



Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise with AT&T IP Flexible Reach - Enhanced Features – Issue 1.3

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 6.2 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.2 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 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 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	8
3.	Reference Configuration.....	8
3.1.	Illustrative Configuration Information	10
3.2.	AT&T IP Flexible Reach - Enhanced Features Service Call Flows	10
3.2.1.	Inbound	10
3.2.2.	Outbound.....	11
3.2.3.	Call Forward Re-direction	12
3.2.4.	Coverage to Voicemail	13
3.3.	AT&T IP Flexible Reach - Enhanced Features – Network Based Blind Transfer Using Refer (Communication Manager Vector) Call Flow	14
4.	Equipment and Software Validated	15
5.	Configure Avaya Aura® Session Manager Release 6.2.....	16
5.1.	SIP Domain	17
5.2.	Locations	18
5.2.1.	Location for CPE Equipment.....	18
5.3.	Configure Adaptations	19
5.3.1.	Adaptation for calls to Avaya Aura® Communication Manager	20
5.3.2.	Adaptation for calls to the AT&T IP Flexible Reach – Enhanced Features Service..	21
5.3.3.	Adaptation for calls to Avaya Aura® Messaging.....	22
5.4.	SIP Entities.....	23
5.4.1.	Avaya Aura® Session Manager SIP Entity	24
5.4.2.	Avaya Aura® Communication Manager SIP Entity - Public	25
5.4.3.	Avaya Aura® Communication Manager SIP Entity – Local	27
5.4.4.	Avaya Session Border Controller for Enterprise SIP Entity.....	27
5.4.5.	Avaya Aura® Messaging SIP Entity	28
5.5.	Entity Links	29
5.5.1.	Entity Link to Avaya Aura® Communication Manager - Public	29
5.5.2.	Entity Link to Avaya Aura® Communication Manager Entity - Local	30
5.5.3.	Entity Link for the AT&T IP Flexible Reach – Enhanced Features Service via the Avaya SBCE	30
5.5.4.	Entity Link to Avaya Aura® Messaging	31
5.6.	Time Ranges.....	31
5.7.	Routing Policies	32
5.7.1.	Routing Policy for Public Routing to Avaya Aura® Communication Manager	32
5.7.2.	Routing Policy for Outbound Calls to AT&T	34
5.7.3.	Routing Policy for Local Routing from Avaya Aura® Communication Manager.....	35
5.7.4.	Routing Policy for Inbound Routing to Avaya Aura® Messaging.....	36
5.8.	Dial Patterns	37
5.8.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager	37

5.8.2.	Matching Outbound Calls to AT&T	40
5.8.3.	Matching Inbound Calls to Avaya Aura® Messaging Pilot Number via Avaya Aura® Communication Manager.....	41
5.8.4.	Message Wait Indicator (MWI) Notification from Avaya Aura® Messaging to Avaya Aura® Communication Manager.....	42
5.8.5.	Matching Outbound Calls from Avaya Aura® Messaging via Avaya Aura® Communication Manager.....	43
6.	Avaya Aura® Communication Manager	44
6.1.	System Parameters	44
6.2.	Dial Plan.....	46
6.3.	IP Node Names.....	47
6.4.	IP Interface for procr	47
6.5.	IP Network Regions	47
6.5.1.	IP Network Region 3 – Local Region.....	47
6.5.2.	IP Network Region 4 – AT&T Trunk Region	49
6.6.	IP Codec Parameters	50
6.6.1.	Codecs for IP Network Region 3 (local calls)	50
6.6.2.	Codecs for IP Network Region 4.....	51
6.7.	SIP Trunks.....	51
6.7.1.	SIP Trunk for AT&T calls	52
6.7.2.	Local SIP Trunk (Avaya Aura® Messaging and Avaya SIP Telephones).....	55
6.8.	Private Numbering	57
6.9.	Route Patterns	58
6.9.1.	Route Pattern for Calls to AT&T.....	58
6.9.2.	Route Pattern for Calls to Aura® Messaging	58
6.10.	Automatic Route Selection (ARS) Dialing	59
6.11.	Automatic Alternate Routing (AAR) Dialing	60
6.12.	Provisioning for Coverage to Aura® Messaging	60
6.12.1.	Hunt Group for Station Coverage to Avaya Aura® Messaging	60
6.12.2.	Coverage Path for Station Coverage to Avaya Aura® Messaging	61
6.12.3.	Station Coverage Path to Avaya Aura® Messaging	61
7.	Avaya Aura® Messaging.....	62
8.	Configure Avaya Session Border Controller for Enterprise	62
8.1.	Initial Installation/Provisioning.....	62
8.2.	Log Into the Avaya SBCE.....	63
8.3.	Global Profiles.....	63
8.3.1.	Server Interworking – Avaya Side.....	63
8.3.2.	Server Interworking – AT&T Side	64
8.3.3.	Routing – Avaya Side	65
8.3.4.	Routing – AT&T Side.....	66
8.3.5.	Server Configuration – To Avaya Aura® Session Manager	66
8.3.6.	Server Configuration – To AT&T	67
8.3.7.	Topology Hiding – Avaya Side	68
8.3.8.	Topology Hiding – AT&T Side.....	69
8.3.9.	Signaling Manipulation.....	69

8.4.	Domain Policies	70
8.4.1.	Application Rules.....	70
8.4.2.	Media Rules	71
8.4.3.	Signaling Rules	72
8.4.4.	Endpoint Policy Groups – Avaya	77
8.4.5.	Endpoint Policy Groups – AT&T	78
8.5.	Device Specific Settings.....	78
8.5.1.	Network Management.....	78
8.5.2.	Media Interfaces.....	79
8.5.3.	Signaling Interface	80
8.5.4.	Endpoint Flows – To Session Manager	80
8.5.5.	Endpoint Flows – To AT&T.....	81
8.6.	Troubleshooting Port Ranges	82
9.	Verification Steps.....	82
9.1.	AT&T IP Flexible Reach – Enhanced Features	82
9.2.	Avaya Aura® Communication Manager	83
9.3.	Avaya Aura® Session Manager	84
9.3.1.	Call Routing Test	85
9.4.	Protocol Traces.....	86
9.4.1.	AT&T IP Flexible Reach – Enhanced Features.....	86
9.5.	Avaya Session Border Controller for Enterprise Verification	88
10.	Conclusion	90
11.	References.....	91
12.	Addendum 1 – Redundancy to Multiple AT&T Border Elements	92
12.1.	Step 1: Configure the Secondary Location in Server Configuration.....	92
12.2.	Step 2: Add Secondary IP Address to Routing.....	93
12.3.	Step 3: Configure End Point Flows – SIP_Trunk_backup	94
13.	Addendum 2 – Dedicated Refer Call Redirection (Blind Transfer) Trunk for AT&T IP Flexible Reach - Enhanced Features Customers.....	96
13.1.	Configure Avaya Session Border Controller.....	96
13.1.1.	Create URI Group	96
13.1.2.	Routing	97
13.1.3.	Signaling Manipulation	98
13.2.	Configure Avaya Aura® Session Manager	99
13.2.1.	Adaptation for NCR Trunk	99
13.2.2.	SIP Entity for NCR Trunk.....	101
13.2.3.	Entity Link for NCR Trunk.....	102
13.2.4.	Routing Policy for NCR Trunk	102
13.2.5.	Dial Pattern for NCR Trunk	103
13.3.	Configure Communication Manager	104
13.3.1.	SIP Trunk for AT&T calls	104
13.3.2.	Network Based Blind Transfer with Refer (Communication Manager Vector) for AT&T IP Flexible Reach - Enhanced Features	107

1. Introduction

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

Avaya Aura® Session Manager 6.2 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.2 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 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 AVPN¹ or MIS/PNT² transport services.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya phones, fax machines (Vontifax application), Avaya Session Border Controller, and Avaya Aura® Messaging.
- A laboratory version of the IPFR-EF service, 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 PSTN across the IPFR-EF service network.

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).

¹ AVPN uses compressed RTP (cRTP).

² MIS/PNT does not support cRTP.

- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.
- Basic telephony features such as hold, resume, conference and transfer.
- Call Forward with Diversion Header.
- Avaya Aura® Messaging Reach-Me and Notify-Me features.

The following IPFR-EF service features were tested:

- Network based Simultaneous Ring
- Network based Sequential Ring (Locate Me)
- Network based Blind Transfer (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 and/or Communication Manager station transfer issues for IPFR-EF customers, if Network Call Redirection (NCR) is enabled on Communication Manager SIP trunks used for “general access”.

- If NCR is enabled on a SIP trunk used for calls to/from AT&T, two issues were observed with the IPFR-EF service:
 - Communication Manager will use SendOnly to signal Mute/Hold. The IPFR-EF network responds to this with Inactive (instead of RecOnly). Therefore when Communication Manager sends Music On Hold, the IPFR-EF network does not send the audio and PSTN hears nothing.
 - Communication Manager station initiated transfers to PSTN will use Refer signaling (Refer with Replaces) to perform the transfers. IPFR-EF does not support Refer with Replaces.
 - The workaround for these issues are:
 - Create a “general access” SIP trunk, with NCR *disabled*, for inbound and outbound calls (see **Section 6.7**).
 - For customers requiring the use of the IPFR-EF “Blind Transfer” feature (utilizing Refer), a separate SIP trunk with NCR enabled is defined for this exclusive use (see **Addendum 2**).

Also note that Meet-Me conference calls must not be directed to the NCR enabled trunk, or loss of Music On Hold may also result.

2. 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; however the subsequent network signaling does not have new calling information.
 - An Avaya SBCE SIP header manipulation script (**PAI_Display**) was created as workaround for this issue, and is documented in **Section 8.3.9**, item **A**.
 - An alternative workaround is described in **Section 6.7.1**, item **5**, however that solution is only applicable to Communication Manager 6.x platforms
3. **IPFR-EF Simultaneous Ring and Sequential Ring - Loss of audio on Communication Manager stations if Communication Manager “Initial IP-IP Direct Media” option is enabled.**
- If the Communication Manager *Initial IP-IP Direct Media* option is enabled on the SIP trunk Signaling Group form, (see **Section 6.7.1**), when the Communication Manager stations associated with these IPFR-EF answers the call, no audio will be heard in either direction.
 - The *Initial IP-IP Direct Media* option should be disabled (default) on the Signaling Group form for IPFR-EF customers.
 - Scheduled to be fixed in Communication Manager 6.2 Service Pack 3.
4. **Calls From/to Customer Trunks via the same AT&T border element (e.g., “looped” calls), which result in Communications Manager sending a 491 Request Pending, may experience a dropped call.**
- This issue was observed during a "looped" call where a Communication Manager station dials an AT&T IP Flexible Reach number, and the network destination of that call is a second Communication Manager station behind the same AT&T border element. Sometimes these calls result in Communication Manager issuing a 491 Request Pending in response to the "looped" Invite from the network. When the network also "loops" the 491 back to Communication Manager, the network inserts a Contact header that contains the IP address of an internal AT&T network node. As a result, Communication Manager attempts to route subsequent Invites to this unroutable address. Eventually these Invites time out and the call may be dropped.
 - This issue is under investigation by AT&T.
5. **Call transfer connection issue with Avaya one-X® Communicator in “Other Phone” mode** – There is a known loss of connection issue during call transfer scenarios with Avaya one-X® Communicator operating in “Other Phone” mode, in conjunction with Communication Manager 6.2.
- A fix for this issue is scheduled for Communication Manager 6.2 Service Pack 4.
6. **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) reviewed in this customer configuration guide 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 several components:

- An Avaya Midsize Enterprise 6.2 platform was used in the reference configuration. This platform includes Communication Manager 6.2, System Manager 6.2, and Session Manager 6.2. The solution described in these application notes is extensible to other Communication Manager, System Manager, and Session Manager 6.2 implementations.
- 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.
- 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 are represented with Avaya A175 (SIP), 1603(H.323), 960x Series IP Telephones (running H.323 or SIP firmware), and 96x1 Series IP Telephones (running H.323 or SIP firmware), Avaya 6424 Digital Telephones, as well as Avaya one-X® Communicator soft phone (in H323 mode).

- 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 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, e.g., the Avaya SBCE and Communication Manager. 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.
- Although the Avaya Midsize Enterprise platform used in the reference configuration includes embedded Communication Manager Messaging, Avaya Aura® Messaging was used in the reference configuration to provide voice messaging capabilities. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.

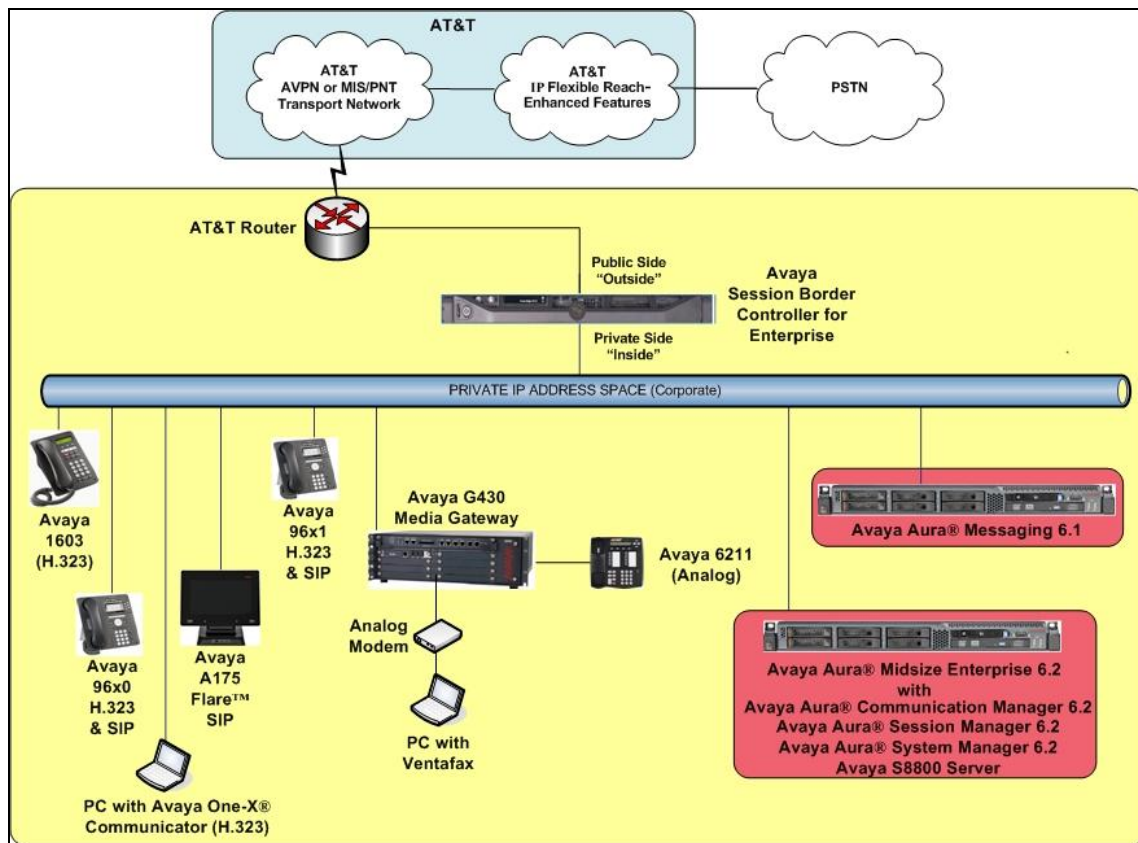


Figure 1: Reference configuration

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.

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes, and are **for illustrative purposes only**. Customers must obtain and use the specific values for their own specific configurations.

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
Avaya Aura® System Manager	
Management IP Address	192.168.67.46
Avaya Aura® Session Manager	
Management IP Address	192.168.67.45
Network IP Address	192.168.67.47
Avaya Aura® Communication Manager	
IP Address	192.168.67.44
Avaya Aura® Communication Manager extensions	19xxx = Stations and VDNs
Voice Messaging Pilot Extension	36000
Avaya Session Border Controller for Enterprise (SBCE)	
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
Avaya Aura Messaging	
IP Address	192.168.67.147
Messaging Mailboxes	19xxx
AT&T IP Flexible Reach - Enhanced Features Service	
Border Element IP Address	135.25.29.74

Table 1: Illustrative Values Used in these Application Notes

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.

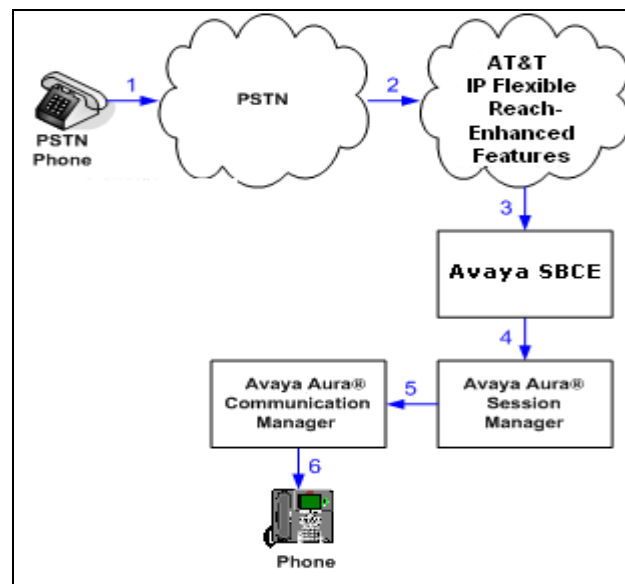


Figure 2: Inbound IPFR-EF Call

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 PSTN.
2. Communication Manager routes the call to the 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 PSTN.

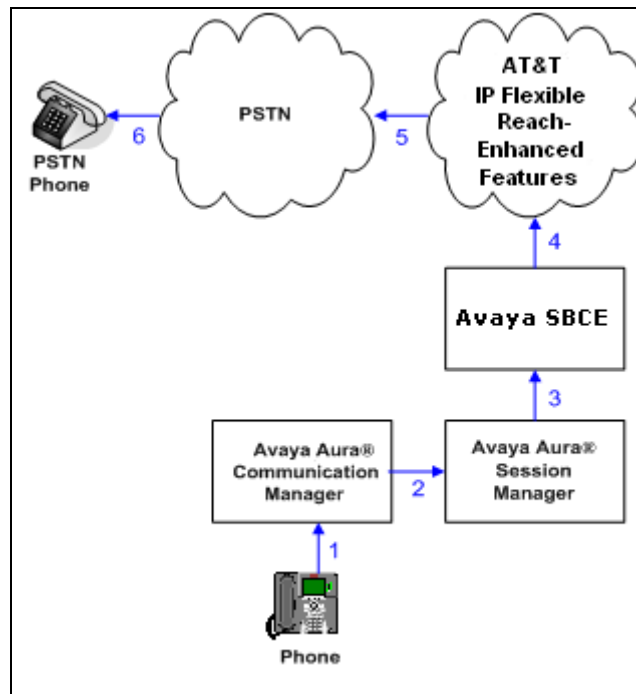


Figure 3: Outbound IPFR-EF Call

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.

