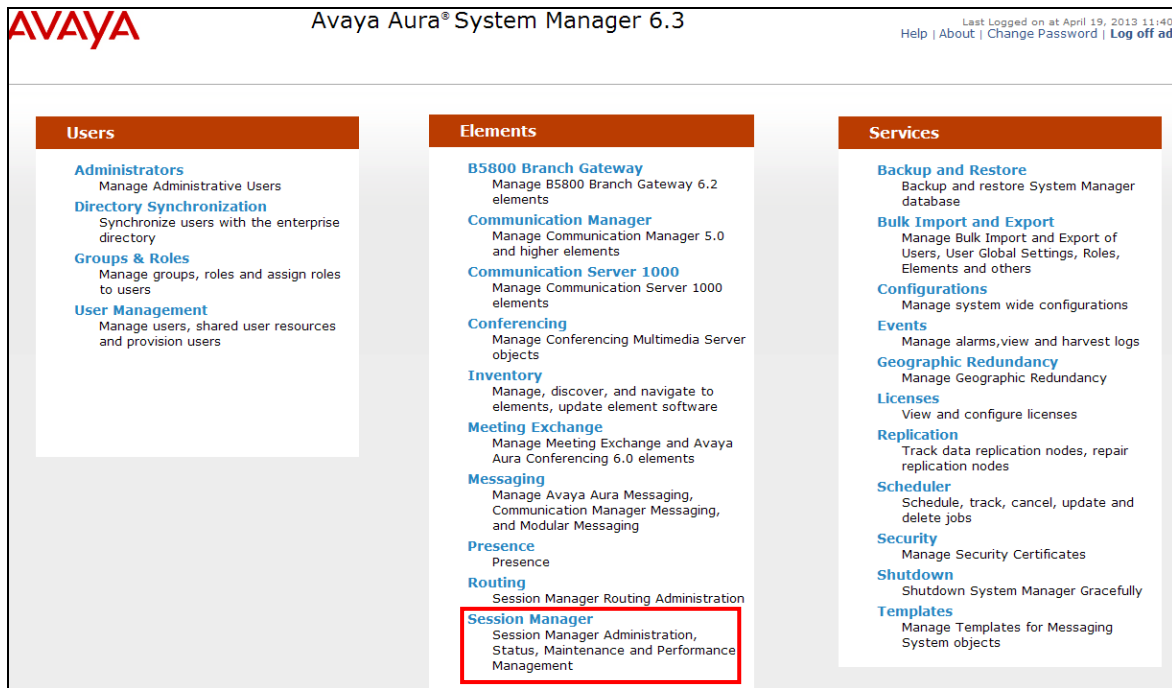
list trace tac 602		LIST TRACE		Page	1
time	data				
15:55:06	TRACE STARTED 04/19/2013 CM Release String cold-02.0.823.0-20396				
15:55:16	SIP<INVITE sip:19001@customera.com SIP/2.0				
15:55:16	Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg				
15:55:16	7ok0				
15:55:16	active trunk-group 2 member 1 cid 0x2e9				
15:55:16	SIP>SIP/2.0 180 Ringing				
15:55:16	Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg				
15:55:16	7ok0				
15:55:16	dial 19001				
15:55:16	ring station 19001 cid 0x2e9				
15:55:16	G711MU ss:off ps:20				
	rgn:1 [192.168.67.75]:18828				
	rgn:1 [192.168.67.50]:16388				
15:55:16	G729B ss:off ps:30				
	rgn:2 [192.168.67.120]:16388				
	rgn:1 [192.168.67.50]:16392				
15:55:16	xoip options: fax:T38 modem:off tty:US uid:0x5000b				
	xoip ip: [192.168.67.50]:16392				
15:55:18	SIP>SIP/2.0 200 OK				
15:55:18	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				
15:55:18	SIP>INVITE sip:192.168.67.120:5060;transport=tcp;gsid=14e31				
15:55:18	SIP<SIP/2.0 100 Trying				
15:55:18	Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg				
15:55:18	7ok0				
15:55:18	SIP<SIP/2.0 200 OK				
15:55:18	Call-ID: SDu4hje01-947fd2711d49d82d40832fa4563d2145-cgg				
15:55:18	7ok0				
15:55:18	SIP>ACK sip:192.168.67.120:5060;transport=tcp;gsid=14e31350				

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

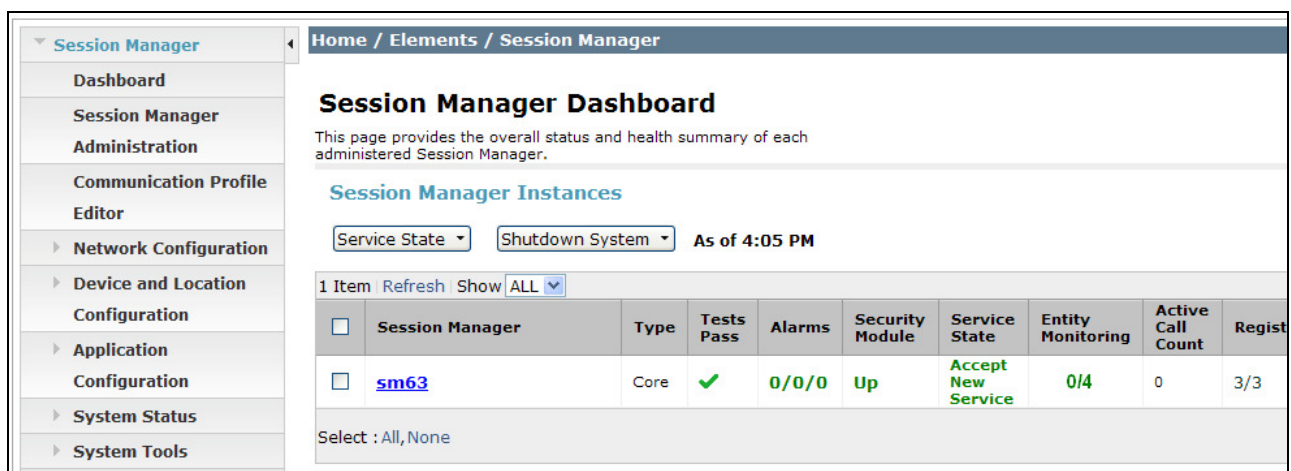
### 9.3. Avaya Aura® Session Manager

The Session Manager configuration may be verified via System Manager.

**Step 1** - Access the System Manager GUI, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. Once logged in, a **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Session Manager**.



**Step 2** – The Session Manager Dashboard is displayed. In the example below, there are no alarms and all SIP Entities are active (0/4). Click on any of these columns for further information.





For example, clicking on the **Entity Monitoring** column results in the following display:

### Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: sm63

Summary View

Status Details for the selected Session Manager:

Refresh

Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">ACM63_local</a>	192.168.67.202	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">ACM63_public</a>	192.168.67.202	5062	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">AA-M</a>	192.168.67.147	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">A-SBCE</a>	192.168.67.120	5060	TCP	FALSE	UP	405 Method Not	UP

Note the **A-SBCE** Entity, from the list of monitored entities. Under normal operating conditions, the **Link Status** should be **Up** as shown by the other displayed entities. 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 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.

### 9.3.1. Call Routing Test

The Call Routing Test verifies the routing for a particular source /destination. To run the routing test, expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. The following example shows an inbound call to Communication Manager from the IPFR-EF service. Note that the Request URI called number was 5553171 and Session Manager converts this to the Communication Manager extension 19021 before routing the call.

**Step 1 – Called Party URI field** = the information passed in the Request URI sent by the Avaya SBCE (e.g., **5553171@ customera.com**)

**Step 2 – Calling Party Address field** = the IP address of the inside interface of the Avaya SBCE (e.g., **192.168.67.120**).

**Step 3 – Calling Party URI field** = The contents of the From header (e.g., **7325551000@192.168.67.120**).

**Step 4 – Session Manager Listening Port** = **5060** and **Transport protocol** = **TCP** (see the note in **Section 5.4** regarding the use of TCP).

**Step 5 – Populate the Day of Week and Time (UTC) fields**, or let them default to current.

**Step 6 – Verify that the Called Session Manager instance** is correct (e.g., sm63).

## Step 7 - Click on **Execute Test**.

### Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

#### SIP INVITE Parameters

<b>Called Party URI</b> 5553171@ customera.com	<b>Calling Party Address</b> 192.168.67.120
<b>Calling Party URI</b> 7325551000@192.168.67.120	<b>Session Manager Listen Port</b> 5060
<b>Day Of Week</b> <b>Time (UTC)</b> Monday 12:08	<b>Transport Protocol</b> TCP
<b>Called Session Manager Instance</b> sm63	<b>Execute Test</b>

The results of the test are shown below. The ultimate routing decision is displayed under the heading **Routing Decisions**. The example shows that a PSTN call to IPFR-EF service, delivering 5553171 in the Request URI, is sent to Communication Manager extension 19021. Further down, the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated). Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 5**.

### Routing Decisions

Route < sip:19021@customera.com > to SIP Entity ACM63\_public (192.168.67.202). Terminating Location is Main.

#### Routing Decision Process

NRP Adaptations: ATT\_Production\_via\_SBCE applied.

BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.

Conference Factory Well-Known URIs: No matches for uri < 5553171@customera.com >.

Originating Location is Main. Using digits < 5553171 > and host < customera.com > for routing.

NRP Dial Patterns: No matches for digits < 5553171 > and domain < customera.com >.

NRP Dial Patterns: Found a Dial Pattern match for pattern < 555 > Min/Max length 7/7 and domain < null >.

NRP Routing Policies: Ranked destination NRP SIP Entities: ACM63\_public.

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP SIP Entities: ACM63\_public.

NRP Dial Patterns: Checking NRP Dial Patterns that specify -ALL- NRP Locations.

NRP Dial Patterns: No matches for digits < 5553171 > and domain < customera.com >.

NRP Dial Patterns: No matches for digits < 5553171 > and domain < null >.

NRP Dial Patterns: Chose route matching pattern 737

END EMERGENCY CALL CHECK: This is not an emergency call.

Adapting and proxying for SIP Entity ACM63\_public.

NRP Entity Links: Found direct link to destination. Link uses TCP to port 5062.

NRP Adaptations: ACM63\_public applied.

NRP Adaptations: P-Asserted-Identity set to < sip:7325551000@customera.com >

NRP Adaptations: Request-URI set to sip:19021@customera.com

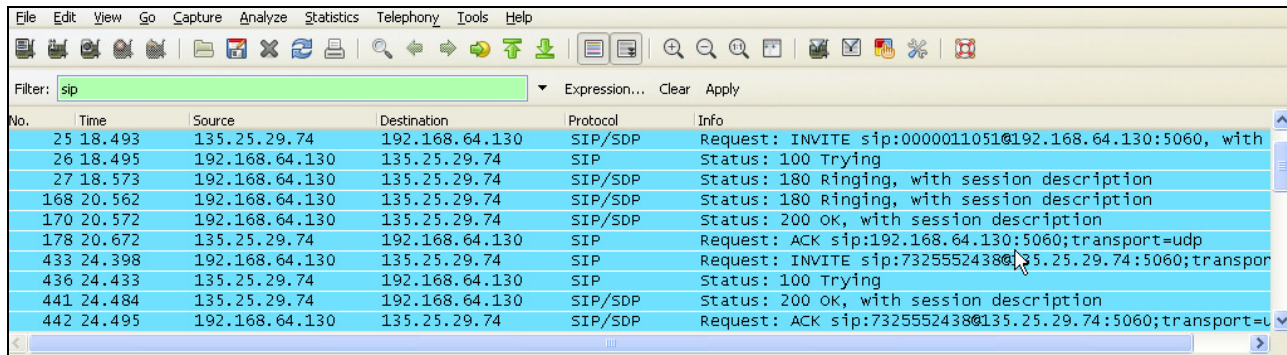
NRP Adaptations: Request URI set to sip:19021@customera.com

Route < sip:19021@customera.com > to SIP Entity ACM63\_public (192.168.67.202). Terminating Location is Main.

## 9.4. Protocol Traces

Using a SIP protocol analyzer (e.g., WireShark), monitor the SIP traffic at the Avaya SBCE public and/or private interface connections. Below are examples of traces taken in a test lab environment.

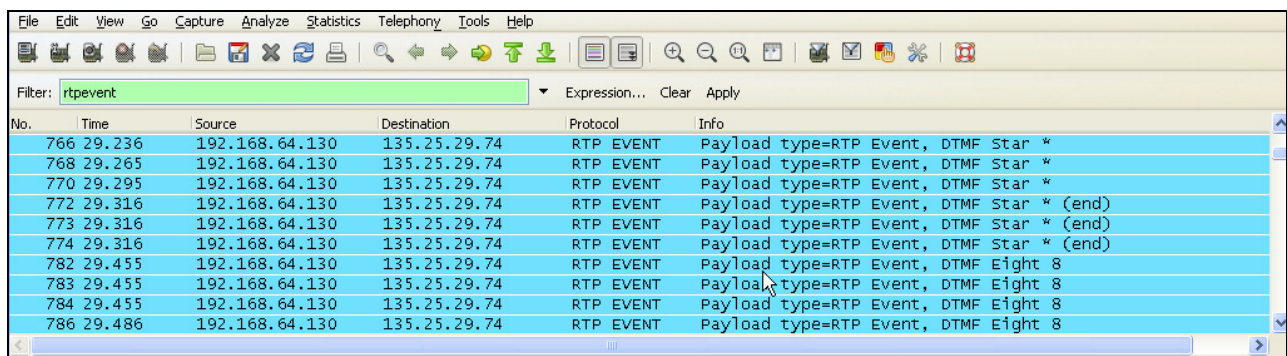
The following are examples of calls filtered on the SIP protocol.