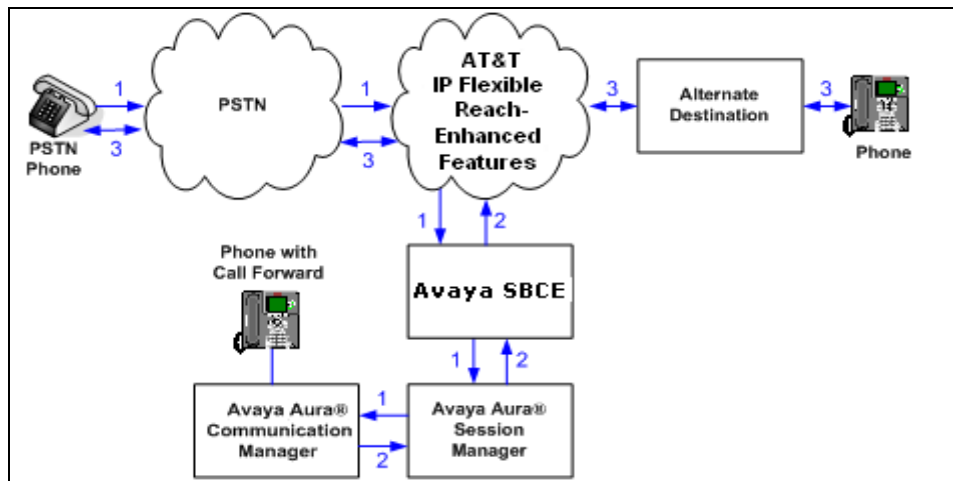


Figure 4: Station Re-directed (e.g. Call Forward) IPFR-EF Call

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.

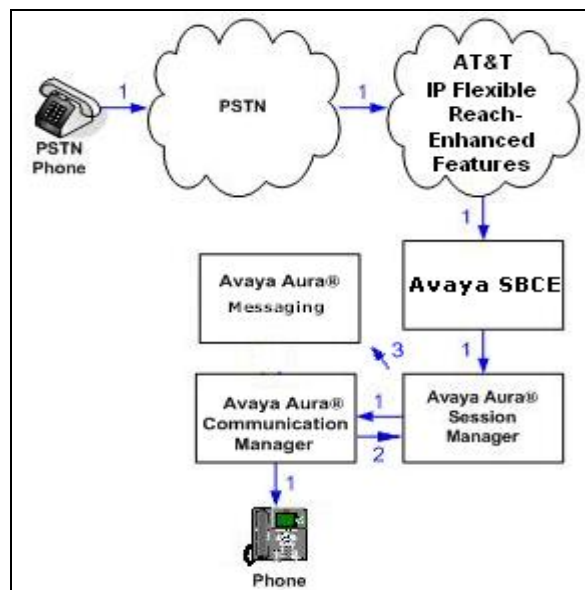


Figure 5: Coverage to Voicemail

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, Item 1** and **Addendum 2**).

This section describes the call flow used for IPFR-EF, which supports 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. 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).

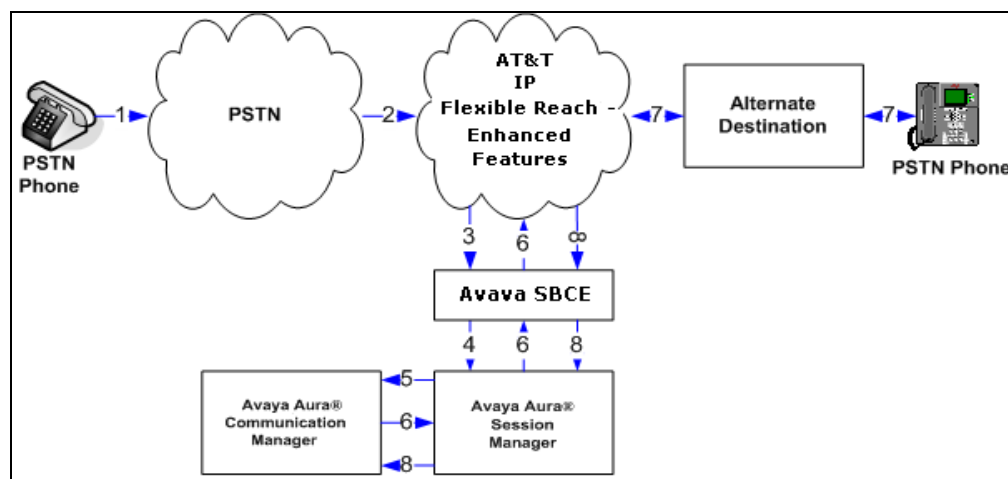


Figure 6: Network Based Blind Transfer Using Refer (Communication Manager Vector)

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/ Avaya Aura® Solution for Midsize Enterprise <ul style="list-style-type: none"> System Platform Avaya Aura® System Manager Avaya Aura® Session Manager Avaya Aura® Communication Manager 	<ul style="list-style-type: none"> 6.2.0.0.27 with patch 6.2.0.2.27 6.2 (6.2.12.0), with patch s12-1822, and SP1 (1871) 6.2 (6.2.0.0.620120) 6.2 (06.2-02.0.823.0), with patch 02.0.823.0-19593, and SP0 (02.0.823.0-0002)
Dell R610/Avaya Aura® Messaging	<ul style="list-style-type: none"> System Platform 6.0.3.6.3 6.1 with SP0 (00.1.510.1-115_0006)
Avaya G430 Media Gateway	30.10.4
MM711 Analog card	HW31 FW094
Dell R310/ Avaya Session Border Controller for Enterprise	4.0.5.Q09
Avaya 96x0 IP Telephone	H.323 Version S3.104S SIP Version 2.6.7.0
Avaya 96x1 IP Telephone	H.323 Version S6.020S SIP Version 6.0.4
Avaya A175 Flare™ Desktop Video Device (SIP telephone function)	SIP Version 1.1.0 (SIP_A175_1_1_0_012004)
Avaya one-X® Communicator	6.1.3.09-SP3-Patch3-35953
Avaya 1603 IP Telephone	H323 (ha1603ua1_3200.bin)
Avaya 6424 Digital telephone	-
Windows PC/ Ventafax Home Version (Fax device)	6.1.59.144
AT&T IP Flexible Reach - Enhanced Features service using AVPN/MIS-PNT transport service connection	VNI 24

Table 2: Equipment and Software Versions

5. Configure Avaya Aura® Session Manager Release 6.2

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 trunk 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.

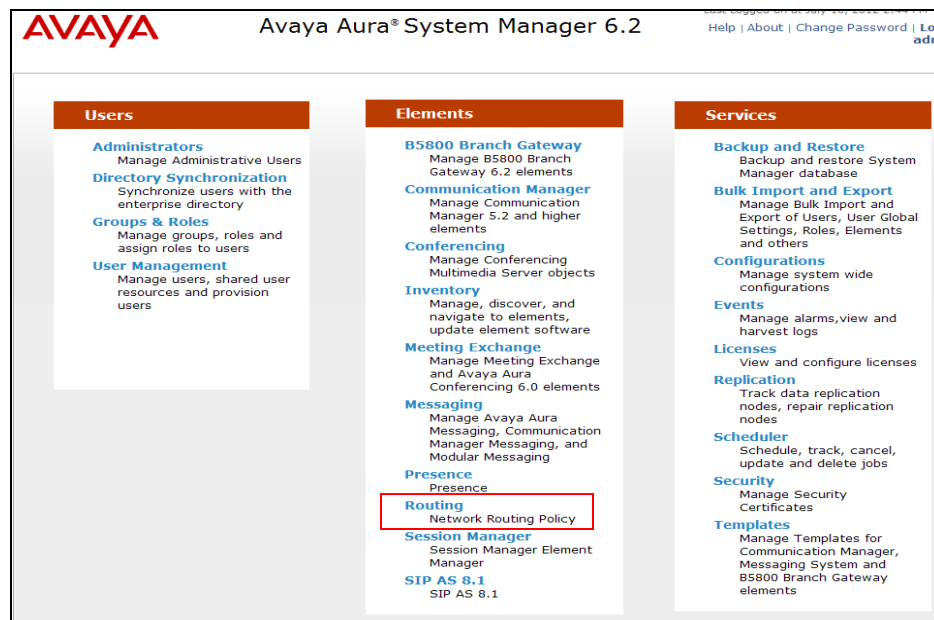
When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as Adaptations, are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose 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 Locations for 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 trunk 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, a Release 6.2 **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.

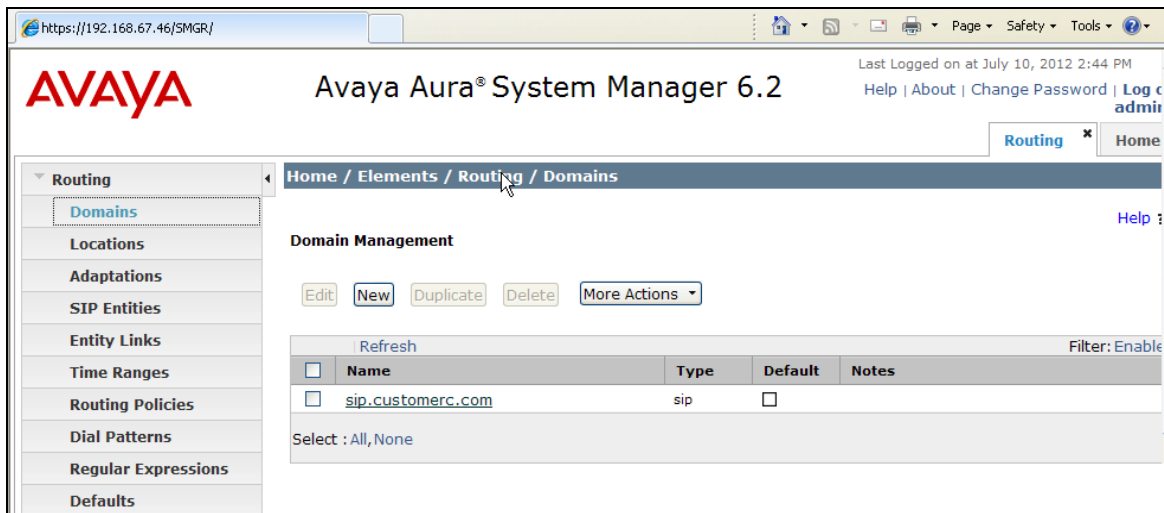


5.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration, domain **sip.customerc.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, **sip.customerc.com** is shown.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description. [Optional]



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

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) subnet **192.168.67.***.

5.2.1. Location for CPE Equipment

The location **Main** is used as a wild card 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 6.2

Last Logged on at July 10, 2012 2:44 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations

Location Details

Commit

Cancel

Help ?

General

* Name:

Main

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

* Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

* Latency before Overall Alarm Trigger:

5

Minutes

* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

1 Item

Refresh

Filter: Enable

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

Select : All, None

* Input Required

Commit

Cancel

5.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers in messages sent by AT&T, before those messages are routed to Communication Manager, and for messages 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 (**sip.customerc.com**).
 - 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 (**sip.customerc.com**) is replaced with the Avaya SBCE public IP address (**135.25.29.74**) in the destination headers.
 - The domain of Session Manager (**sip.customerc.com**) is replaced with the Avaya SBCE private IP address (**192.168.67.120**) in the origination headers.
 - The AT&T called number digit strings in the Request URI are replaced with their associated Communication Manager extensions/VDNs.
- Calls from AT&T to Avaya Aura® Messaging (**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:

- A descriptive **Name**, (e.g., **ACM62**).
- 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=sip.customerc.com**
osrcd=sip.customerc.com. The **odstd** parameter will replace the IP address of Session Manager (**192.168.67.47**) with **sip.customerc.com** in the *inbound* Request URI, and the **osrcd** parameter will replace the AT&T border element IP address (**135.25.29.74**) with **sip.customerc.com** in the PAI header, when Session Manager sends the Invite to Communication Manager.

The screenshot shows the Avaya Aura® System Manager 6.2 web interface. The left navigation pane is expanded to 'Routing', and 'Adaptations' is selected. The main content area is titled 'Adaptation Details' and 'General'. The form contains the following fields:

- Adaptation name:** ACM62
- Module name:** DigitConversionAdapter (selected from a dropdown menu)
- Module parameter:** odstd=sip.customerc.com osrcd=sip.customerc.com
- Egress URI Parameters:** (empty field)
- Notes:** (empty text area)

At the top right, there are links for 'Help', 'About', 'Change Password', and 'Log off admin'. At the bottom right, there are 'Commit' and 'Cancel' buttons.

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: 7325553161 is a DNIS string sent in the Request URI by AT&T Flexible Reach service that is associated with Communication Manager extension 19001.

- Enter **7325553161** in the **Matching Pattern** column.
- Enter **10** in the **Min/Max** columns.
- Enter **10** 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. For example **7325553162** is converted to the Vector Directory Number (VDN) **19011** used to generate an outbound SIP Refer (see **Section 6.13**).

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									
<input type="button" value="Add"/> <input type="button" value="Remove"/>									
0 Items <input type="button" value="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									
<input type="button" value="Add"/> <input type="button" value="Remove"/>									
<input type="button" value="Refresh"/> Filter: Enable									
<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*7325553161	*10	*10		*10	19010	destination		Enhanced
<input type="checkbox"/>	*7325553162	*10	*10		*10	19011	destination		Enhanced
<input type="checkbox"/>	*7325554383	*10	*10		*10	19001	destination		Basic
<input type="checkbox"/>	*7325554384	*10	*10		*10	19002	destination		Basic
<input type="checkbox"/>	*7325554385	*10	*10		*10	19003	destination		Basic

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), sent by Communication Manager.

- In the **Module parameter** field enter **odstd=<AT&T border Element IP address>**
osrcd=<Avaya SBCE public IP address>. For example:

odstd= 135.25.29.74 osrcd=192.168.64.130

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

The screenshot shows the Avaya Aura System Manager 6.2 web interface. The left navigation pane is expanded to 'Routing', and the 'Adaptations' sub-menu is selected. The main content area displays the 'Adaptation Details' page for an adaptation named 'ATT'. The 'General' tab is active, showing the following fields: 'Adaptation name' (ATT), 'Module name' (AttAdapter), 'Module parameter' (odstd=135.25.29.74 osrcd=192.168.64.130), 'Egress URI Parameters' (empty), and 'Notes' (Outbound to ATT). Below the 'General' tab, there are two sections for 'Digit Conversion'. The first section, 'Digit Conversion for Incoming Calls to SM', has an 'Add' button and a 'Remove' button, and a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, Address to modify, Adaptation Data, and Notes. The second section, 'Digit Conversion for Outgoing Calls from SM', also has 'Add' and 'Remove' buttons and a similar table. At the bottom right, there are 'Commit' and 'Cancel' buttons.

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:

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

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

- Example: 7325553170 is a DNIS string sent in the Request URI by AT&T Flexible Reach service that is associated with Avaya Aura® Messaging pilot number 36000.
- Enter **7325553170** in the **Matching Pattern** column.

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

Step 4 - Click on **Commit** (not shown).

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

Commit Cancel

Adaptation Details

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

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

Digit Conversion for Outgoing Calls from SM

Add Remove

Refresh Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	*7325553170	*10	*10		*10	36000	destination	

Select : All, None

* Input Required Commit Cancel

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 5060, 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 for local trunk calls as well as 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, TCP (port 5060) is used as the transport protocol between Session Manager and the Communication Manager Public SIP trunk, the Avaya SBCE, and Avaya Aura® Messaging. This was done to facilitate protocol trace analysis. TLS was used on the SIP trunk between Session Manager and Communication Manager for local traffic (e.g., to/from Avaya Aura® Messaging). 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., **sm62**).
- **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.

These entries enable Session Manager to accept SIP requests on the specified ports/protocols. In addition, Session Manager will accept SIP requests containing the IP address of Session Manager (192.168.67.47) in the host part of the Request-URI.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: sm62

* 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 - In the **Port** section of the **SIP Entity Details** page, click on **Add** and provision an entry as follows:

- **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., **sip.customer.com**)

This is for public traffic between the CPE and the IPFR-EF service.

Step 5 - Repeat **Step 4** to provision another entry, with **5061** for **Port** and **TLS** for **Protocol**. This is for local traffic between Session Manager and Communication Manager.

Port

TCP Failover port:

TLS Failover port:

Add Remove

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	sip.customer.com	
<input type="checkbox"/>	5061	TLS	sip.customer.com	

Select : All, None

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**.

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. **ACM62_Public**).
- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.3** (e.g. **192.168.67.44**).
- **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 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**.

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

Avaya Aura® System Manager 6.2

Last Logged on at July 19, 2012 3:24 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing * **Home**

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#) **Commit** **Cancel**

General

* **Name:** ACM62_Public

* **FQDN or IP Address:** 192.168.67.44

Type: CM

Notes:

Adaptation: ACM62

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

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

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.

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

The screenshot displays the Avaya Aura Configuration Manager web interface. On the left is a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / SIP Entities'. It contains the 'SIP Entity Details' form for a 'General' tab. The form includes the following fields and settings:

- Name:** ACM62_Local
- FQDN or IP Address:** 192.168.67.44
- Type:** CM (dropdown menu)
- Notes:** (empty text box)
- 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 box)
- Call Detail Recording:** egress (dropdown menu)
- 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)

At the top right of the form area are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

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 **Other**. See the figure below for the values used in the reference configuration.

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

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

Home / Elements / Routing / SIP Entities

▼ Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

[Help ?](#)
Commit
Cancel

SIP Entity Details

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:

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring:

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.