The screenshot shows the Wireshark interface with the filter 'sip' applied. The packet list displays several SIP messages between 192.168.64.130 and 135.25.29.74. The packet details pane shows the selected packet's structure, including Request, Status, and Session Description.

No.	Time	Source	Destination	Protocol	Info
25	18.493	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:0000011051@192.168.64.130:5060, with
26	18.495	192.168.64.130	135.25.29.74	SIP	Status: 100 Trying
27	18.573	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description
168	20.562	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description
170	20.572	192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description
178	20.672	135.25.29.74	192.168.64.130	SIP	Request: ACK sip:192.168.64.130:5060;transport=udp
433	24.398	192.168.64.130	135.25.29.74	SIP	Request: INVITE sip:7325552438@135.25.29.74:5060;transport=
436	24.433	135.25.29.74	192.168.64.130	SIP	Status: 100 Trying
441	24.484	135.25.29.74	192.168.64.130	SIP/SDP	Status: 200 OK, with session description
442	24.495	192.168.64.130	135.25.29.74	SIP/SDP	Request: ACK sip:7325552438@135.25.29.74:5060;transport=u

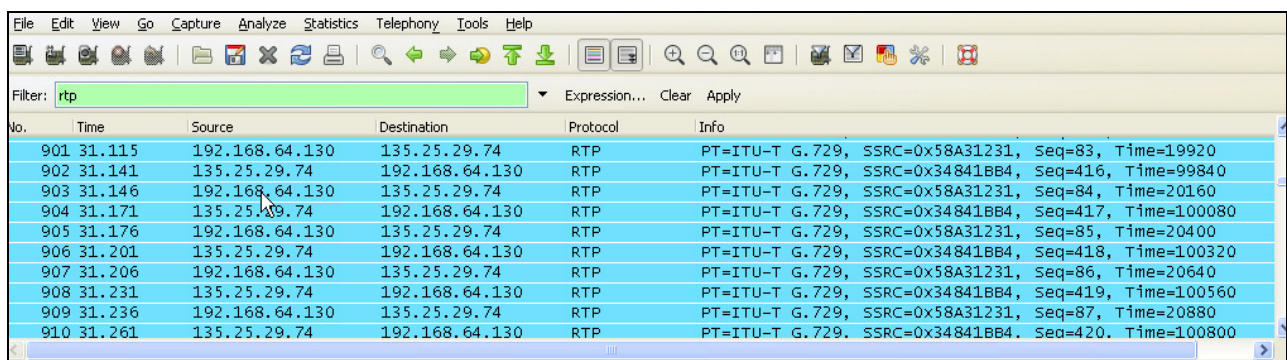
The following is an example of a call filtered on DTMF.



The screenshot shows the Wireshark interface with the filter 'rtpevent' applied. The packet list displays RTP events between 192.168.64.130 and 135.25.29.74. The packet details pane shows the selected packet's structure, including Payload type and DTMF Star \*.

No.	Time	Source	Destination	Protocol	Info
766	29.236	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star *
768	29.265	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star *
770	29.295	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star *
772	29.316	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star * (end)
773	29.316	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star * (end)
774	29.316	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Star * (end)
782	29.455	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8
783	29.455	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8
784	29.455	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8
786	29.486	192.168.64.130	135.25.29.74	RTP EVENT	Payload type=RTP Event, DTMF Eight 8

The following is an example of a call filtered on RTP.



The screenshot shows the Wireshark interface with the filter 'rtp' applied. The packet list displays RTP packets between 192.168.64.130 and 135.25.29.74. The packet details pane shows the selected packet's structure, including PT=ITU-T G.729, SSRC=0x58A31231, Seq=83, Time=19920.

No.	Time	Source	Destination	Protocol	Info
901	31.115	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=83, Time=19920
902	31.141	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=416, Time=99840
903	31.146	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=84, Time=20160
904	31.171	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=417, Time=100080
905	31.176	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=85, Time=20400
906	31.201	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=418, Time=100320
907	31.206	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=86, Time=20640
908	31.231	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=419, Time=100560
909	31.236	192.168.64.130	135.25.29.74	RTP	PT=ITU-T G.729, SSRC=0x58A31231, Seq=87, Time=20880
910	31.261	135.25.29.74	192.168.64.130	RTP	PT=ITU-T G.729, SSRC=0x34841BB4, Seq=420, Time=100800

After receiving the initial *Invite* in frame 20, the Communication Manager Vector generated the *Refer* sent in frame 115. Note the *Refer-To* header highlighted below. This contains the redirect destination (17325552438) specified in the Communication Manager Vector.

No.	Time	Source	Destination	Protocol	Info
20	23.074	135.25.29.74	192.168.64.130	SIP/SDP	Request: INVITE sip:7325554037@192.168.64.130:5060, with
21	23.076	192.168.64.130	135.25.29.74	SIP	Status: 100 Trying
22	23.153	192.168.64.130	135.25.29.74	SIP/SDP	Status: 180 Ringing, with session description
23	23.156	192.168.64.130	135.25.29.74	SIP/SDP	Status: 200 OK, with session description
31	23.318	135.25.29.74	192.168.64.130	SIP	Request: ACK sip:44010@192.168.64.130:5060;transport=udp
115	24.843	192.168.64.130	135.25.29.74	SIP	Request: REFER sip:135.25.29.74:5060, in-dialog
119	24.883	135.25.29.74	192.168.64.130	SIP	Status: 202 Accepted
120	24.886	135.25.29.74	192.168.64.130	SIP	Request: BYE sip:44010@192.168.64.130:5060
121	24.896	192.168.64.130	135.25.29.74	SIP	Status: 200 OK

Frame 115: 673 bytes on wire (5384 bits), 673 bytes captured (5384 bits)