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

The screenshot shows the 'SIP Entity Details' configuration page. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb 'Home / Elements / Routing / SIP Entities' and a 'Help ?' link. The 'General' tab is active, showing fields for:

- * Name: AA-M
- * FQDN or IP Address: 192.168.67.147
- Type: Modular Messaging
- Notes: (empty text area)
- Adaptation: AAM_Digits
- Location: Main
- Time Zone: America/New_York
- Override Port & Transport with DNS SRV: (unchecked)
- * SIP Timer B/F (in seconds): 4
- Credential name: (empty text area)
- Call Detail Recording: none

 The 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. At the bottom, there are checkboxes for 'Supports Call Admission Control' and 'Shared Bandwidth Manager', both unchecked, and dropdowns for 'Primary Session Manager Bandwidth Association' and '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., **ACM62_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 **5060**.
- **Protocol** – Select **TCP**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity.
- **SIP Entity 2 Port** - Enter **5060**.
- **Connection Policy** – Select **Trusted**.

Step 3 - Click on **Commit**.

The screenshot shows the 'Entity Links' configuration page in the Avaya Aura Configuration Manager. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail 'Home / Elements / Routing / Entity Links' and a 'Help ?' link. Below this, there are 'Commit' and 'Cancel' buttons. The 'Entity Links' section shows a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row shows: Name: *ACM62_Public, SIP Entity 1: sm62, Protocol: TCP, Port: *5060, SIP Entity 2: *ACM62_Public, Port: *5060, Connection Policy: Trusted, Notes: ATT traffic. At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
*ACM62_Public	sm62	TCP	*5060	*ACM62_Public	*5060	Trusted	ATT traffic

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., **ACM62_Local**). The **Protocol** is **TLS** and the **Port** is **5061**. See the figure below for the values used in the reference configuration.

The screenshot shows the 'Entity Links' configuration page in the Avaya Aura Configuration Manager. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail 'Home / Elements / Routing / Entity Links' and a 'Help ?' link. Below this, there are 'Commit' and 'Cancel' buttons. The 'Entity Links' section shows a table with 1 item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The row shows: Name: *ACM62_Local, SIP Entity 1: sm62, Protocol: TLS, Port: *5061, SIP Entity 2: *ACM62_Local, Port: *5061, Connection Policy: Trusted, Notes: Local traffic. At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
*ACM62_Local	sm62	TLS	*5061	*ACM62_Local	*5061	Trusted	Local traffic

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.

Routing x Home

Home / Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* A-SBCE	* sm62	TCP	* 5060	* A-SBCE	* 5060	Trusted	

* Input Required Commit Cancel

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.

Routing x Home

Home / Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to AA-M	* sm62	TCP	* 5060	* AA-M	* 5060	Trusted	

* Input Required Commit Cancel

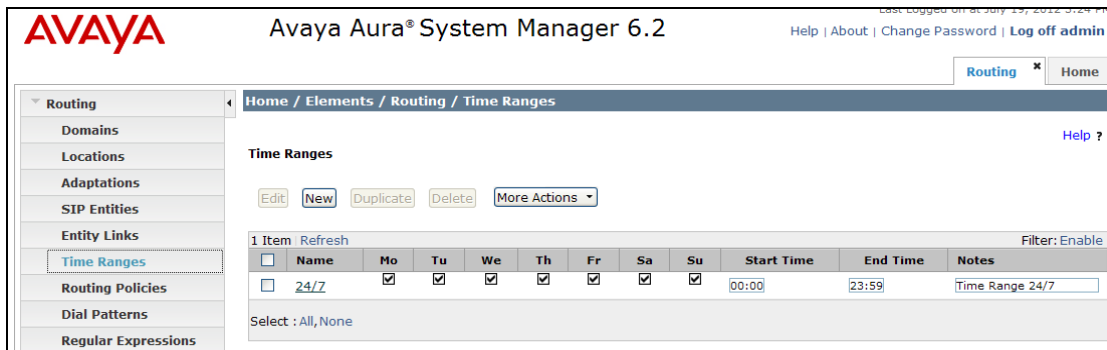
5.6. Time Ranges

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 checkboxes for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

Step 3 - Click on **Commit**.

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



5.7. Routing Policies

In this section, the following Routing Policies are administered:

- Calls to Communication Manager (**Section 5.7.1**).
- Calls to AT&T (**Section 5.7.2**).
- Avaya Aura® Messaging Message Wait Indicator (MWI) notification to Communication Manager (**Section 5.7.3**).
- Communication Manager call coverage to Avaya Aura® Messaging (**Section 5.7.4**)

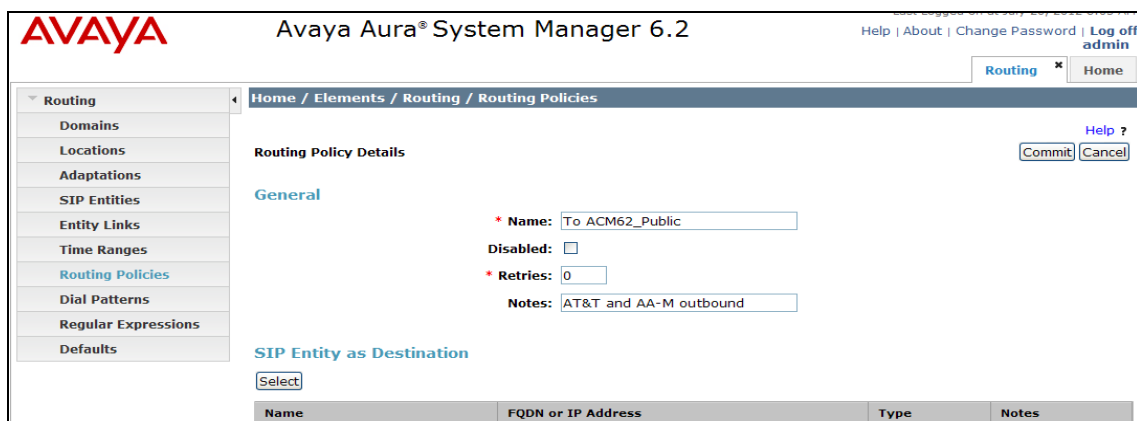
5.7.1. Routing Policy for Public Routing to Avaya Aura® Communication Manager

This routing policy is used for inbound calls from AT&T as well as for outbound calls from Avaya Aura® Messaging (Reach-Me and Notify-Me).

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., **To ACM62_Public**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

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



Step 4 - In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**ACM62_Public**), and click on **Select**.

SIP Entity List Select Cancel

SIP Entities

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

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	AA-M	192.168.67.147	Modular Messaging	
<input type="radio"/>	ACM62_Local	192.168.67.44	CM	
<input checked="" type="radio"/>	ACM62_Public	192.168.67.44	CM	
<input type="radio"/>	A-SBCE	192.168.67.120	Other	
<input type="radio"/>	sm62	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**.

Avaya Aura® System Manager 6.2

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit

Cancel

Help ?

General

* Name:

To ACM62_Public

Disabled:

☐

* Retries:

0

Notes:

AT&T and AA-M outbound

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM62_Public	192.168.67.44	CM	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item

Refresh

Filter: 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

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
--------------------------	---------	------------	------	-------

* Input Required

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 local calls to Communication Manager (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-SCBE to ATT**).
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

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

Time of Day

1 Item Filter: [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

Filter: [Enable](#)

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
Select : All, None							

Regular Expressions

0 Items Filter: [Enable](#)

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

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

This routing policy is used for Message Wait Indicator (MWI) from Avaya Aura® Messaging to Communication Manager. 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. **ACM62_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. **ACM62_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: ACM62_Local

Disabled: ☐

* Retries: 0

Notes: MWI

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM62_Local	192.168.67.44	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

Filter: 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, from AT&T 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_AA-M**), 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.

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

Routing Policy Details

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

[Select](#)

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

Time of Day

[Add](#)
[Remove](#)
[View Gaps/Overlaps](#)

1 Item [Refresh](#) Filter: [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

[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
--------------------------	---------	------------	------	-------

5.8. Dial Patterns

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

- Inbound PSTN calls via IPFR-EF service to Communication Manager.
- Outbound calls to AT&T.
- 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 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 10 digit pattern 732555xxxx 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 Request URI, not the digit string that was 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 10 digit number in the Request URI with the format 732555xxxx. Enter **732555**. Note - The adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 732555xxxx numbers into their corresponding Communication Manager extensions.
- **Min** and **Max** – Enter **10**.
- **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.

The screenshot shows the 'Dial Pattern Details' page in the 'Routing' section. The left navigation pane has 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and has a 'General' section. The fields in the 'General' section are: Pattern (732555), Min (10), Max (10), Emergency Call (unchecked), Emergency Priority (1), Emergency Type, SIP Domain (-ALL-), and Notes (AT&T inbound). There are buttons for 'Commit', 'Cancel', and 'Help ?' in the top right corner.

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 Location and Routing Policy List** 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 **-ALL-** is selected, 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., **To_ACM62_Public**).

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

Filter: Enable

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

Select : All, None

Routing Policies

7 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ACM62_Local	<input type="checkbox"/>	ACM62_Local	MWI
<input type="checkbox"/>	A-SBCE to ATT	<input type="checkbox"/>	A-SBCE	
<input type="checkbox"/>	To_AA-M	<input type="checkbox"/>	AA-M	
<input checked="" type="checkbox"/>	To ACM62_Public	<input type="checkbox"/>	ACM62_Public	ATT traffic

Select : All, None

Step 6 - In the Originating Location and Routing Policy List page, 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.

Dial Pattern Details

General

* Pattern: 732555

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: AT&T inbound

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		To ACM62_Public	0	<input type="checkbox"/>	ACM62_Public	ATT traffic

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

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

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 1xxxxyyyxxxx, x11, and 011 international calls were verified. In addition, IPFR-EF access codes (e.g., *7xxxxyyyxxxx) were verified. 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 AT&T (e.g. **1732**).
- Enter a **Min** and **Max** pattern of **11**.
- In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to “**Apply The Selected Routing Policies to All Originating Locations**”.
- In the **Routing Policies** section of the **Originating Location and Routing Policy List** 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**).

Dial Pattern Details
General

* Pattern:

1732

* Min:

11

* Max:

11

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

outbound

Originating Locations and Routing Policies

Add

Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	A-SBCE to ATT	0	<input type="checkbox"/>	A-SBCE	

Select : All, None

Denied Originating Locations

Add

Remove

0 Items Refresh

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

* Input Required

Commit

Cancel

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 Location and Routing Policy List** page, check the checkbox corresponding to “**Apply The Selected Routing Policies to All Originating Locations**”.
- In the **Routing Policies** section of the **Originating Location and Routing Policy List** 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_AA-M**).

Dial Pattern Details
General

* Pattern:

36000

* Min:

5

* Max:

5

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

AA-M Pilot Number

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To_AA-M	0	<input type="checkbox"/>	AA-M	

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

Refresh

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

* Input Required

Commit

Cancel

5.8.4. Message Wait Indicator (MWI) Notification from Avaya Aura® Messaging to Avaya Aura® Communication Manager

Avaya Aura® Messaging signals MWI by sending a SIP Notify message to the associated Communication Manager extension. 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, extensions used the pattern 190xx.
- Enter a **Min** and **Max** pattern of **5**.
- In the **Originating Location** section of the **Originating Location and Routing Policy List** 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 Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy administered for routing calls to Communication Manager public trunk in **Section 5.4.2** (e.g., **To_ACM62_Local**).

Dial Pattern Details

Commit

Cancel

General

* Pattern:

190

* Min:

5

* Max:

5

Emergency Call:

☐

Emergency Priority:

1

Emergency Type:

SIP Domain:

-ALL-

Notes:

Station MWI

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		ACM62_Local	0	<input type="checkbox"/>	ACM62_Local	MWI

Select : All, None

Denied Originating Locations

Add

Remove

0 Items

Refresh

Filter: Enable

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

* Input Required

Commit

Cancel

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. 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**. 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. 9).
- Enter a **Min** and **Max** pattern of 12 (the ARS code 9 plus an 11 digit outbound number, e.g., 91732xxxxxxx).
- In the **Originating Location** section of the **Originating Location and Routing Policy List** 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 Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy administered for routing calls to Communication Manager public trunk in **Section 5.4.2** (e.g., **To_ACM62_Public**).

Dial Pattern Details
General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Main		To_ACM62_Public	0	<input type="checkbox"/>	ACM62_Public	ATT traffic

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

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

* Input Required

Commit Cancel

6. 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], [6] and [7] 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: 18000 1
      Maximum Video Capable IP Softphones: 18000 2
      Maximum Administered SIP Trunks: 24000 24
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)? y	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	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	IP Stations? y	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	ISDN-PRI? y	
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		
(NOTE: You must logoff & login to effect the permission changes.)		

Step 5 - On Page 5 of the 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? y	Station as Virtual Extension? y
Multiple Locations? n	
	System Management Data Transfer? n
Personal Station Access (PSA)? y	Tenant Partitioning? y
PNC Duplication? n	Terminal Trans. Init. (TTI)? y
Port Network Support? y	Time of Day Routing? y
Posted Messages? y	TN2501 VAL Maximum Capacity? y
	Uniform Dialing Plan? y
Private Networking? y	Usage Allocation Enhancements? y
Processor and System MSP? y	
Processor Ethernet? y	Wideband Switching? y
Remote Office? y	Wireless? n
Restrict Call Forward Off Net? y	
Secondary Data Module? y	

6.2. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager.

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 dial access codes (indicated with a **Call Type** of **dac**) beginning with * for Trunk Access Codes (TACs) defined for trunk groups in the reference configuration.
- 5-digit extensions with a **Call Type** of **ext** beginning with:
 1. The digit **1** (Local extensions for Communication Manager stations and VDNs).
 2. The digit **3** (Avaya Aura® Messaging pilot number 36000).
- 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**).

change dialplan analysis						Page 1 of 12		
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						
8	1	fac						
9	1	fac						
*	3	dac						

6.3. IP Node Names

Node names define IP addresses to various Avaya components in the enterprise.

Step 1 - Enter the **change node-names ip** command, and add a node name and IP address for the Session Manager signaling interface (e.g., **SM** and **192.168.67.47**). 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** & **192.168.67.44**) appear automatically based on the address defined during installation. This IP address was used to define the Communication Manager SIP Entities in **Section 5.4**.

```
change node-names ip                                     Page 1 of 2
IP NODE NAMES
  Name              IP Address
SM                 192.168.67.47
default            0.0.0.0
procr              192.168.67.44
procr6             ::
```

6.4. IP Interface for procr

The **display ip-interface procr** command can be used to verify the Processor Ethernet (PE) 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., **3**).
- Use default values for the remaining parameters.

```
display ip-interface procr                               Page 1 of 2
                                                    IP INTERFACES
Type: PROCR
Target socket load: 1700
Enable Interface? y      Allow H.323 Endpoints? y
                        Allow H.248 Gateways? y
                        Gatekeeper Priority: 5
Network Region: 3
IPV4 PARAMETERS
Node Name: procr        IP Address: 192.168.67.44
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 3 – Local Region

In the reference configuration, local Communication Manager elements (e.g., procr) as well as other local Avaya devices (e.g., IP telephones, Avaya Aura® Messaging) are assigned to **ip-network-region 3**.

Step 1 – Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region **3**). 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 **sip.customer.com** in the **Authoritative Domain** field.
 - Enter **1** for the **Codec Set** parameter.
 - **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
 - **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
 - **UDP Port Min:** – Set to **16384** (AT&T requirement).
 - **UDP Port Max:** – Set to **32767** (AT&T requirement).

change ip-network-region 3	Page 1 of 20
IP NETWORK REGION	
Region: 3	
Location: 1	Authoritative Domain: sip.customer.com
Name: Local	
MEDIA PARAMETERS	
Codec Set: 1	Intra-region IP-IP Direct Audio: yes
UDP Port Min: 16384	Inter-region IP-IP Direct Audio: yes
UDP Port Max: 32767	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	
AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	
H.323 Link Bounce Recovery? y	
Idle Traffic Interval (sec): 20	
Keep-Alive Interval (sec): 5	
Keep-Alive Count: 5	
RSVP Enabled? n	

Step 2 - On page 2 of the form:

- Verify that RTCP reporting and monitoring are set to **y**.

change ip-network-region 3	Page 2 of 20
IP NETWORK REGION	
RTCP Reporting Enabled? y	
RTCP MONITOR SERVER PARAMETERS	
Use Default Server Parameters? y	

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

- Verify that next to region **3** in the **dst rgn** column, the codec set is **1**.
- Next to region **4** in the **dst rgn** column, enter **2** for the codec set (this means region 3 is permitted to talk to region 4 and it will use codec set 2 to do so). The **direct WAN** and **Units** columns will self populate with **y** and **No Limit** respectively.
- Let all other values default for this form.

change ip-network-region 3										Page 4 of 20		
Source Region: 3										Inter Network Region Connection Management		
										I		M
										G	A	t
dst rgn	codec set	direct WAN	WAN-BW-limits Units	Video Total Norm	Prio Shr	Intervening Regions	Dyn CAC	A R	G L	c e		
1												
2												
3	1								all			
4	2	y	NoLimit					n		t		
5												

6.5.2. IP Network Region 4 – AT&T Trunk Region

In the reference configuration, AT&T SIP trunk calls are assigned to **ip-network-region 4**. Repeat the steps in **Section 6.5.1** with the following changes:

Step 1 – On **Page 1** of the form:

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

change ip-network-region 4		Page 1 of 20	
IP NETWORK REGION			
Region: 4			
Location: 1		Authoritative Domain: sip.customerb.com	
Name: AT&T			
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 2		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 16384		IP Audio Hairpinning? n	
UDP Port Max: 32767			
DIFFSERV/TOS PARAMETERS			
Call Control PHB Value: 46			
Audio PHB Value: 46			
Video PHB Value: 26			
802.1P/Q PARAMETERS			
Call Control 802.1p Priority: 6			
Audio 802.1p Priority: 6			
Video 802.1p Priority: 5			
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 4 of the form:

- Verify that codec set **2** is listed for **dst rgn 3** and **4**.

change ip-network-region 4										Page	4 of	20
Source Region: 4										Inter Network Region Connection Management		
										I		M
										G	A	t
dst codec direct	WAN-BW-limits	Video	Intervening		Dyn		A	G	c			
rgn set	WAN Units	Total Norm	Prio Shr	Regions	CAC	R	L	e				
1												
2												
3	2	y	NoLimit					n		t		
4	2							all				
5												

6.6. IP Codec Parameters

6.6.1. Codecs for IP Network Region 3 (local calls)

In the reference configuration, IP Network Region 3 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				
4:							

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

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

6.6.2. Codecs for IP Network Region 4

In the reference configuration IP Network Region 4 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 G.729B and G.729A set **3** for the **Frames Per Pkt**. This will automatically populate **30** for the Packet Size (ms). Let G.711MU 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			
4:						

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

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

6.7. SIP Trunks

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

- AT&T access – SIP Trunk 4
 - Note that this trunk will use TCP port 5060 as described in **Section 5.5.1**.
- Local for Avaya Aura® Messaging and Avaya SIP telephone access – SIP Trunk 3
 - 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, the transport protocol used between the Avaya SBCE and the IPFR-EF service is UDP.

Note – In the reference configuration, TCP (port 5060) is used as the transport protocol between Session Manager and all the SIP Entities including the Communication Manager public SIP trunk. This was done to facilitate protocol trace analysis. The link between Session Manager and Communication Manager Local SIP trunk was TLS (port 5061). This is the default configuration during the installation of Midsize Enterprise (ME), used in the reference configuration. Note that Avaya best practices call for TLS to be used as the transport protocol in customer environments whenever possible.

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 **ACM62_Public** 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., **4**), 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., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060** (see the note at the beginning of this section).
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 6.5.2**.
- **Far-end Domain** – Enter **sip.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 initiates Communication Manager to send SIP OPTIONS messages to Session Manager to provide link status.

Note – Verify that the **Initial IP-IP Direct Media?** option is set to **n** (default). See **Section 2.2.1, Item 3**.

add signaling-group 4		Page 1 of 1
SIGNALING GROUP		
Group Number: 4	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: SM	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 4	
	Far-end Secondary Node Name:	
Far-end Domain: sip.customercc.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., **4**). 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., ***04**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **4**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **20**).

add trunk-group 4		Page 1 of 21
TRUNK GROUP		
Group Number: 4	Group Type: sip	CDR Reports: y
Group Name: ATT	COR: 1	TN: 1
Direction: two-way	Outgoing Display? n	TAC: *04
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 4	
	Number of Members: 20	

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

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

add trunk-group 4		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
SCCAN? n	Redirect On OPTIM Failure: 6000	
Preferred Minimum Session Refresh Interval(sec): 900		Digital Loss Group: 18
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.

add trunk-group 4		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
<div style="text-align: right;"> UI Treatment: service-provider Replace Restricted Numbers? y Replace Unavailable Numbers? y </div>		
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 **n** (default).
- **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 required by the IPFR-EF service (e.g., **100**).

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.

Note – The display issue described in item **2** of **Section 2.2.1** 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.