- Ethernet II, Src: IntelCor\_c9:53:f9 (00:1b:21:c9:53:f9), Dst: Cisco\_01:c5:a1 (00:22:55:01:c5:a1)
- Internet Protocol, Src: 192.168.64.130 (192.168.64.130), Dst: 135.25.29.74 (135.25.29.74)
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol
  - Request-Line: REFER sip:135.25.29.74:5060 SIP/2.0
  - Message Header
    - From: "User 7325554037" <sip:7325554037@192.168.64.130;user=phone>;tag=80ee188cfcd7e11bf574fec324500
    - To: <sip:7325551000@135.25.29.74;user=phone>;tag=1543067091-1342552043577-
    - CSeq: 1 REFER
    - Call-ID: Bw190723577170712606096938@invisibleA51
    - Contact: "REFER" <sip:44010@192.168.64.130:5060>
    - Record-Route: <sip:192.168.64.130:5060;ipcs-line=10402;lr;transport=udp>
    - User-Agent: Avaya CM/R016x.02.0.823.0 AVAYA-SM-6.2.1.0.621010
    - Max-Forwards: 66
    - Via: SIP/2.0/UDP 192.168.64.130:5060;branch=z9hG4bK-s1632-001551037370-1--s1632-Refer-To: <sip:17325552438@135.25.29.74>
    - Content-Length: 0

No.	Time	Source	Destination	Protocol	Info
9	6.776	135.25.29.74	192.168.64.130	SIP	Request: OPTIONS sip:192.168.64.130:5060
10	6.781	192.168.64.130	135.25.29.74	SIP	Status: 200 OK
29	23.276	192.168.64.130	135.25.29.74	SIP	Request: OPTIONS sip:135.25.29.74;transport=udp
30	23.304	135.25.29.74	192.168.64.130	SIP	Status: 405 Method Not Allowed

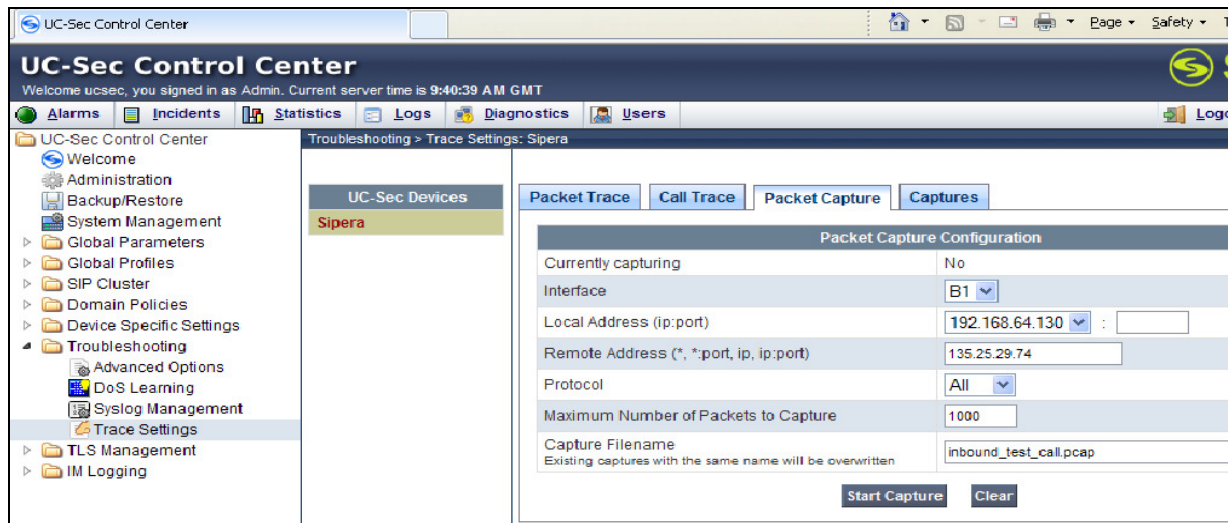


Avaya Session Border Controller for Enterprise Verification  
The Avaya SBCE can take internal traces of specified interfaces.

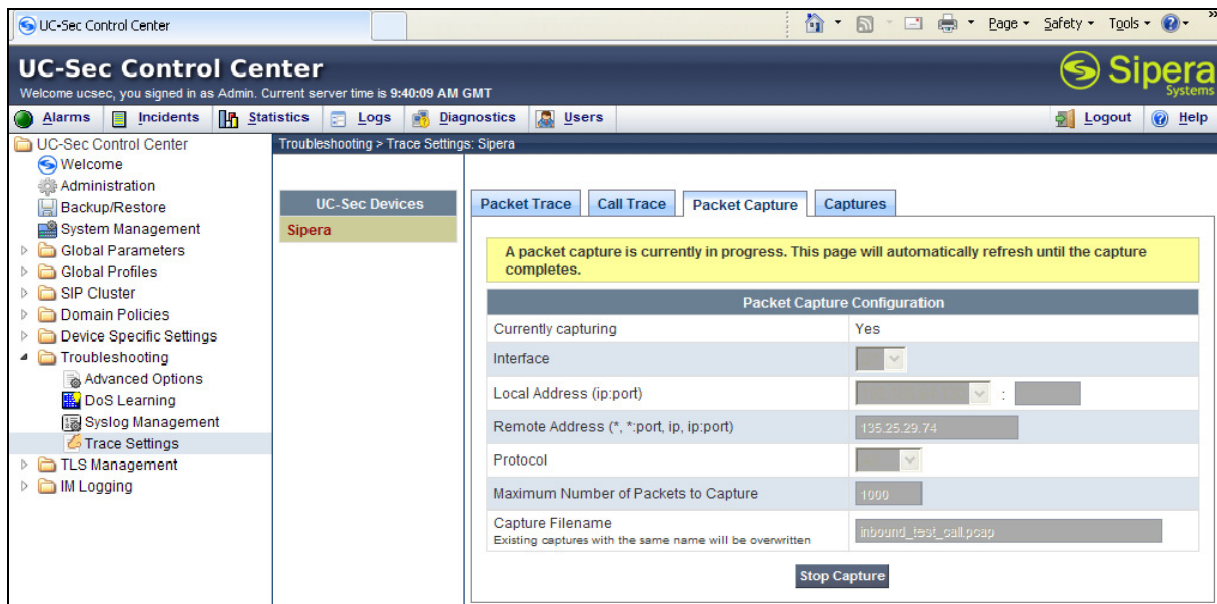
**Step 1** - Navigate to UC-Sec Control Centre → Troubleshooting → Trace Settings

**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:

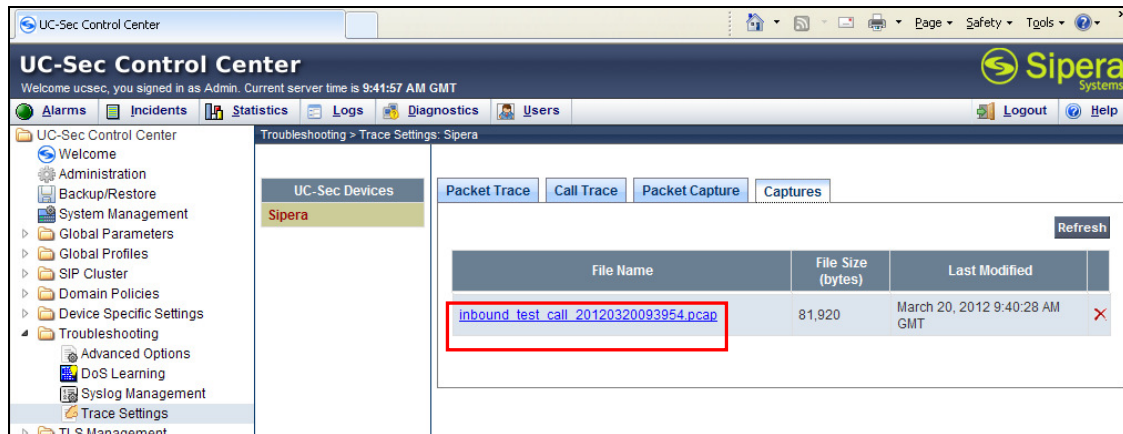


**Step 3** – Run the test.

**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.



## 10. 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) 4.0.5, 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**.