```

                                PROTOCOL VARIATIONS
                                Mark Users as Phone? n
                                Prepend '+' to Calling Number? n
                                Send Transferring Party Information? n
                                Network Call Redirection? n
                                Send Diversion Header? y
                                Support Request History? y
                                Telephone Event Payload Type: 100
                                Convert 180 to 183 for Early Media? n
                                Always Use re-INVITE for Display Updates? n
                                Identity for Calling Party Display: P-Asserted-Identity
                                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 **ACM62_Local** 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., **3**), 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 **3**, as defined in **Section 6.5.1**.

add signaling-group 3

Page 1 of 1

```

                                SIGNALING GROUP
Group Number: 3                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: SM
Near-end Listen Port: 5061     Far-end Listen Port: 5061
Far-end Network Region: 3
Far-end Domain: sip.customer.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., **3**). 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., ***03**).
- **Service Type** – Set to **tie**.

- **Signaling Group** – Set to the number of the signaling group administered in **Step 1** (e.g., **3**).

add trunk-group 3		Page 1 of 21
TRUNK GROUP		
Group Number: 3	Group Type: sip	CDR Reports: y
Group Name: Local	COR: 1	TN: 1 TAC: *03
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: 3	
	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:

- Set **Numbering Format**: to **private**.

add trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: internal	
	Maintenance Tests? y	
Numbering Format: private		
	UII Treatment: service-provider	
	Replace Restricted Numbers? y	
	Replace Unavailable Numbers? y	
	Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y		
DSN Term? n		

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.

add trunk-group 3		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling 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		
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, (previously identified by AT&T), for inclusion in any SIP headers directed to the IPFR-EF service via the public trunk (e.g., 4) defined in **Section 6.7.1**.
- Direct local extensions to Avaya Aura® Messaging (call coverage/retrieval) to the local trunk (e.g., 3) defined in **Section 6.7.2**.

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 6.13.1** (e.g., **36000**).
- Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **3**).
- 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**).
- Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **3**).
- 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 AT&T trunk group (e.g., **4**).
- CPN Prefix** – Enter the corresponding IPFR-EF DNIS number (e.g., **7325554300**).
- 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	3		5	Total Administered: 5
5	36000	3		5	Maximum Entries: 540
5	19001	4	7325554300	10	
5	19002	4	7325554036	10	
5	19011	4	7325554037	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 6.11** (e.g., calls to AT&T).

Step 1 – Enter the **change route-pattern 4** command and enter the following:

- In the **Grp No** column enter **4** for SIP trunk 4 (Public trunk).
- In the **FRL** column enter **0** (zero).
- In the Numbering Format column, across from line **1**: enter **unk-unk**.
- In the LAR column enter **next**.

change route-pattern 4															Page 1 of 3		
Pattern Number: 4															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		
															Intw		
1:	4	0													n	user	
2:															n	user	
3:															n	user	
4:															n	user	
5:															n	user	
6:															n	user	
BCC		VALUE		TSC	CA-TSC	ITC		BCIE	Service/Feature		PARM	No.	Numbering	LAR			
0		1 2 M 4 W			Request							Dgts	Format				
													Subaddress				
1:	y	y	y	y	y	n	n	rest				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				

6.9.2. 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 6.12** (e.g., calls to the Avaya Aura® Messaging pilot number 36000).

Step 1 – Enter the **change route-pattern 3** command and enter the following:

- In the **Grp No** column enter **3** 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 3													Page	1 of 3	
Pattern Number: 3													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:	3	0										n	user		
2:													n	user	
3:													n	user	
4:													n	user	
5:													n	user	
6:													n	user	
BCC VALUE		TSC	CA-TSC		ITC BCIE			Service/Feature			PARM	No.	Numbering	LAR	
0 1 2 M 4 W		Request										Dgts	Format		
													Subaddress		
1:	y	y	y	y	y	n	rest						unk-unk	next	
2:	y	y	y	y	y	n	rest						none		
3:	y	y	y	y	y	n	rest						none		
4:	y	y	y	y	y	n	rest						none		
5:	y	y	y	y	y	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 6.10.1**).

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

- In the **Dialed String** column enter a matching dial pattern (e.g. **1732**) Note – The best match will route first, that is 1732555xxxx will be selected before 17xxxxxxxxx.
- In the **Min** and **Max** columns enter the corresponding matching digit lengths, (e.g. **11** and **11**).
- In the Route Pattern column select a route-pattern to be used for these calls (e.g.**1**).
- In the **Call Type** column enter **hnpa**.

In the example below outbound calls to 1732xxxxxxx and 1800xxxxxxx will be sent to route-pattern 4, but calls to 1900xxxxxxx will be denied.

change ars analysis 1732										Page 1 of 2
ARS DIGIT ANALYSIS TABLE										
Location: all Percent Full: 1										
Dialed	Total	Route	Call	Node	ANI					
String	Min Max	Pattern	Type	Num	Reqd					
1732	11 11	4	hnpa		n					
1800	11 11	4	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 6.10.2**.

Step 1 – For the Avaya Aura® Messaging coverage hunt group extension, enter the following:

- **Dialed String** – Enter **36000**.
- **Min & Max** – Enter **5**.
- **Route Pattern** – Enter **3**.
- **Call Type** – Enter **aar**.

change aar analysis 0						Page 1 of 2	
AAR DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
36000	5	5	3	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 need *not* be the same as the Avaya Aura® Messaging pilot number.
- **ISDN/SIP Caller Display** – Enter **mbr-name**.
- Let all other fields default.

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

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

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

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

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.

add coverage path 1		Page 1 of 1
COVERAGE PATH		
Coverage Path Number: 1		
Cvg Enabled for VDN Route-To Party? n	Next Path Number:	Hunt after Coverage? n Linkage
COVERAGE CRITERIA		
Station/Group Status	Inside Call	Outside Call
Active?	n	n
Busy?	y	y
Don't Answer?	y	y
All?	n	n
DND/SAC/Goto Cover?	y	y
Holiday Coverage?	n	n
COVERAGE POINTS		
Terminate to Coverage Pts. with Bridged Appearances? n		
Point1: h1	Rng: 4	Point2:
Point3:	Point4:	Number of Rings: 4
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 6.13.2**. Note that the coverage path field will appear at different positions on the form depending on whether agent or station extensions are being provisioned.

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

7. 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 [8] and [9] for further details.

8. Configure Avaya Session Border Controller for Enterprise

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

8.1. Initial Installation/Provisioning

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to [10], [11], and [12] for additional information.

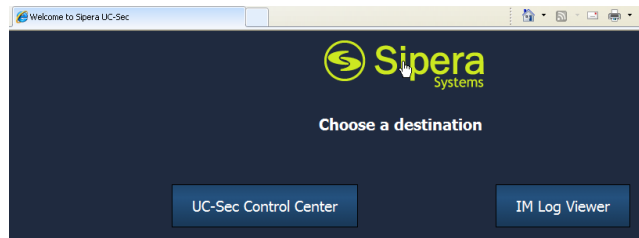
IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this resolved.

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

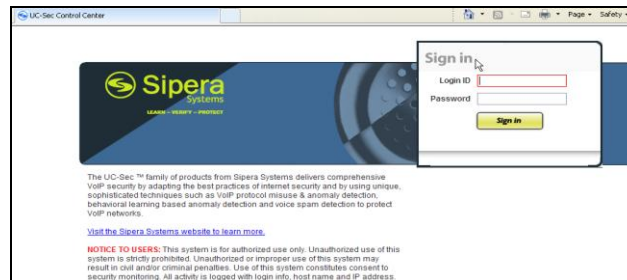
8.2. Log Into the Avaya SBCE

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.



8.3. Global Profiles

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

8.3.1. Server Interworking – Avaya Side

Server Interworking allows you 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**).
4. Select the **General** Tab:
 - a. Enter profile name: **Avaya**
 - b. Check **T38 Support** → **Yes**
 - c. All other options on the General Tab can be left at default
 - d. Select **Next**

General	
Hold Support	<input type="radio"/> None <input checked="" 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 type="radio"/> RFC3261 <input checked="" type="radio"/> RFC2543

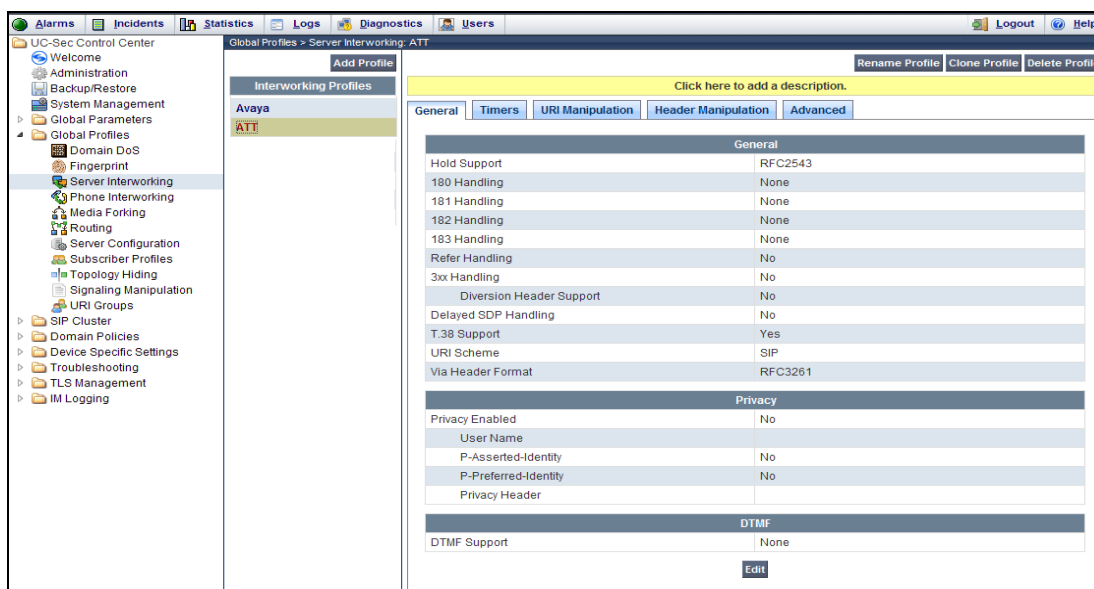
Next

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**.

8.3.2. Server Interworking – AT&T Side

Repeat the steps shown in **Section 8.3.1** 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**)
 - 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), select **Next** to accept default values.
8. Click **Finish**.

8.3.3. Routing – Avaya Side

The Routing Profile allows you to manage parameters related to routing SIP signaling messages.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select the **Routing** tab (not shown).
3. Select **Add Profile** (not shown).
4. Enter Profile Name: (e.g., **To_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**.

Routing Profile

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

Next Hop Routing

URI Group	*	
Next Hop Server 1	192.168.67.47	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

Back
Finish

8.3.4. Routing – AT&T Side

Repeat the steps in **Section 8.3.3** to add a Routing Profile for the AT&T connection.

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select the **Routing** tab.
3. Select **Add Profile**.
4. Enter Profile Name: (e.g., **To_ATT**).
5. Click **Next**, then enter the following:
 - a. **Next Hop Server 1: 135.25.29.74** (AT&T Border Element IP address)
 - b. Select **Routing Priority Based on Next Hop Server**
 - c. **Outgoing Transport: UDP**
6. Click **Finish**.

The screenshot shows a 'Routing Profile' configuration window. At the top, a yellow banner states 'Each URI group may only be used once per Routing Profile.' Below this is a 'Next Hop Routing' section. It includes a 'URI Group' dropdown menu, and two input fields for 'Next Hop Server 1' (containing '135.25.29.74') and 'Next Hop Server 2'. Below these are three checkboxes: 'Routing Priority based on Next Hop Server' (checked), 'Use Next Hop for In Dialog Messages' (unchecked), and 'Ignore Route Header for Messages Outside Dialog' (unchecked). There are also checkboxes for 'NAPTR' and 'SRV'. The 'Outgoing Transport' section has three radio buttons: 'TLS', 'TCP', and 'UDP' (selected). At the bottom are 'Back' and 'Finish' buttons.

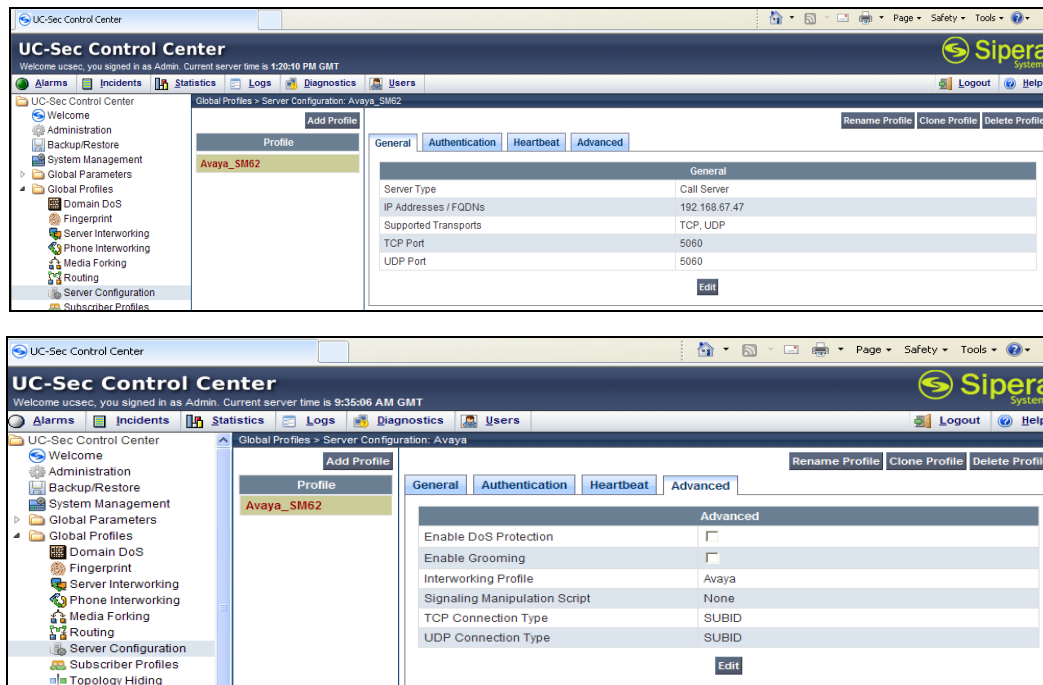
8.3.5. Server Configuration – To Avaya Aura® Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage 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**.
3. Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **Avaya_SM62**) and select **Next**.
4. The **Add Server Configuration Profile - General** window will Open (not shown).
 - a. Select Server Type: **Call Server**
 - b. **IP Address: 192.168.67.47** (Session Manager IP Address)
 - c. **Supported Transports:** Check **UDP** and **TCP**
 - d. **TCP Port: 5060**
 - e. **UDP Port: 5060**
 - f. 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 remaining default values.
7. The **Add Server Configuration Profile - Advanced** window will open.
 - a. Select **Finish** to accept remaining default values.

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



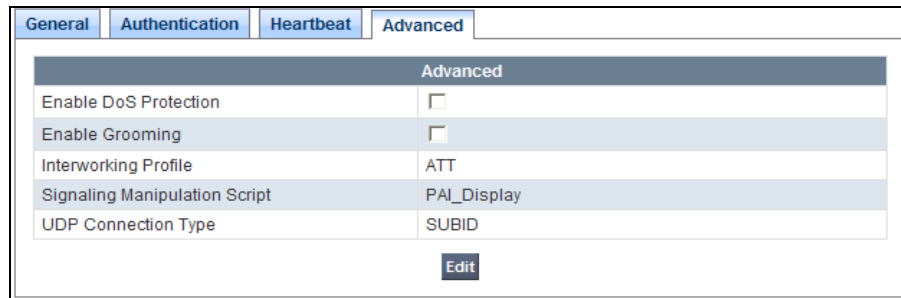
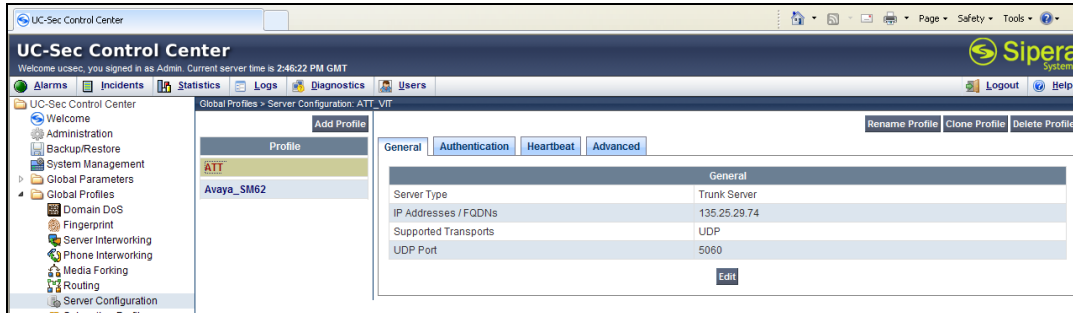
8.3.6. Server Configuration – To AT&T

Repeat the steps in **Section 8.3.5** 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: 135.25.29.74** (AT&T Border Element IP Address)
 - 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.
 - b. Select **ATT** for **Interworking Profile**.

- c. In the **Signaling Manipulation Script** field select the script defined in **Section 8.3.9, item A** (e.g., **PAI_Display**).
- a. Select **Finish**.

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

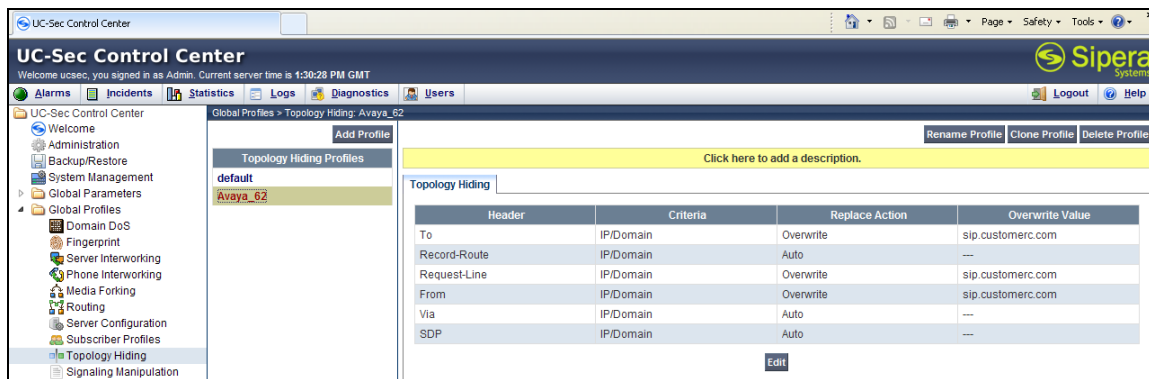


8.3.7. Topology Hiding – Avaya Side

The **Topology Hiding** screen allows you 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**).
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: **sip.customerbc.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: **sip.customerbc.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: **sip.customerbc.com**

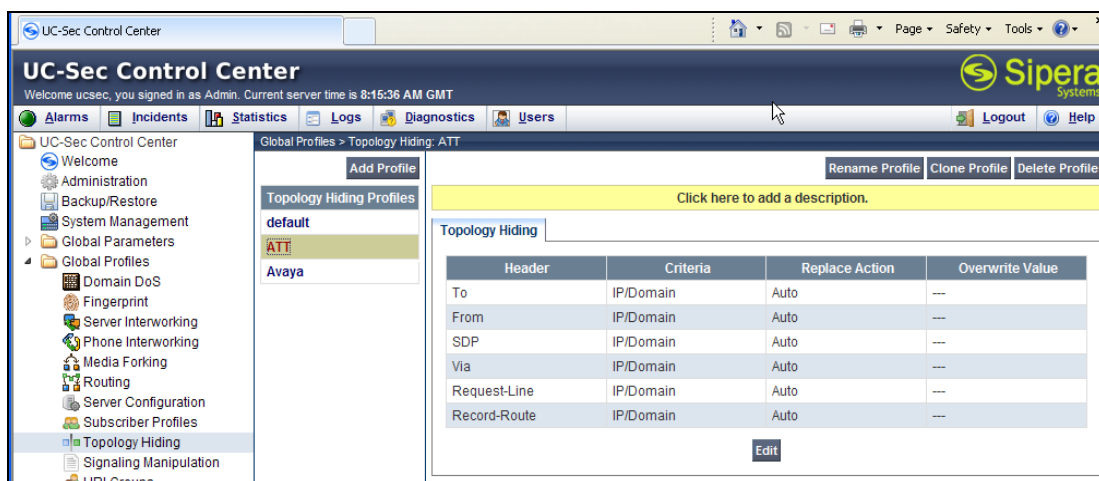
- Click **Finish** (not shown).



8.3.8. Topology Hiding – AT&T Side

Repeat the steps in **Section 8.3.7** to create a Topology Hiding Profile for the connection to AT&T.

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



8.3.9. Signaling Manipulation

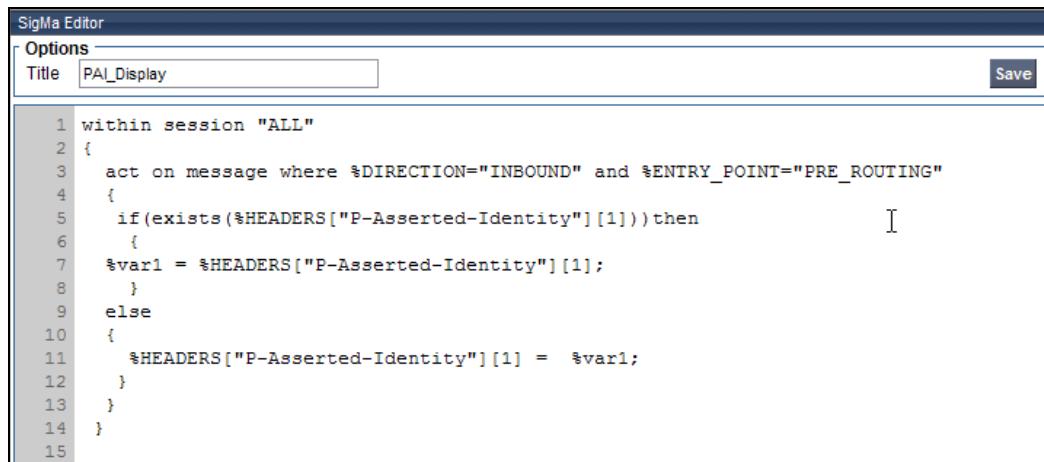
The Avaya SBCE can manipulate inbound and outbound SIP headers.

Note – Use of the Signaling Manipulation scripts require 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 8.4.3**) does not meet the desired result. Refer to [8] for information on the Avaya SBCE scripting language.

In the reference configuration two signaling manipulations were used to modify SIP headers:

Script **PAI_Display** – This script was created as a workaround for the display issue described in **item 2** of **Section 2.1.1**. It is applied to the Server Configuration **ATT** defined in **Section 7.3.6**.

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., **PAI_Display**). Note that this script will be applied to the AT&T server Configuration in **Section 8.3.6**.
5. The following script is defined:

The screenshot shows a window titled "Sigma Editor". At the top, there is an "Options" section with a "Title" field containing "PAI_Display" and a "Save" button. Below this is a text area containing a script. The script is as follows:

```
1 within session "ALL"
2 {
3   act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
4   {
5     if (exists (%HEADERS["P-Asserted-Identity"][1])) then
6     {
7       %var1 = %HEADERS["P-Asserted-Identity"][1];
8     }
9     else
10    {
11      %HEADERS["P-Asserted-Identity"][1] = %var1;
12    }
13  }
14 }
15
```

6. Click on **Save**. The script editor will test for any errors, and the editor window will close.

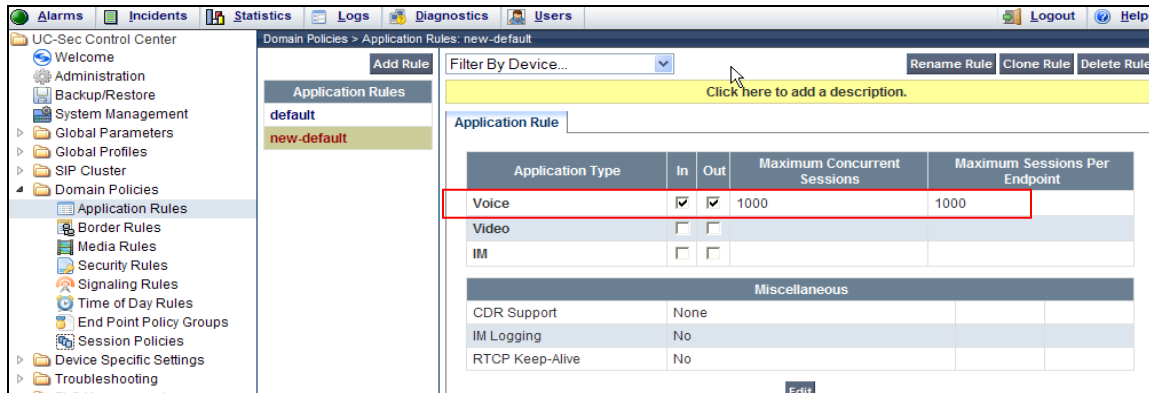
8.4. Domain Policies

The Domain Policies feature allows you to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies.

8.4.1. Application Rules

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **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:

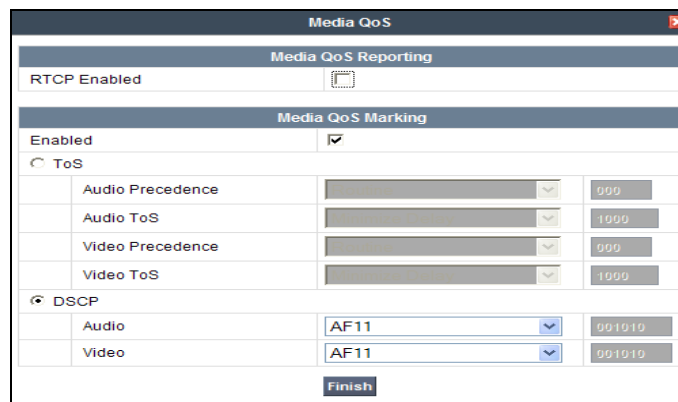
- i. Change the **Maximum Concurrent Sessions** to **1000**
- ii. Change the **Maximum Sessions per Endpoint** to **1000**



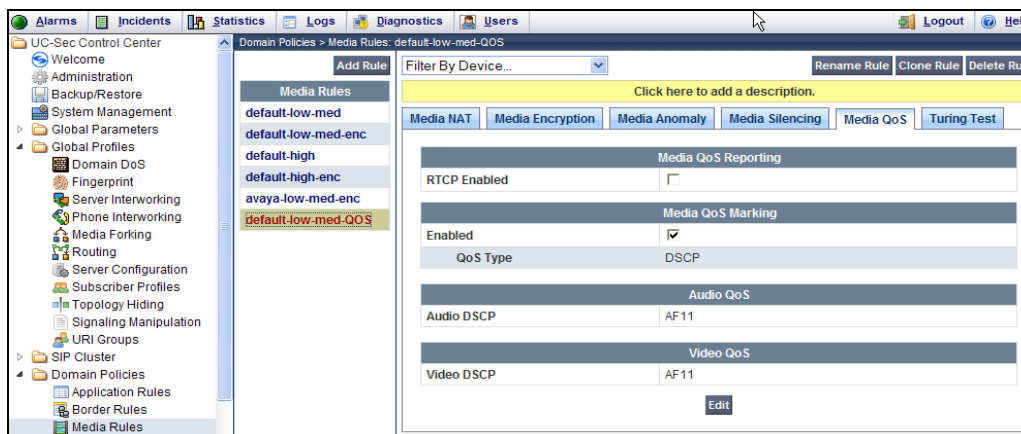
8.4.2. Media Rules

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 the **Media Rules** (not shown).
3. The Media Rules window will open (not shown). From the Media Rules menu, select the **default-low-med** rule
4. Select **Clone 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.



8.4.3. Signaling Rules

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

Note – SIP headers may be removed by the Signaling Manipulation function (see **Section 8.3.9**). However, Signaling Rules are a more efficient use of Avaya SBCE resources.

8.4.3.1 Avaya - Requests

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

Note – In configurations that include Avaya Aura® Session Manager, the History-Info header is removed by Session Manager.

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 the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. Select **Clone Rule** button
 - Enter a name: **Avaya_with_SM**
 - Click **Finish**
5. Highlight the **Avaya_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.
 - From the **Header Name** menu select **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**

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

7. Repeat **Steps 5** and **6** to create a rule to remove the **Alert-Info** header
8. Select the **Response Headers** tab (not shown).
- 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**.
9. Click **Finish**

Proprietary Request Header?	<input type="checkbox"/>
Header Name	Alert-Info
Method Name	INVITE
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional
Presence Action	Remove header 488 Busy Here
Finish	

Repeat **Steps 5** and **6** to create a rule to remove the **Endpoint-View** header

10. 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 select **Alert-Info**
 - From the **Method Name** menu select **Invite**.
 - For **Header Criteria** select **Forbidden**
 - From the **Presence Action** menu select **Remove Header**.
11. Click **Finish**

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

General Requests Responses Request Headers Response Headers Signaling QoS							
				Add In Header Control		Add Out Header Control	
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Alert-Info	INVITE	Forbidden	Remove Header	No	IN	
2	Endpoint-View	INVITE	Forbidden	Remove Header	Yes	IN	
3	P-Location	INVITE	Forbidden	Remove Header	Yes	IN	

8.4.3.2 Avaya - Responses

The following Signaling Rules remove P-Location SIP headers sent by Communication Manager SIP responses (e.g., 1xx or 200OK) that are not required by AT&T.

Note – In configurations that include Avaya Aura® Session Manager, the History-Info header is removed by Session Manager.

The following steps remove the P-Location header from 1xx responses:

1. Highlight the **Avaya_with_SM** rule created in **Section 8.4.3.1** 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.
 - From the **Header Name** menu select **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**.
2. Click **Finish**

Repeat Steps 1 and 2 to create a rule to remove the P-Location header from 200 responses.

3. Select the **Response Headers** tab (not shown).
 - 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 select **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**.
4. Click **Finish**

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

Edit Header Control								
<div> <div>General</div> <div>Requests</div> <div>Responses</div> <div>Request Headers</div> <div>Response Headers</div> <div>Signaling QoS</div> </div> <div> <div>Add In Header Control</div> <div>Add Out Header Control</div> </div>								
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
1	P-Location	1XX	INVITE	Forbidden	Remove Header	Yes	IN	
2	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN	

8.4.3.3 Avaya – Signaling QoS

1. Highlight the **Avaya_with_SM** rule created in **Section 8.4.3.1** and enter the following:
 - Select the **Signaling QoS** tab (not shown).
 - Click the **Edit** button and the **Signaling QoS** window will open.
 - Select **DCSP**.
 - Select **Value = AF11**.
2. Click **Finish**

The screenshot shows the 'Signaling QoS' configuration window. It has a title bar with 'Signaling QoS' and a close button. The window is divided into sections. The first section is 'Enabled' with a checked checkbox. Below that is a radio button for 'ToS'. The next section is 'DSCP' with a radio button selected. Under 'DSCP', there is a 'Value' dropdown menu set to 'AF11' and a corresponding text box showing '001010'. At the bottom right is a 'Finish' button.

8.4.3.4 AT&T - Requests

AT&T sends Invites containing the Resource-Priority header which is not supported by Communication Manager (see **Section 2.2.1, item 4**). Follow the steps shown in **Section 8.4.3.1** with the following changes:

1. Select **Clone Rule** button
 - Enter a name: **ATT**
 - Click **Finish**
2. Highlight the **ATT** rule just created in **Step 1** and enter the following:
 - Select the **Request Headers** tab (not shown).
 - 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 **Resource-Priority**
 - From the **Method Name** menu select **Invite**.
 - For **Header Criteria** select **Forbidden**.
 - From the **Presence Action** menu select **Remove Header**.
3. Click **Finish**

The screenshot shows the 'Edit Header Control' window. It has a title bar with 'Edit Header Control' and a close button. The window contains several fields: 'Proprietary Request Header?' with an unchecked checkbox, 'Header Name' with a dropdown menu set to 'Resource-Priority', 'Method Name' with a dropdown menu set to 'INVITE', 'Header Criteria' with radio buttons where 'Forbidden' is selected, and 'Presence Action' with a dropdown menu set to 'Remove header' and a text box showing '426' and 'Busy Here'. At the bottom right is a 'Finish' button.

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	Resource-Priority	INVITE	Forbidden	Remove Header	No	IN		

Note – No Response Header manipulation is required.

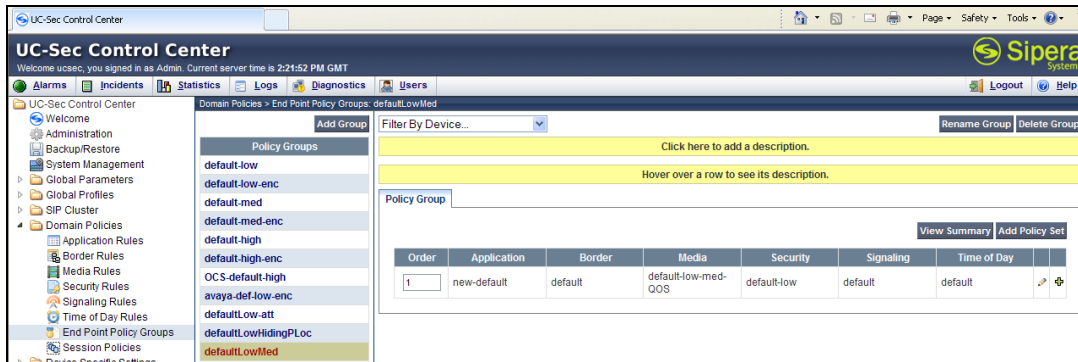
8.4.3.5 AT&T – Signaling QoS

- Highlight the **ATT** rule created in **Section 8.4.3.4** and enter the following:
 - Select the **Signaling QOS** tab (not shown).
 - Click the **Edit** button and the **Signaling QOS** window will open.
 - Select **DCSP**.
 - Select **Value = AF11**.
- Click **Finish**

Signaling QoS			
Enabled		<input checked="" type="checkbox"/>	
<input type="radio"/> ToS			
Precedence			000
ToS			1000
<input checked="" type="radio"/> DSCP			
Value	AF11		001010
<input type="button" value="Finish"/>			

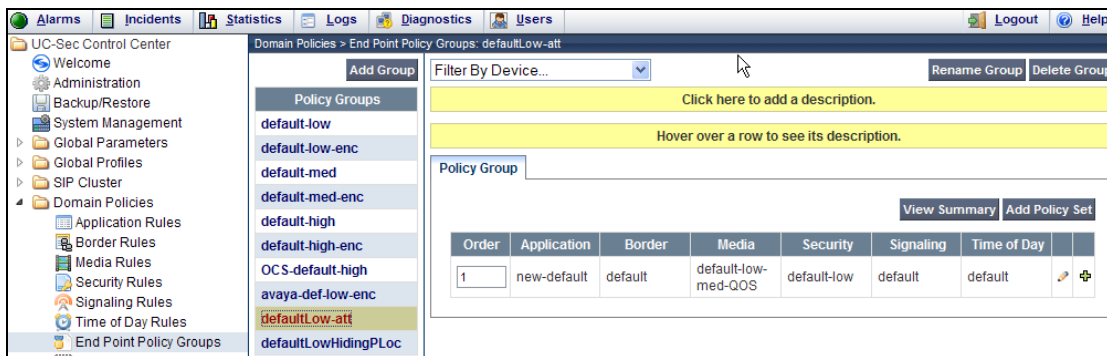
8.4.4. Endpoint Policy Groups – Avaya

- Select **Domain Policies** from the menu on the left-hand side
- Select **End Point Policy Groups**
- Select **Add Group**
 - Name: defaultLowMed**
 - Application Rule: new-default**
 - Border Rule: default**
 - Media Rule: default-low-med-QOS**
 - Security Rule: default-low**
 - Signaling Rule: default**
 - Time of Day: default**
- Select **Finish** (not shown)



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



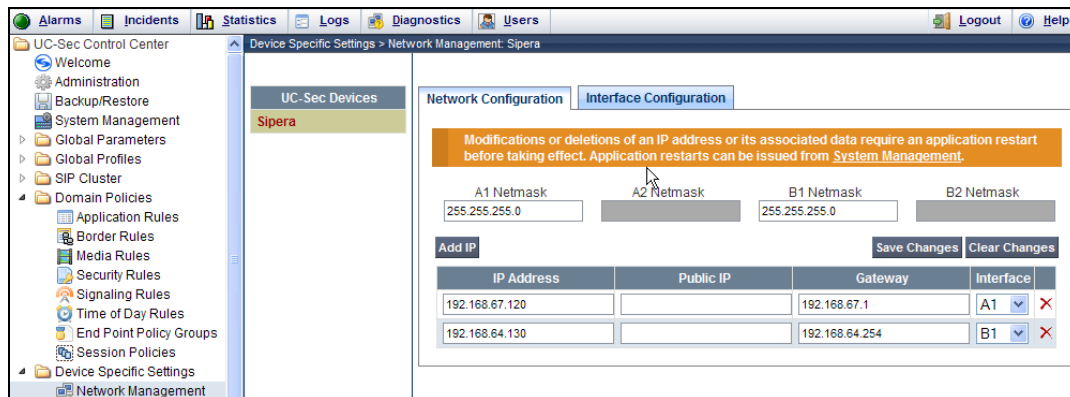
8.5. Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view system information, and manage various device-specific network parameters. Specifically, you have the 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.

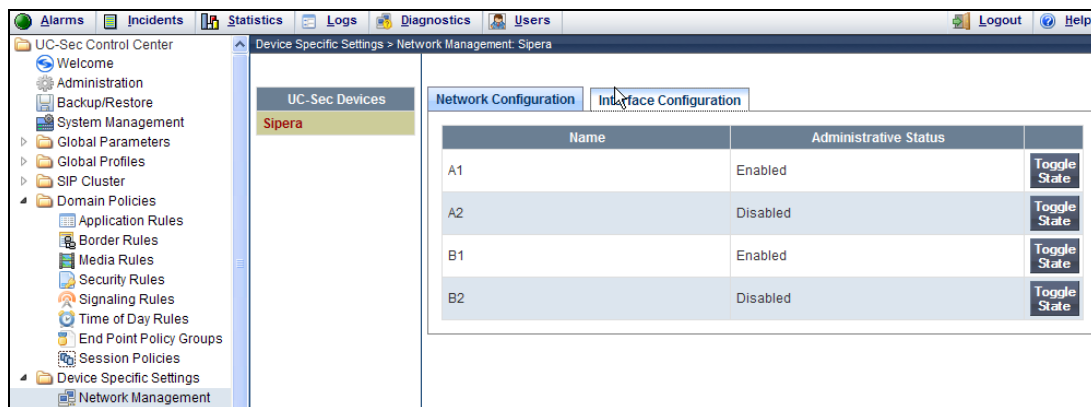
8.5.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**

- a) The network interfaces were provisioned in **Section 8.3**. 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.

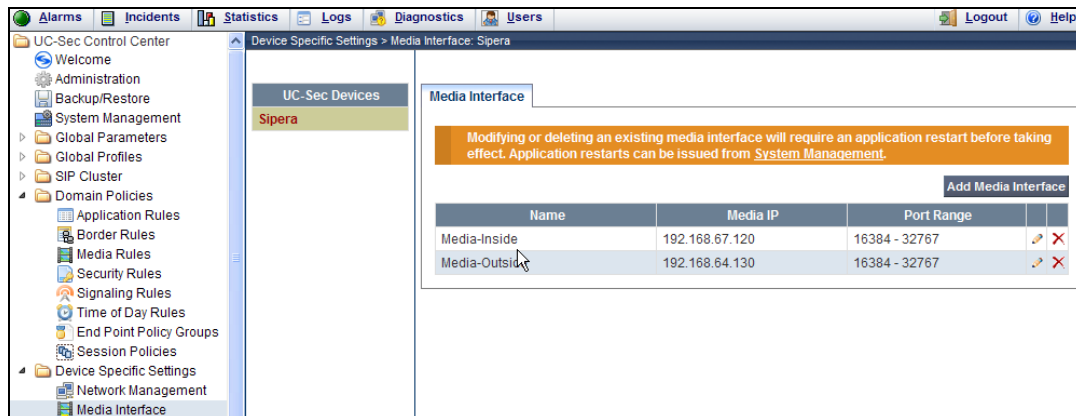


8.5.2. Media Interfaces

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 required by AT&T.

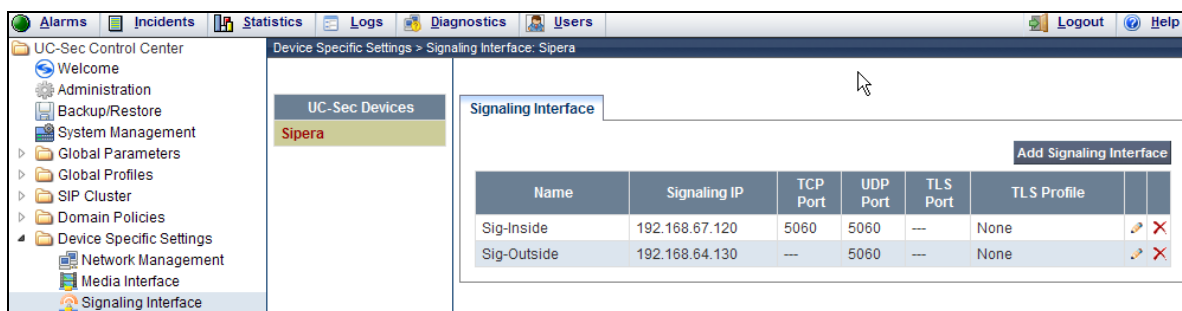
1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Media Interface**
3. Select **Add Media Interface**
 - a) **Name: Media-Inside**
 - b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Session Manager)
 - c) **Port Range: 16384 - 32767**
4. Click **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)



8.5.3. 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**



8.5.4. Endpoint Flows – To 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_SM**
 - b) **Server Configuration: Avaya_SM62**
 - 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: defaultLowMed**
 - j) **Routing Profile: To_ATT**
 - k) **Topology Hiding Profile: Avaya**
 - l) **File Transfer Profile: None**
5. Click **Finish** (not shown)

8.5.5. 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**
 - 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**
 - j) **Routing Profile: To_Avaya**
 - k) **Topology Hiding Profile: ATT**
 - l) **File Transfer Profile: None**
5. Click **Finish** (not shown)

The screenshot shows the UC-Sec Control Center interface. The left-hand side contains a navigation tree with 'Device Specific Settings' expanded, showing 'End Point Flows' selected. The main area displays the 'Server Flows' tab for 'Sipera'. Below this, there are two tables showing server configurations for 'ATT' and 'Avaya_SM62'.

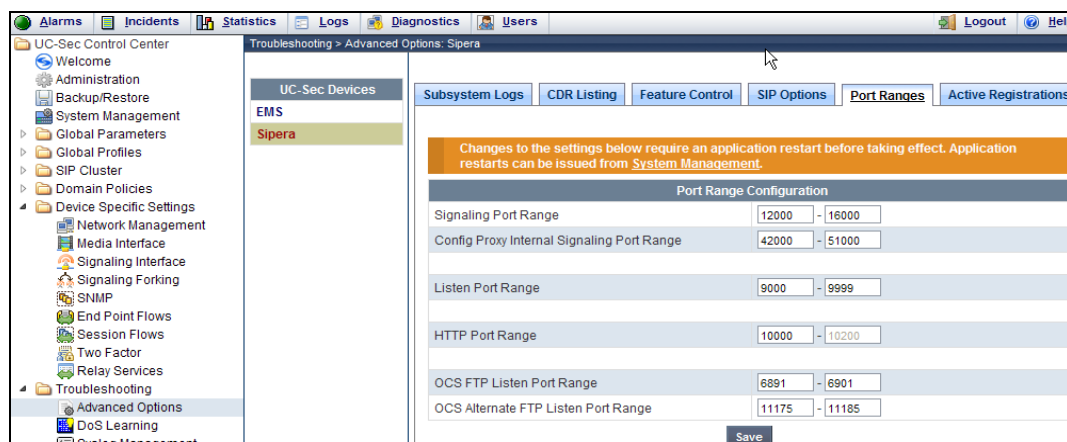
Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	ATT	*	*	*	Sig-Inside	Sig-Outside	Media-Outside	defaultLow-att	Avaya_SM62	ATT	None			

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_SM_62	*	*	*	Sig-Outside	Sig-Inside	Media-Inside	defaultLowMed	ATT	Avaya	None			

8.6. 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 8.5.2).

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**



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 disconnects 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 a telephone, 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. 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] and [6] for more information.

- 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., *04). Note that Session Manager has previously converted the IPFR-EF DNIS number included in the Request URI, to the Communication Manager extension 19011, before sending the INVITE to Communication Manager.