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

## 11. 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, December, 2012
2. *Implementing Avaya Aura® Session Manager*, Release 6.3, March, 2013
3. *Implementing Avaya Aura® System Manager*, Release 6.3, Issue 1, December, 2012
4. *Administering Avaya Aura® System Manager*, Release 6.3, Issue 1.0, December, 2012

### Avaya Aura® Communication Manager

5. *Administering Avaya Aura® Communication Manager*, Release 6.3 03-300509, Issue 8, May 2013
6. *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

### Avaya Aura® Messaging

7. *Administering Avaya Aura® Messaging*, Release 6.2, Issue 2.1, February, 2013

### Avaya Session Border Controller for Enterprise

Product documentation for UC-Sec version 4.0.5, can be obtained from Sipera using the link at <http://www.sipera.com>

8. *E-SBC IU Installation Guide*, Release 4.0.5, Part Number: 101-5225-405v1.00, Release Date: November 2011
9. *E-SBC Administration Guide*, Release 4.0.5, Part Number: 010-5424-405v1.00, Release Date: November 2011

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

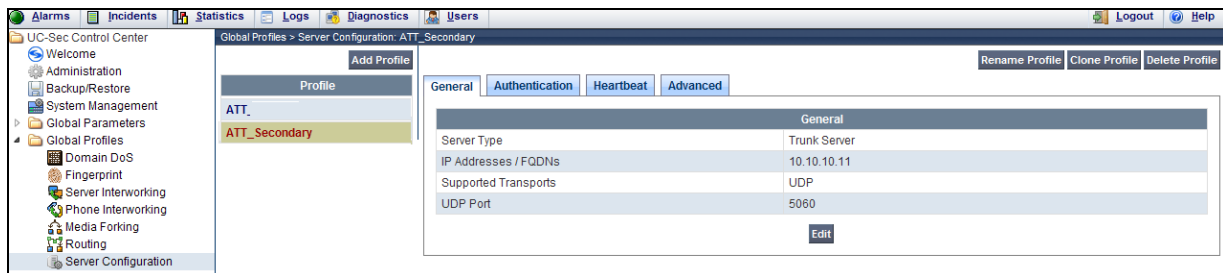
10. AT&T IP Flexible Reach - Enhanced Features Service description - <http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-flexible-reach-enterprise/>

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

AT&T 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 **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 7.3.6**).

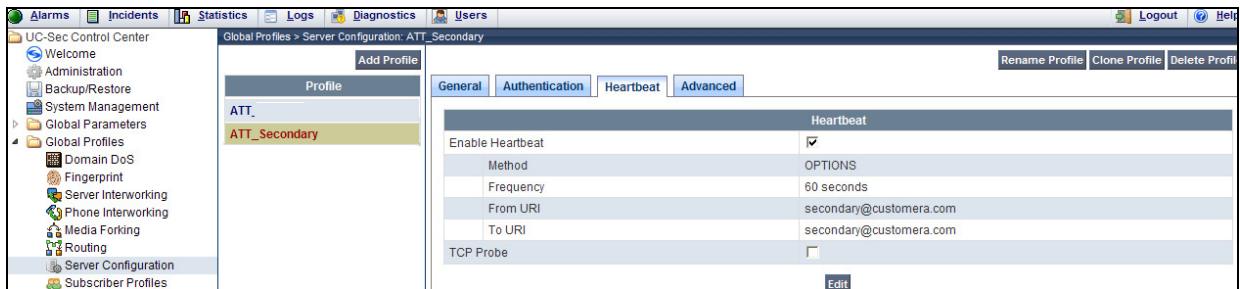
### 12.1. Step 1: Configure the Secondary Location in Server Configuration

1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Server Configuration**
3. Select **Add Profile**
  - a) **Name:** **ATT\_Secondary**
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.

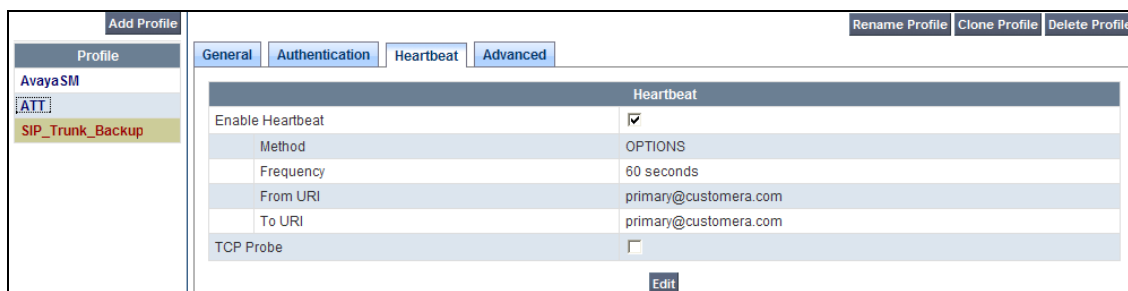


5. On the **Authentication** tab:
  - a) Select **Next** (not shown)
6. On the **Heartbeat** tab:
  - a) Check **Enable Heartbeat**
  - b) **Method:** **OPTIONS**
  - c) **Frequency:** As desired (e.g., 60 seconds).
  - d) **From URI:** **secondary@customer.com**
  - e) **To URI:** **secondary@customer.com**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



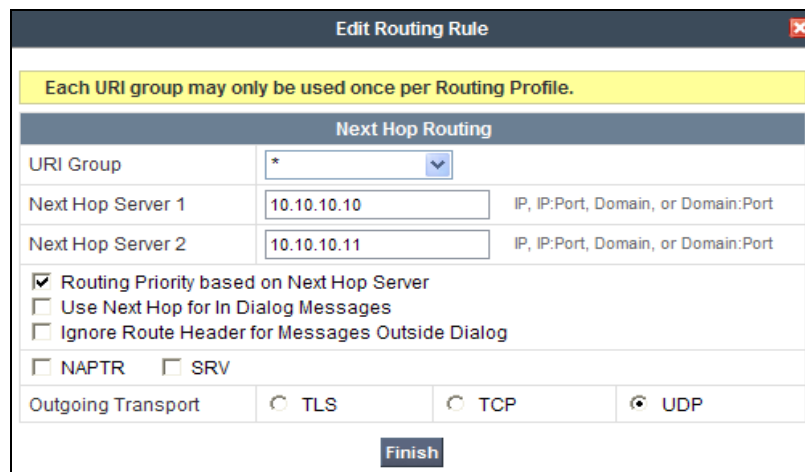


8. Select the Server Configuration created in **Section 7.3.6** (e.g., **ATT**)
9. Select the **Heartbeat Tab**
10. Select **Edit**
11. Repeat **Steps 6 – 7**, but with information for the Primary Trunk as shown below.



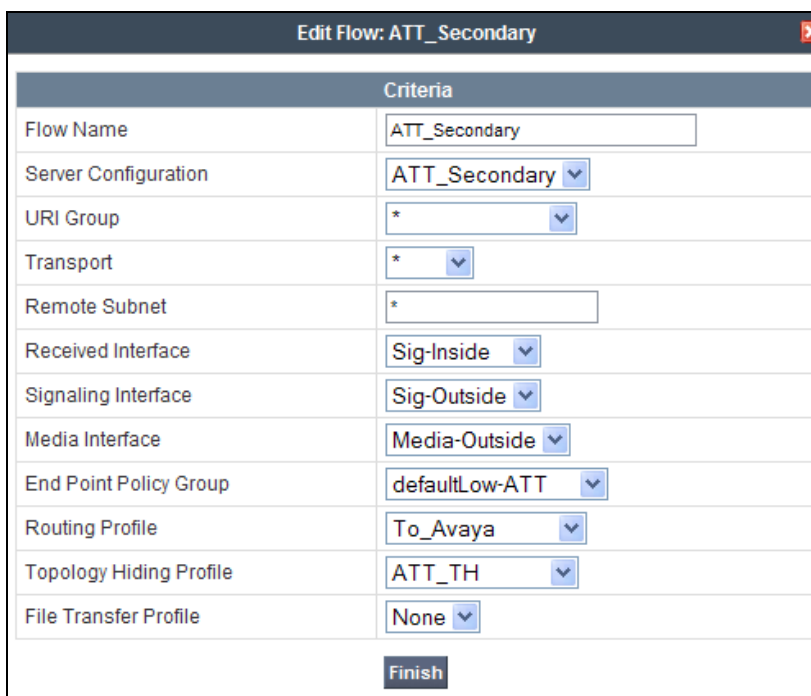
## 12.2. Step 2: Add Secondary IP Address to Routing

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** )
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**



## 12.3. Step 3: Configure End Point Flows – 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
  - c) **URI Group:** \*
  - d) **Transport:** \*
  - e) **Remote Subnet:** \*
  - f) **Received Interface:** Sig-Inside
  - g) **Signaling Interface:** Sig-Outside
  - h) **Media Interface:** Media-Outside
  - i) **End Point Policy Group:** defaultLow-ATT (Section 7.4.5)
  - j) **Routing Profile:** To\_Avaya (Section 7.3.3)
  - k) **Topology Hiding Profile:** ATT\_TH (Section 7.3.8)
  - l) **File Transfer Profile:** None
5. Click **Finish**



Criteria	
Flow Name	ATT_Secondary
Server Configuration	ATT_Secondary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig-Inside
Signaling Interface	Sig-Outside
Media Interface	Media-Outside
End Point Policy Group	defaultLow-ATT
Routing Profile	To_Avaya
Topology Hiding Profile	ATT_TH
File Transfer Profile	None

Finish

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

## 13. Addendum 2 – Dedicated SIP Trunk for Blind Transfer (Refer Call Redirection) AT&T IP Flexible Reach - Enhanced Feature

As described in **Section 2.2.1**, an issue was found with the use of Communication Manager Network Call Redirection (NCR) Refer processing for call redirection (IPFR-EF blind transfer feature). If NCR is enabled on the Communication Manager SIP trunk to AT&T, issues may occur with attended or unattended transfers initiated by Communication Manager stations. In addition, issues with Music on Hold and Meet-Me conferences were also observed.

A workaround for these issues is to provision a dedicated SIP trunk, with NCR enabled, used only for the Refer based IPFR-EF “Blind Transfer” feature. The provisioning for this feature is performed on the Avaya SBCE, Session Manager, and on Communication Manager. Note that specific AT&T IP Flexible Reach - Enhanced Features service DNIS number(s) must be defined as the dedicated IPFR-EF blind transfer feature access number(s), and routed exclusively to this trunk.

### 13.1. Configure Avaya Session Border Controller for Enterprise

#### 13.1.1. Create URI Group

**Step 1** – Navigate to **Global Profiles** → **URI Groups** and click on **Add Group** (not shown).

- Enter a URI Group name (e.g. **NCR**) and click the **Next** button, The **Edit URI** window will open. Enter the following:
  - For **URI Type** select **Regular Expression**
  - In the **URI** field enter **xxxxxxx@.\*** where **xxxxxxx** is the inbound AT&T IP Flexible Reach - Enhanced Features service DNIS number selected for IPFR-EF blind transfer feature access (e.g., **5553180@.\***)
  - Click on **Finish**.

Edit URI	
<b>WARNING:</b> Invalid or incorrectly entered regular expressions may cause unexpected results.	
Note: This regular expression is case-insensitive.	
Ex: [0-9]{3,5}\.user@domain\.com, (simple advanced)\.user[A-Z]{3}@.*	
URI Type	<input type="radio"/> Plain <input type="radio"/> Dial Plan <input checked="" type="radio"/> Regular Expression
URI	<input type="text" value="5553180@.*"/>
<b>Finish</b>	

### 13.1.2. Routing

**Step 1** – Navigate to **Global Profiles → Routing**, and select the Routing Profile created in **Section 7.3.3** (e.g., **To\_Avaya**).

**Step 2** – Click on the **Add Routing Rule** button and enter the following:

- In the **URI Group** menu select the URI Group name created in **Section 13.1.1** above (e.g., **NCR**).
- In the **Next Hop Server 1** field enter **192.168.67.47:5080**. This is the IP address and port defined in Session Manager for NCR specific traffic in **Section 13.2.3**.
- Leave the **Routing Priority Based on Next Hop Server** and **TCP** options checked (default).
- Click on **Finish**.

Each URI group may only be used once per Routing Profile.