```
list trace tac *04                                     Page 1
LIST TRACE
time      data
09:05:40 TRACE STARTED 07/25/2012 CM Release String cold-02.0.823.0-19593
09:05:47 SIP<INVITE sip:19011@sip.customerc.com SIP/2.0
09:05:47      Call-ID: BW130643036250712257513136@invisibleAS1
09:05:47      active trunk-group 4 member 1      cid 0x23
09:05:47      dial 19011
09:05:47      term station      19011 cid 0x23
09:05:47 SIP>INVITE sip:19011@sip.customerc.com SIP/2.0
09:05:47      Call-ID: 80e4856993d8e119955015459f00
09:05:47 SIP<SIP/2.0 100 Trying
09:05:47      Call-ID: 80e4856993d8e119955015459f00
09:05:47 SIP>INVITE sip:19011@sip.customerc.com SIP/2.0
09:05:47      Call-ID: 80e4856993d8e119955015459f00
09:05:47 SIP>SIP/2.0 100 Trying
09:05:47      Call-ID: 80e4856993d8e119955015459f00
09:05:47 SIP>SIP/2.0 180 Ringing
09:05:47      Call-ID: BW130643036250712257513136@invisibleAS1
09:05:47      G729B ss:off ps:30
09:05:47      rgn:2 [192.168.67.120]:17268
09:05:47      rgn:1 [192.168.67.50]:16398
09:05:47      xoip options: fax:T38 modem:off tty:US uid:0x50001
09:05:47      xoip ip: [192.168.67.50]:16398
09:05:50 SIP>SIP/2.0 200 OK
09:05:50      Call-ID: 80e4856993d8e119955015459f00
09:05:50 SIP<SIP/2.0 200 OK
09:05:50      Call-ID: 80e4856993d8e119955015459f00
09:05:50 SIP>ACK sip:19011@192.168.67.75:5061;transport=tls;epv=%3cs
```

- 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

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 Release 6.2 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Session Manager** (not shown).

Step 2 - Expand System Status → SIP Entity Monitoring.

The screenshot displays the Avaya Aura Session Manager GUI. The left sidebar contains a navigation menu with options: Session Manager, Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, System Tools, and Performance. The main content area is titled 'SIP Entity Link Monitoring Status Summary' and includes a 'Run Monitor' button. Below this is a table with the following data:

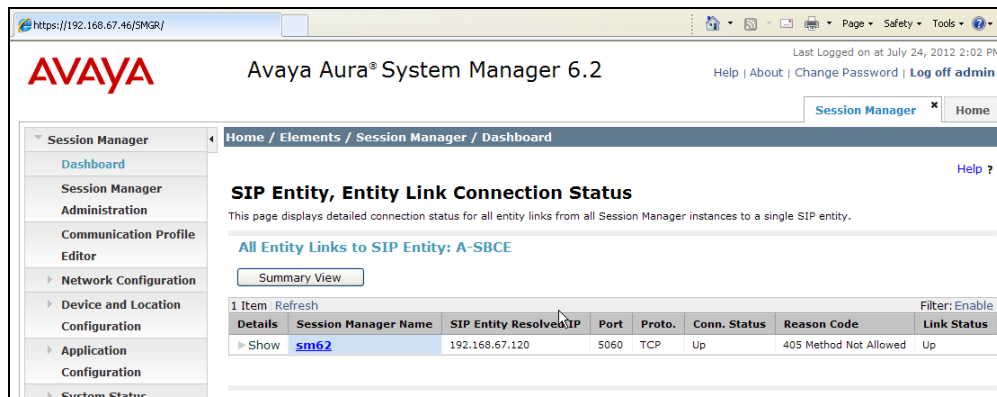
Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
sm62	0/4	0	0	0

Below the table is a 'Select : All, None' dropdown. Further down, there is a section titled 'All Monitored SIP Entities' with another 'Run Monitor' button. This section includes a 'Refresh' button, a 'Show ALL' dropdown, and a 'Filter: Enable' button. The table below this section lists the following entities:

SIP Entity Name
A-SBCE
AA-M
ACM62_Local
ACM62_Public

At the bottom of this section is a 'Select : All, None' dropdown.

Step 3 - From the list of monitored entities, select an entity of interest, such as **A-SBCE**. Under normal operating conditions, the **Link Status** should be **Up** as shown in the example screen below. The **Reason Code** column indicates that Session Manager has received a **SIP 405 Method Not Allowed** response (normal for the Avaya SBCE to AT&T test environment) to the SIP OPTIONS it generated. This response is sufficient for SIP Link Monitoring to consider the link up. Note that the Avaya SBCE sends the Session Manager generated OPTIONS on to the AT&T Border Element, and it is the 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 7325554037 and Session Manager converts this to Communication Manager extension 19011 before routing the call.

- Step 1 – Called Party URI** field = the information passed in the Request URI sent by the Avaya SBCE (e.g., 7325554037@sip.customerc.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 (if multiple ones are defined).
- 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

Called Party URI
7325554037@sip.customerc.com

Calling Party URI
7325551000@sip.customerc.com

Day Of Week
Wednesday

Called Session Manager Instance
sm62

Time (UTC)
13:36

Calling Party Address
192.168.67.120

Session Manager Listen Port
5060

Transport Protocol
TCP

Execute Test

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 7325554037 in the Request URI, is sent to Communication Manager extension 19011. 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:19011@sip.customermerc.com > to SIP Entity ACM62_Public (192.168.67.44). Terminating Location is ACM62.
Routing Decision Process
NRP Adaptations: ACM62 applied.
BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.
Conference Factory Well-Known URIs: No matches for uri < 7325554037@sip.customermerc.com >.
Originating Location is A-SBCE. Using digits < 7325554037 > and host < sip.customermerc.com > for routing.
NRP Dial Patterns: No matches for digits < 7325554037 > and domain < sip.customermerc.com >.
NRP Dial Patterns: No matches for digits < 7325554037 > and domain < customermerc.com >.
NRP Dial Patterns: Found a Dial Pattern match for pattern < 732555 > Min/Max length 10/10 and domain < null >.
NRP Routing Policies: Ranked destination NRP SIP Entities: ACM62_Public.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP SIP Entities: ACM62_Public.
NRP Dial Patterns: Checking NRP Dial Patterns that specify -ALL- NRP Locations.
NRP Dial Patterns: No matches for digits < 7325554037 > and domain < sip.customermerc.com >.
NRP Dial Patterns: No matches for digits < 7325554037 > and domain < customermerc.com >.
NRP Dial Patterns: No matches for digits < 7325554037 > and domain < null >.
NRP Dial Patterns: Chose route matching pattern 732555
END EMERGENCY CALL CHECK: This is not an emergency call.
Adapting and proxying for SIP Entity ACM62_Public.
NRP Entity Links: Found direct link to destination. Link uses TCP to port 5060.
NRP Adaptations: ACM62 applied.
NRP Adaptations: Request-URI set to sip:19011@sip.customermerc.com
NRP Adaptations: Request URI set to sip:19011@sip.customermerc.com
Route < sip:19011@sip.customermerc.com > to SIP Entity ACM62_Public (192.168.67.44). Terminating Location is ACM62.

9.4. Protocol Traces

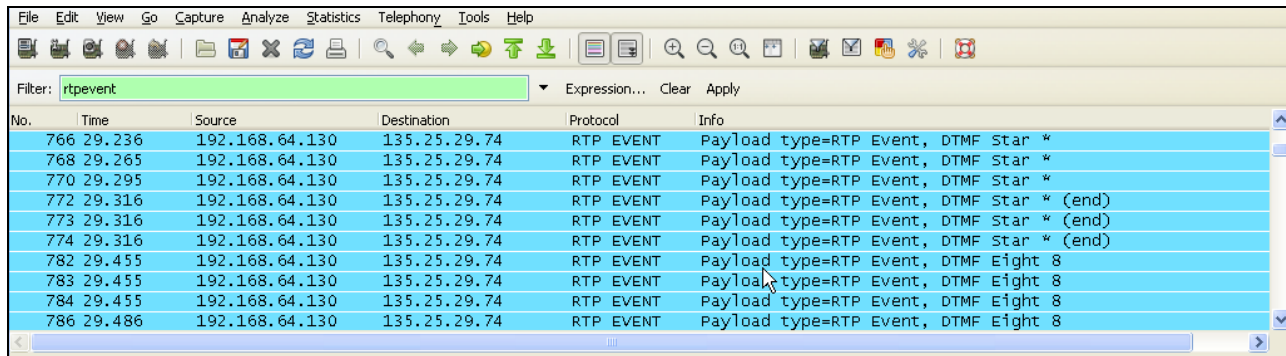
9.4.1. AT&T IP Flexible Reach – Enhanced Features

Using a SIP protocol analyzer (e.g., Wireshark), monitor the SIP traffic at the Avaya SBCE public outside interface connection to the IPFR-EF service. Traces taken at the Avaya SBCE inside interface are also helpful in verifying correct sip header manipulations.

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

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=

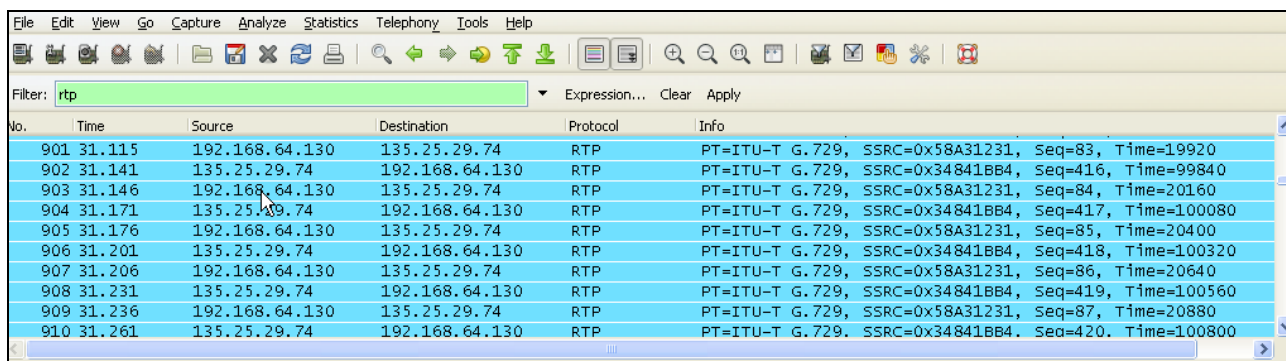
The following is an example of a call filtering on DTMF.



Filter: `rtpevent` Expression... Clear Apply

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 filtering on RTP.



Filter: `rtp` Expression... Clear Apply

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

The following traces show an example of the IPFR-EF Network Based Blind Transfer with Refer (Communication Manager Vector) based on the configuration shown in **Appendix2**.

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.

The network responds to the *Refer* with *202 Accepted* in frame 119, and terminates the original inbound call in frame 120.

Filter: sip					
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=80ee188cfd7e11bf574fec324500					
To: <sip:7325551000@135.25.29.74;user=phone>;tag=1543067091-1342552043577-					
CSeq: 1 REFER					
Call-ID: Bw190723577170712606096938@invisibleAS1					
Contact: "REFER" <sip:44010@192.168.64.130:5060>					
Record-Route: <sip:192.168.64.130:5060;ipcs-line=10402;tr;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					

Verify that your Sip Trunk from the Avaya SBCE (192.168.64.130) to the IPFR-EF Service (135.25.29.74) is up and communicating with SIP *OPTIONS* messages and response messages. A SIP *405 Method Not Allowed* response is normal for the Avaya SBCE to AT&T test environment. If AT&T sends *OPTIONS*, the typical CPE response will be *200 OK*.

Filter: sip					
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

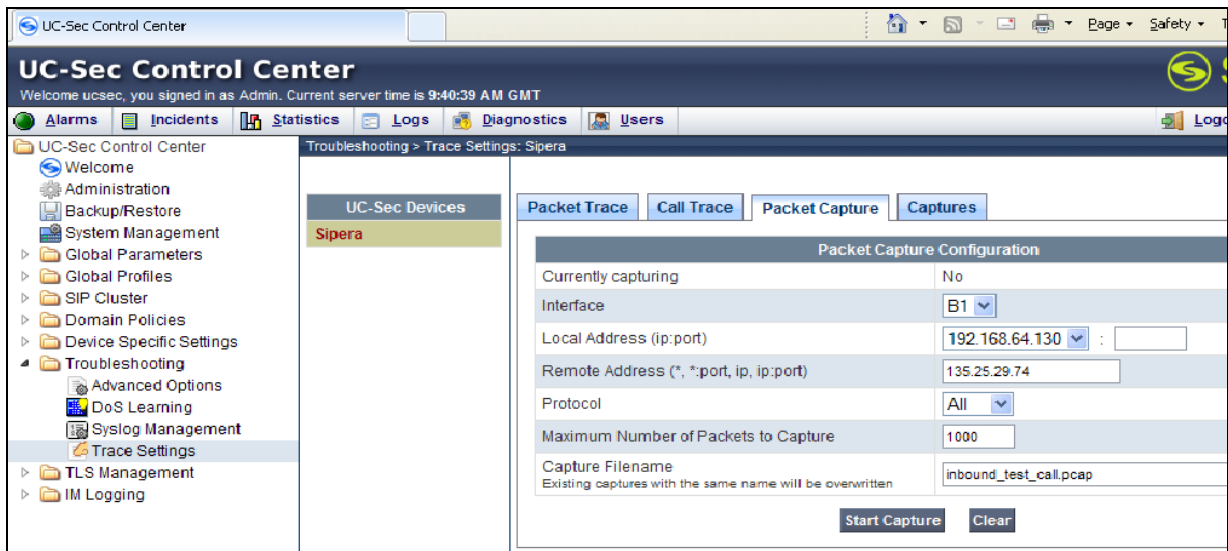
9.5. Avaya Session Border Controller for Enterprise Verification

The Avaya SBCE can take internal traces of specified interfaces.

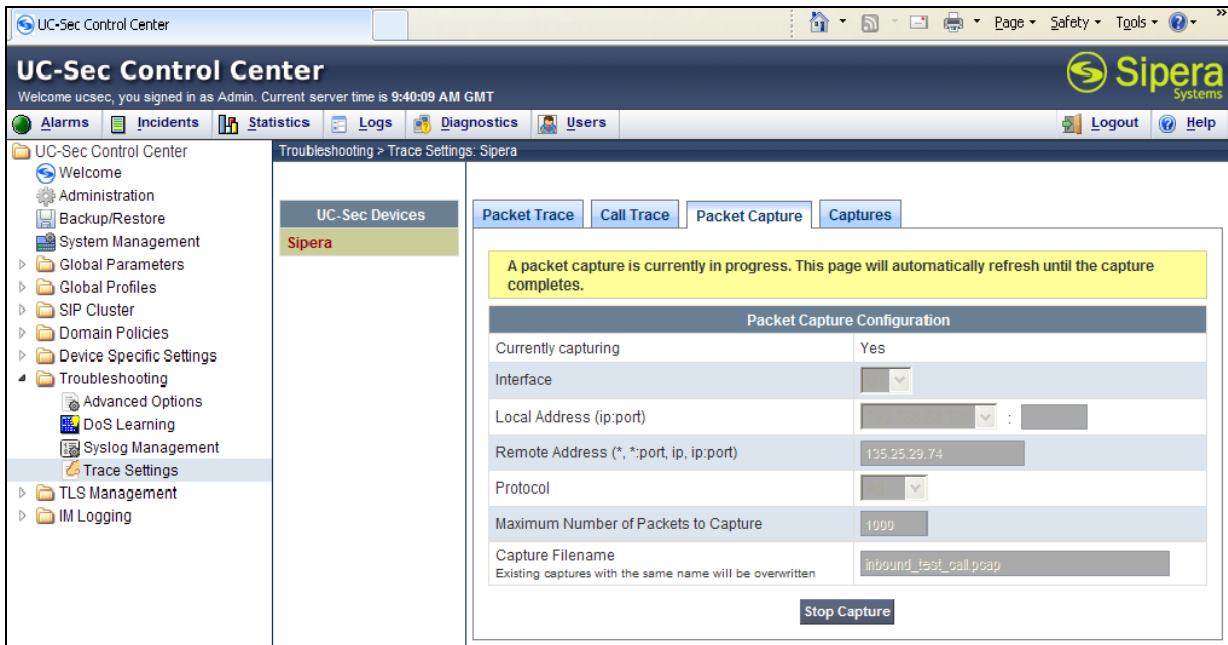
Step 1 - Navigate to UC-Sec Control Centre → Troubleshooting → Trace Settings

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:

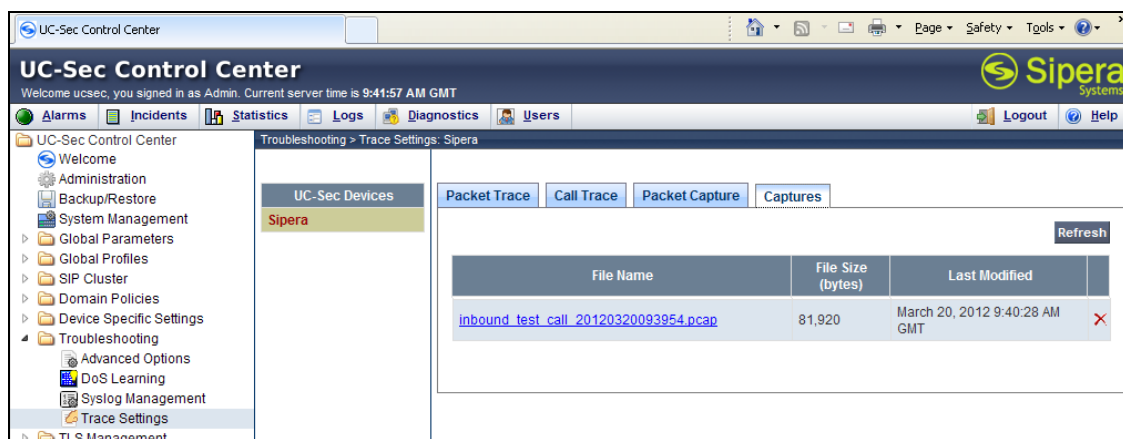


Step 3 – Run the test.