**Next Hop Routing**

URI Group: NCR

Next Hop Server 1: 192.168.67.47:5080 IP, IP:Port, Domain, or Domain:Port

Next Hop Server 2: IP, IP:Port, Domain, or Domain:Port

☒ Routing Priority based on Next Hop Server

☐ Use Next Hop for In Dialog Messages

☐ Ignore Route Header for Messages Outside Dialog

☐ NAPTR ☐ SRV

Outgoing Transport: ☐ TLS ☒ TCP ☐ UDP

Finish

**Step 3** – In the completed Routing Profile table, enter the following:

- In the **Priority** column change the original URI Group “\*” from **1** to **2**
- In the **Priority** column change the new URI Group “NCR” from **2** to **1**
- Click on the **Update Order** button, and the NCR group will be placed first.

Global Profiles > Routing: To\_Avaya

Routing Profile

Click here to add a description.

Update Order

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	NCR	192.168.67.47:5080	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP
2	*	192.168.67.47	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

Add Routing Rule

Therefore, if the Request URI digit string on an inbound call matches the defined string in the “NCR” URI Group (5553180), the Avaya SBCE will send the call to the Session Manager IP address using port 5080, defined in **Section 13.2.3**. If there is no match, then the “\*” URI Group is

used and the call is sent to the Session Manager IP address using port 5062, as defined in **Section 5.5.1**).

## 13.2. Configure Avaya Aura® Session Manager

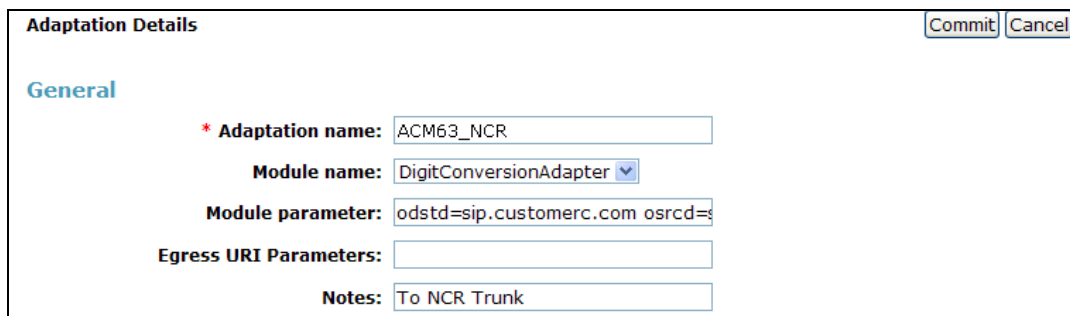
### 13.2.1. Adaptation for NCR Trunk

Following the procedures shown in **Section 5.3.1**, add a new Adaptation for Communication Manager (e.g., **ACM63\_NCR**).

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

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

- A descriptive **Name**, (e.g., **ACM63\_NCR**).
- Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select **<click to add module>** and enter **DigitConversionAdapter**).
- In the **Module parameter** field enter **odstd= customera.com osrcd= customera.com**.
- Enter any desired notes.



The screenshot shows the 'Adaptation Details' form with the 'General' tab selected. The form contains the following fields:

- Adaptation name:** ACM63\_NCR
- Module name:** DigitConversionAdapter (selected from a dropdown menu)
- Module parameter:** odstd=sip.customerc.com osrcd=
- Egress URI Parameters:** (empty field)
- Notes:** To NCR Trunk

Buttons for 'Commit' and 'Cancel' are located in the top right corner.

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

- Enter an AT&T DNIS number chosen specifically for access to the NCR enabled trunk in the **Matching Pattern** column (e.g., **5553180**).
- Enter **7** in the **Min/Max** columns.
- Enter **7** in the **Delete Digits** column.
- Enter **44010** in the **Insert Digits** column. Note that this is the extension of the Vector Directory Number (VDN) defined in **Section 13.3.2**.
- 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 defined for NCR trunk/Refer vector access.

**Step 5** - Click on **Commit** (not shown).

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

Digit Conversion for Incoming Calls to SM
Add Remove
0 Items Refresh
Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes

Digit Conversion for Outgoing Calls from SM
Add Remove
1 Item Refresh
Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*5553180	*7	*7		*7	44010	destination		NCR trunk - IPFR REFER

Select : All, None

Commit Cancel

### 13.2.2. SIP Entity for NCR Trunk

Following the procedures shown in **Section 5.4.2**, enter the following:

**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\_NCR**).
- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.3** (e.g. **192.168.67.202**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation administered in **Section 13.2.1**.
- **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 **Use Session Manager Configuration for SIP Link Monitoring** field.
  - Use the default values for the remaining parameters.

**Step 3** - Click on **Commit**.

**Note** – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Link is defined in **Section 13.2.3**.

**SIP Entity Details** Commit Cancel

**General**

\* **Name:**

\* **FQDN or IP Address:**

**Type:**

**Notes:**

**Adaptation:**

**Location:**

**Time Zone:**

**Override Port & Transport with DNS SRV:** ☐

\* **SIP Timer B/F (in seconds):**

**Credential name:**

**Call Detail Recording:**

**SIP Link Monitoring**

**SIP Link Monitoring:**

**Supports Call Admission Control:** ☐

**Shared Bandwidth Manager:** ☐

**Primary Session Manager Bandwidth Association:**

**Backup Session Manager Bandwidth Association:**

### 13.2.3. Entity Link for NCR Trunk

Following the procedures shown in **Section 5.5.1**, enter the following:

**Step 1** - In the left pane under **Routing**, click on **Entity Links**. In the **Entity Links** page, 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 the Communication Manager NCR trunk (e.g., **ACM63\_NCR**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager. SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter **5080**.
- **Protocol** – Select **TCP**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 13.2.2** for the Communication Manager NCR trunk.
- **SIP Entity 2 Port** - Enter **5080**.
- **Connection Policy** – Select **Trusted**.
- Enter any desired notes.

**Step 3** - Click on **Commit**.

Entity Links <span>Commit</span> <span>Cancel</span>								
1 Item <a href="#">Refresh</a> <span>Filter: Enable</span>								
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* <input type="text" value="ACM63_NCR"/>	* <input type="text" value="sm63"/>	<input type="text" value="TCP"/>	* <input type="text" value="5080"/>	* <input type="text" value="ACM63_NCR"/>	* <input type="text" value="5080"/>	<input type="text" value="Trusted"/>	<input type="checkbox"/>	<input type="text"/>

### 13.2.4. Routing Policy for NCR Trunk

Following the procedures shown in **Section 5.7.1**, enter the following:

- 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 (not shown), enter a descriptive **Name** for routing AT&T calls to the Communication Manager NCR trunk (e.g., **ACM63\_NCR**), 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 (not shown), click on **Select** and the SIP Entity list page will open.
- Step 4** - In the **SIP Entity List** page (not shown), select the SIP Entity administered in **Section 13.2.2** for the NCR trunk (**ACM63\_NCR**), and click on **Select**.
- Step 5** - Returning to the **Routing Policy Details** page in the **Time of Day** section (not shown), 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 13.2.5**) 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**.

The screenshot displays the 'Routing Policy Details' form. At the top right are 'Commit' and 'Cancel' buttons. The 'General' section includes fields for 'Name' (ACM63\_NCR), 'Disabled' (unchecked), 'Retries' (0), and 'Notes' (IPFR Call Forward with Refer). The 'SIP Entity as Destination' section has a 'Select' button. Below it is a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one entry: ACM63\_NCR, 192.168.67.202, CM, NCR trunk. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons. Below these is a table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The table shows one item with Ranking 0, Name 24/7, and Start/End times 00:00 and 23:59. A 'Filter: Enable' link is at the top right of the table. At the bottom is a 'Select : All, None' dropdown.

Name	FQDN or IP Address	Type	Notes
ACM63_NCR	192.168.67.202	CM	NCR trunk

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	Time Range 24/7



### 13.2.5. Dial Pattern for NCR Trunk

Following the procedures shown in **Section 5.8.1**, enter the following:

**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 (not shown), provision the following:

- **Pattern** – Enter the AT&T DNIS number specified in **Section 13.1.1** for access to the NCR enabled trunk (e.g., **5553180**).
- **Min and Max** – Enter **7**.
- **SIP Domain** – Select the SIP Domain defined in **Section 5.1** or **-ALL-**, to select all of the administered SIP Domains.

**Step 3** - In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on **Add**.

**Step 4** - In the **Originating Location** section of the **Originating Locations and Routing Policies** page (not shown), check the checkbox corresponding to the Location **Main** see **Section 5.2.1**).

**Step 5** - In the **Routing Policies** section (not shown), check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager NCR trunk in **Section 13.2.4** (e.g., **ACM63\_NCR**).

**Step 6** - In the **Originating Location** page (not shown), 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 required for access to the NCR trunk.

**Dial Pattern Details** [Commit] [Cancel]

**General**

\* Pattern: 5553180

\* Min: 7

\* Max: 7

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: IPFR with Refer

**Originating Locations and Routing Policies**

[Add] [Remove]

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name <sup>1</sup> ▲	Originating Location Notes	Routing Policy Name	Rank <sup>2</sup> ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		ACM63_NCR	0	<input type="checkbox"/>	ACM63_NCR	NCR trunk

Select : All, None

**Denied Originating Locations**

[Add] [Remove]

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

## 13.3. Configure Communication Manager

### 13.3.1. SIP Trunk for NCR calls

This section describes the steps for administering the NCR enabled SIP trunk used for IPFR-EF calls utilizing the “Blind Transfer” feature. This trunk corresponds to the **ACM63\_NCR** Entity Link defined in **Section 13.2.3**.

**Step 1** - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **5**), and provision the following:

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp** (see the note at the beginning of **Section 6.7.1**).
- 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 6.3**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g., **SM63**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5080** (see **Section 13.2.3**).
- **Far-end Network Region** – Set the IP network region to **2**, as set in **Section 6.5.2**.
- **Far-end Domain** – Enter **customerera.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.

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	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		
	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, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **NCR\_Trunk**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **605**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group administered in **Step 1** (e.g., **5**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

<b>add trunk-group 5</b>		<b>Page 1 of 21</b>	
TRUNK GROUP			
Group Number: 5	<b>Group Type: sip</b>	CDR Reports: y	
<b>Group Name: NCR_Trunk</b>	COR: 1	TN: 1	<b>TAC: 605</b>
<b>Direction: two-way</b>	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
<b>Service Type: public-ntwrk</b>	Auth Code? n		
		Member Assignment Method: auto	
		<b>Signaling Group: 5</b>	
		<b>Number of Members: 10</b>	

**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 header pertaining to active call session refresh.

<b>add trunk-group 5</b>		<b>Page 2 of 21</b>	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto	Redirect On OPTIM Failure: 6000		
SCCAN? n	Digital Loss Group: 18		
<b>Preferred Minimum Session Refresh Interval(sec): 900</b>			
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 **Numbering Format:** to **private** (see Note in Section 6.7.1, Step 4).

<b>add trunk-group 5</b>		<b>Page 3 of 21</b>	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
<b>Numbering Format: private</b>			
UII 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:**

- Set **Network Call Redirection** to **y**. This enables the use of Refer.
- Set **Send Diversion Header** to **y**.
- Set **Telephone Event Payload Type** to the RTP payload type required by the IPFR-EF service (e.g., **100**).

<b>add trunk-group 5</b>	<b>Page 4 of 21</b>
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
<b>Network Call Redirection? y</b>	
Build Refer-To URI of REFER From Contact For NCR? n	
<b>Send Diversion Header? y</b>	
Support Request History? y	
<b>Telephone Event Payload Type: 100</b>	
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	

### 13.3.2. Communication Manager Vector (Refer Generation)

The Refer used by the IPFR-EF “Blind Transfer” feature is generated by a Communication Manager Vector Directory Number (VDN), and an associated Vector.

**Note** – The programming of vectors and the creation of system announcements is beyond the scope of this document. The vector example shown below was used in the reference configuration.

**Step 1** – Create the Vector by entering the **change vector x** command, where x is an available vector number (e.g., **37**). In the example vector below:

- Line **02** plays a previously recorded announcement **42008** (“Your call is being redirected”).
- Line **04** generates the Refer to the new destination number **17325552468**.

<b>change vector 37</b>	<b>Page 1 of 6</b>
CALL VECTOR	
Number: 37 <b>Name: Refer</b>	
Multimedia? n	Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y	EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y	LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y	3.0 Enhanced? y
01 #      Answer call immediately with announcement then NCR REFER	
<b>02 announcement 42008</b>	
03 #      Refer occurs since this is post answer	
<b>04 route-to      number ~r17325552468      with cov n if unconditionally</b>	

**Step 2** – Create the VDN.

- Enter the **add vdn x** command, where x is the extension defined in **Section 13.2.1, Step 3** (e.g., **44010**)
- In the **Name** field enter a descriptive name.
- In the **Destination** field enter **Vector Number** and the number of the vector provisioned in **Step 1** (e.g., **37**).

<b>add vdn 44010</b>	<b>Page 1 of 3</b>
VECTOR DIRECTORY NUMBER	
<b>Extension: 44010</b>	
<b>Name*: IPFR-EF_REFER</b>	
<b>Destination: Vector Number</b>	<b>37</b>
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: none	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	

**Step 3** – Enter the command **save translation** to save the Communication Manager provisioning.

---

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>TM</sup> and <sup>®</sup> are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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](mailto:devconnect@avaya.com).