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 an application such as Wireshark to open the trace.



10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Avaya Session Border Controller for Enterprise (Avaya SBCE) can be configured to interoperate successfully with the AT&T IP Flexible Reach – Enhanced Features service, within the constraints described in **Section 2.1.1**.

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. *Implementing Avaya Aura® Session Manager*, 03-603473, Release 6.2, July 2012
2. *Implementing Avaya Aura® Session Manager*, 03-603473, Release 6.2, July 2012
3. *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Issue 4, May 2011
4. *Administering Avaya Aura® System Manager*, Document Number 03-603324, June 2010

Avaya Aura® Communication Manager

5. *Administering Avaya Aura® Communication Manager* Release 6.2, 03-300509, Issue 7.0, July 2012
6. *Implementing Avaya Aura® Communication Manager*, 03-603558, Issue 3, Release 6.2, July 2012
7. *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya Aura® Messaging

8. *Administering Avaya Aura® Messaging 6.1*, CID: 151610, December 2011
9. *Implementing Avaya Aura® Messaging 6.1*, CID: 150976, October 2011

Avaya Session Border Controller for Enterprise

10. Product documentation for UC-Sec can be obtained from Sipera using the link at <http://www.sipera.com>
11. *E-SBC IU Installation Guide, Release 4.0.5*, Part Number: 101-5225-405v1.00, Release Date: November 2011
12. *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:

13. 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/>

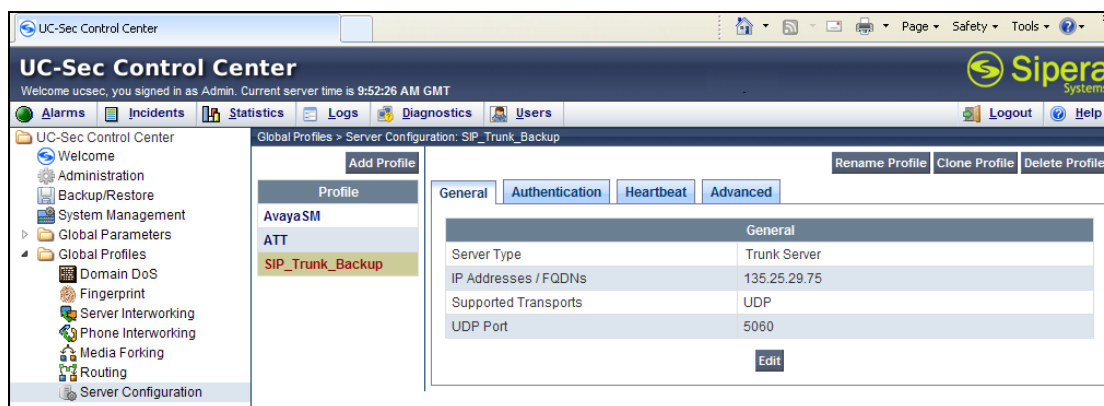
12. Addendum 1 – Redundancy to Multiple AT&T Border Elements

AT&T may provide multiple network border elements for redundancy purposes. The Avaya SBCE can be provisioned to support this redundant configuration.

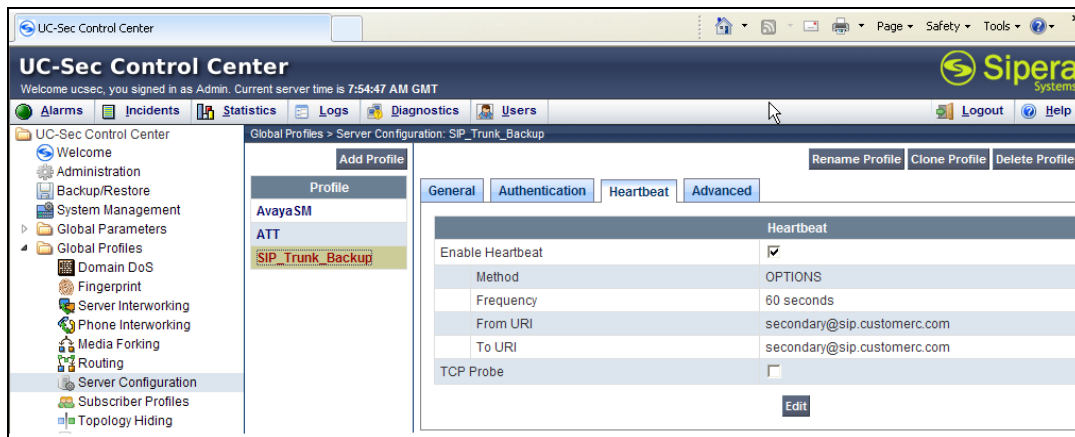
Given two AT&T border elements **135.25.29.74** and **135.25.29.75**, the Avaya SBCE is provisioned as follows to include the backup trunk connection to 135.25.29.75 (the primary AT&T trunk connection to 135.25.29.74 is defined in **Section 8.3.6**).

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

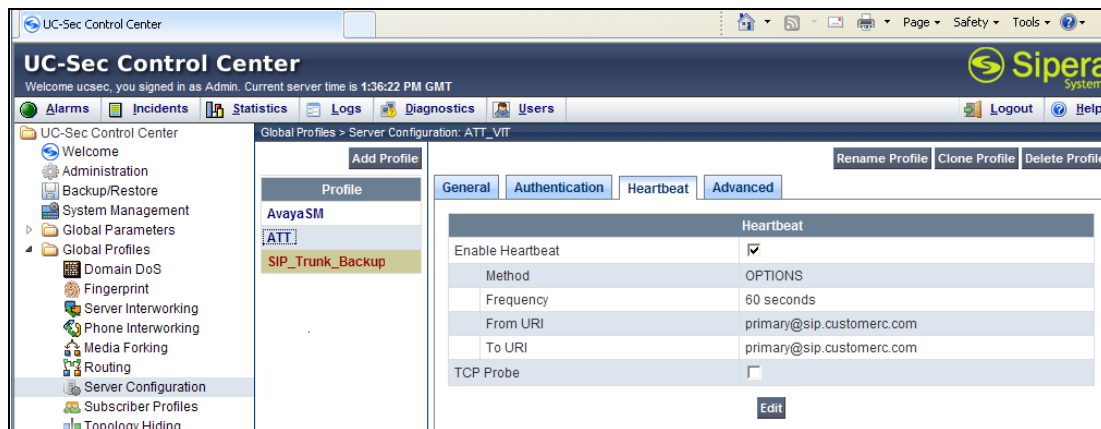
1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**
 - a) **Name: SIP_Trunk_backup**
4. On the **Add Server Configuration Profile – General** tab:
 - a) Select **Server Type: Trunk Server**
 - b) **IP Address: 135.25.29.75** (Example Address for a secondary location)
 - c) **Supported Transports: Check UDP**
 - d) **UDP Port: 5060**
 - e) Select **Next** (not shown)



5. On the **Authentication** tab
 - a) Select **Next** (not shown)
6. On the **Heartbeat** tab (The Heartbeat must be enabled on the Primary trunk also)
 - a) Check **Enable Heartbeat**
 - b) **Method: OPTIONS**
 - c) **Frequency: 60 seconds**
 - d) **From URI: secondary@sip.customer.com**
 - e) **To URI: secondary@sip.customer.com**
 - f) Select **Next** (not shown)



7. On the **Advanced** Tab
 - a) Click **Finish** (not shown)
8. Select the Trunk created in **Section 8.4.6** (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 the **Routing**
3. Select the profile created in **Section 8.4.4** (e.g., **To_ATT**)
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., **135.25.29.75**)
5. Click **Finish**

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

Next Hop Routing

URI Group: *

Next Hop Server 1: 135.25.29.74 IP, IP:Port, Domain, or Domain:Port

Next Hop Server 2: 135.25.29.75 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

12.3. Step 3: Configure End Point Flows – SIP_Trunk_backup

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: Backup**
 - b) **Server Configuration: SIP_Trunk_Backup**
 - 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**
 - j) **Routing Profile: To_Avaya**
 - k) **Topology Hiding Profile: ATT**
 - l) **File Transfer Profile: None**
5. Click **Finish**

Criteria	
Flow Name	Backup
Server Configuration	SIP_Trunk_Backup
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
File Transfer Profile	None
<div>Finish</div>	

When completed the Avaya SBCE will issue OPTIONS messages to the primary (135.25.29.74) and secondary (135.25.29.75) border elements.

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

As described in **Section 2.2.1**, an issue with the use of Communication Manager Network Call Redirection (NCR) Refer processing for call redirection (IPFR-EF blind transfer feature) was found. 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.

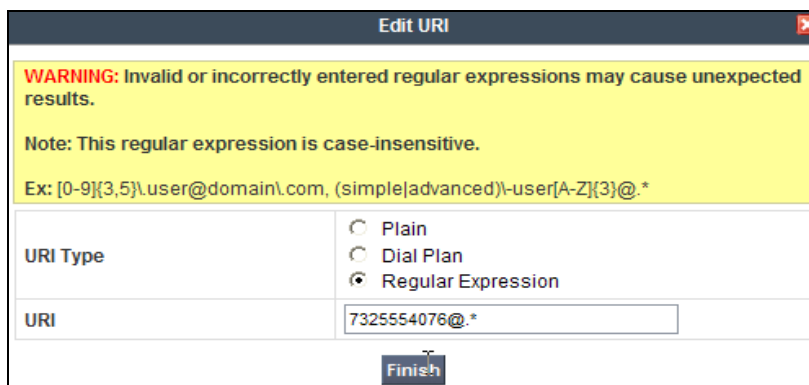
A workaround for this issue is to provision a dedicated SIP trunk, with NCR enabled, used only for Refer based IPFR-EF blind transfer feature. The provisioning for this access is performed on the Avaya SBCE, Session Manager, and on Communication Manager. Note that specific AT&T IP Flexible Reach - Enhanced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

13.1. Configure Avaya Session Border Controller

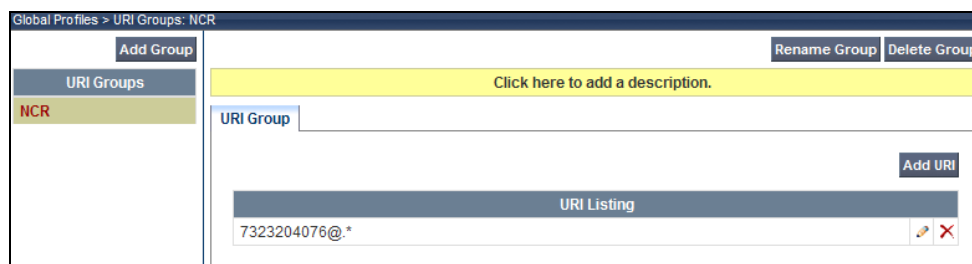
13.1.1. Create URI Group

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

- Enter a URI Group name (e.g. **NCR**) and the **Edit URI** window will open. Enter the following:
 - For **URI Type** select **Regular Expression**
 - In the **URI** field enter **xxxxxxxxxx@.*** where xxxxxxxxxxxx is the inbound AT&T IP Flexible Reach - Enhanced Features service DNIS number selected for IPFR-EF blind transfer feature access (e.g., **7325554076@.***)

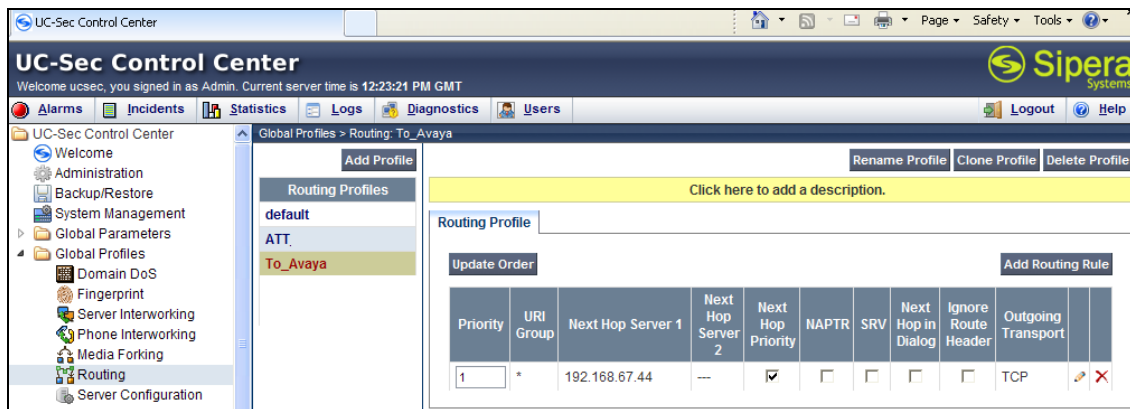


- Click on **Finish**.



13.1.2. Routing

Step 1 – Navigate to **Global Profiles → Routing**, and select the Routing Profile created in **Section 8.3.3** (e.g., **To_Avaya**).



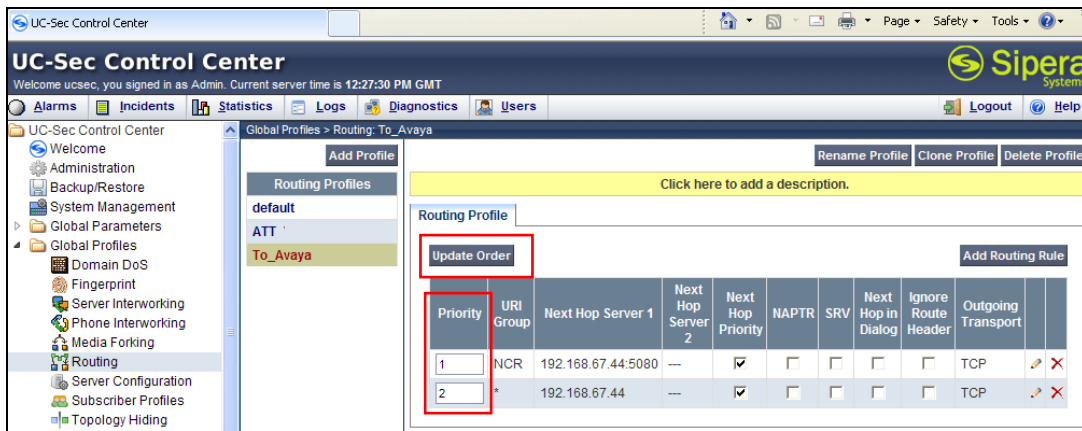
Step 2 – Click on the **Add Routing Rule** button and enter the following:

- 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 **xx.xx.xx.xx:5080** where xx.xx.xx.xx is the IP address used to create the Communication Manager IPFR-EF blind transfer feature SIP trunk Signaling Group in **Section 13.3.1** (e.g., **192.168.67.44:5080**)
- Leave the **Routing Priority Based on Next Hop Server** and **TCP** options checked (default).
- Click on **Finish**.

The 'Edit Routing Rule' dialog box is shown. It has a yellow warning banner: 'Each URI group may only be used once per Routing Profile.' The 'Next Hop Routing' section is expanded. Fields include: URI Group (dropdown with 'NCR' selected), Next Hop Server 1 (text field with '192.168.67.44:5080' and a red border), and Next Hop Server 2 (empty text field). Below these are checkboxes: 'Routing Priority based on Next Hop Server' (checked), 'Use Next Hop for In Dialog Messages' (unchecked), and 'Ignore Route Header for Messages Outside Dialog' (unchecked). There are also checkboxes for 'NAPTR' and 'SRV'. The 'Outgoing Transport' section has radio buttons for 'TLS', 'TCP' (selected), and 'UDP'. A 'Finish' button is at the bottom.

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.



Therefore, if the Request URI digit string on an inbound call matches the defined string in the “NCR” URI Group, the Avaya SBCE will send the call to the Communication Manager IP address using port 5080 (SIP trunk 5, with NCR *enabled*, defined in **Section 13.3.1**).

If there is no match, then the “*” URI Group is used and the call is sent to Communication Manager IP address using port 5060 (SIP trunk 4, with NCR *disabled*, defined in **Section 5.7.1**).

13.1.3. Signaling Manipulation

As mentioned in **Section 2.2.1, item 1**, when Communication Manager Network Call Redirection (NCR) is enabled, Communication Manager uses SendOnly SIP signaling to indicate Hold conditions. The Broadsoft responds to this with Inactive (instead of RecOnly). Therefore when Communication Manager sends Music On Hold, the network does not send the audio and PSTN hears nothing. Therefore a SIP header manipulation must be added to the Avaya SBCE to change SendOnly to SendRecv when NCR is enabled.

Following the procedures shown in **Section 8.3.9**, enter the following:

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

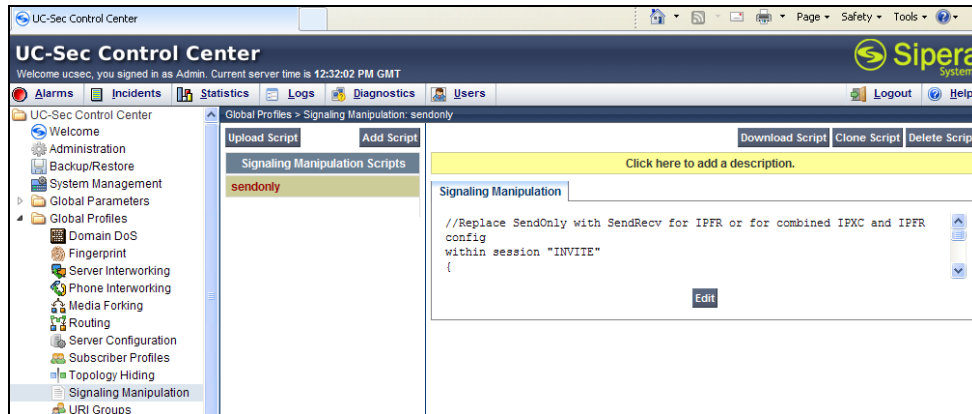
```

SigMa Editor
Options
Title sendonly Save

1 //Replace SendOnly with SendRecv for IPFR
2 within session "INVITE"
3 {
4
5   act on request where $DIRECTION="INBOUND" and $ENTRY_POINT="PRE_ROUTING"
6
7   {
8
9     $BODY[1].regex_replace( "a=sendonly","a=sendrecv");
10
11   }
12 }
13

```

- Click on **Save**. The script editor will test for any errors, and the editor window will close.



- Select **Global Profiles** → **Server Configuration** (not shown), and select the **Avaya_SM** profile created in **Section 8.3.5**.
- Select the **Advanced** tab (not shown) and click on **Edit**.
- In the **Signaling Manipulation Script** field select the **sendonly** script defined in **Step 4** above.
- Click on **Finish**.

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 (e.g., **ACM62_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., **ACM62_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=sip.customerc.com**
osrcd=sip.customerc.com.
- Enter any desired notes.

Adaptation Details

CommitCancel

General

* Adaptation name:ACM62_NCR

Module name:DigitConversionAdapter

Module parameter:odstd=sip.customerc.com osrcd=sip.customerc.com

Egress URI Parameters:

Notes:To NCR Trunk

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

- Enter a AT&T DNIS number chosen specifically for access to the NCR enabled trunk in the **Matching Pattern** column (e.g., **7325554076**).
- Enter **10** in the **Min/Max** columns.
- Enter **10** in the **Delete Digits** column.
- Enter **19999** in the **Insert Digits** column. Note that this is the extension of the Vector Directory Number (VDN) defined in **Section 13.2.2**.
- 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

AddRemove

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

AddRemove

1 Item Refresh

Filter: Enable

	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*7325554076	*10	*10		*10	19999	destination		

Select : All, None

* Input Required

CommitCancel

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. **ACM62_NCR**).
- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.3** (e.g. **192.168.67.44**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation administered in **Section 13.1.1**.
- **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 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**.

Note – The **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 13.1.3**.

The screenshot shows the 'SIP Entity Details' form with the 'General' tab selected. The form contains the following fields and values:

- Name:** ACM62_NCR
- FQDN or IP Address:** 192.168.67.44
- Type:** CM (dropdown menu)
- Notes:** To ACM NCR trunk
- Adaptation:** ACM62_NCR (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:** egress (dropdown menu)
- 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)

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

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., **ACM62_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 **5062**.
- **Protocol** – Select **TLS** (see the note in **Section 5.4** regarding the use of TLS in the reference configuration).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 13.4.2** for the Communication Manager NCR trunk entity.
- **SIP Entity 2 Port** - Enter **5062**.
- **Connection Policy** – Select **Trusted**.
- Enter any desired notes.

Step 3 - Click on **Commit**.

The screenshot shows the 'Entity Links' configuration page. At the top right are 'Commit' and 'Cancel' buttons. Below is a table with the following data:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Not
* ACM62_NCR	* sm62	TLS	* 5062	* ACM62_NCR	* 5062	Trusted	To f

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., **ACM62_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 13.1.2** for the NCR trunk (**ACM62_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 13.1.5**) 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**.

Routing Policy Details
Commit
Cancel

General

* Name: ACM62_NCR
Disabled: ☐
* Retries: 0
Notes: To NCR trunk

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM62_NCR	192.168.67.44	CM	To ACM NCR trunk

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: 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

Add Remove

0 Items Refresh Filter: Enable

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

Regular Expressions

Add Remove

0 Items Refresh Filter: Enable

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

* Input Required
Commit
Cancel

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, step 3** for access to the NCR enabled trunk (e.g., **7325554076**).
- **Min** and **Max** – Enter **10**.
- **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 Location and Routing Policy List** 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 13.1.4** (e.g., **ACM62_NCR**).

Step 6 - In the **Originating Location and Routing Policy List** 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 NCR trunk.

Dial Pattern Details
Commit
Cancel

General

* Pattern: 7325554076

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: to NCR trunk

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	ACM62_NCR	0	<input type="checkbox"/>	ACM62_NCR	To NCR trunk

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh

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

13.3. Configure Communication Manager

13.3.1. 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 **ACM62_NCR** Entity defined in **Section 13.1.2**.

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., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5062** (see **Section 13.1.3**).
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 6.5.2**.
- **Far-end Domain** – Enter **sip.customermerc.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 initiates Communication Manager to send SIP OPTIONS messages to Session Manager to provide link status.

Note – Verify that the **Initial IP-IP Direct Media?** option is set to **n** (default). See **Section 2.2.1, Item 3**.

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: SM	
Near-end Listen Port: 5062	Far-end Listen Port: 5062	
	Far-end Network Region: 4	
	Far-end Secondary Node Name:	
Far-end Domain: sip.customermerc.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., ***05**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the number of 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., **20**).

add trunk-group 5		Page 1 of 21
TRUNK GROUP		
Group Number: 5	Group Type: sip	CDR Reports: y
Group Name: NCR_Trunk	COR: 1	TN: 1
Direction: two-way	Outgoing Display? n	TAC: *05
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 5	
	Number of Members: 20	

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

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

add trunk-group 5		Page 2 of 21
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
	Redirect On OPTIM Failure: 6000	
SCCAN? n	Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 900		
Disconnect Supervision - In? y Out? y		
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n	

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

- Set **Numbering Format:** to **private** (see note in **Section 6.7.1, Step 4**).

add trunk-group 5		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
	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.

Note –When enabled, Communication Manager uses the **SendOnly** SIP signaling method to indicate Hold/Mute conditions (see **Section 2.2.1, item 1**, regarding issues between IPFR-EF and the use of SendOnly).

- 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**).

```
add trunk-group 5                                     Page 4 of 21
               PROTOCOL VARIATIONS
               Mark Users as Phone? n
               Prepend '+' to Calling Number? n
               Send Transferring Party Information? n
               Network Call Redirection? y
               Send Diversion Header? y
               Support Request History? y
               Telephone Event Payload Type: 100
               Convert 180 to 183 for Early Media? n
               Always Use re-INVITE for Display Updates? n
               Identity for Calling Party Display: P-Asserted-Identity
               Enable Q-SIP? n
```

13.3.2. Network Based Blind Transfer with Refer (Communication Manager Vector) for AT&T IP Flexible Reach - Enhanced Features

The IPFR-EF service supports a Network based Blind Transfer call redirection scenario. In this case an IPFR-EF call comes into Communication Manager and is redirected back to a different PSTN destination by use of SIP Refer signaling. The Refer is generated by a Communication Manager Vector Directory Number (VDN) and an associated Vector. Refer functionality is enabled in Communication Manager by the Network Call Redirection SIP trunk option shown in **Section 13.2.1. Step 5**.

Note - Communication Manager vector based call redirection can occur using either the Refer method or by use of a 302 Moved Temporarily. The difference is determined by the inclusion (Refer) or omission (302) of an initial media stream prior to the redirection (generated by an announcement statement in the vector). **Only the Refer method is supported by IPFR-EF.**

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 **05** generates the Refer to new destination **17325552468**.
- Note - You may enter comments by putting **#** in the first column of an entry line.

change vector 37

Page 1 of 6

```
CALL VECTOR
Number: 37          Name: Refer
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
02 announcement 42008
03
04 #    Refer occurs since this is post answer
05 route-to      number ~r17325552468    with cov n if unconditionally
06
```

Step 2 – Create the VDN.

- Enter the **add vdn x** command, where x is the extension defined in **Section 13.1.1, Step 3** (e.g., **19999**)
- 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**).

add vdn 19999

Page 1 of 3

```
VECTOR DIRECTORY NUMBER
Extension: 19999
Name*: REFER
Destination: Vector Number    37
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*:
* Follows VDN Override Rules
```

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 TM and ® 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.