



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.2 and Avaya Session Border Controller for Enterprise with AT&T IP Toll Free SIP Trunk Service – Issue 1.0

Abstract

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

Avaya Aura® Communication Manager 6.2 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Session Border Controller for Enterprise. The Avaya Session Border Controller for Enterprise is the point of connection between Avaya Aura® Communication Manager and the AT&T IP Toll Free 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 IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks. Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free 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.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	5
2.2.1.	Known Limitations	5
2.3.	Support	6
3.	Reference Configuration	6
3.1.	Illustrative Configuration Information	8
3.2.	Call Flows	9
4.	Equipment and Software Validated	11
5.	Avaya Aura® Communication Manager	12
5.1.	System Parameters	12
5.2.	Dial Plan	14
5.3.	IP Node Names.....	15
5.4.	IP Interface for procr	15
5.5.	IP Network Regions	15
5.5.1.	IP Network Region 3 – Local Region.....	15
5.5.2.	IP Network Region 4 – AT&T Trunk Region	17
5.6.	IP Codec Parameters	18
5.6.1.	Codecs for IP Network Region 3 (local calls)	18
5.6.2.	Codecs for IP Network Region 4	19
5.7.	SIP Trunks.....	19
5.7.1.	SIP Trunk for AT&T IP Toll Free calls.....	20
5.7.2.	Local SIP Trunk (Avaya Aura® Messaging access)	23
5.8.	Incoming Call Handling	25
5.9.	Public Unknown Numbering.....	25
5.10.	Private Numbering.....	26
5.11.	Route Patterns.....	27
5.11.1.	Route Pattern for Calls to Avaya Aura® Messaging	27
5.12.	Automatic Alternate Routing (AAR) Dialing	27
5.13.	Provisioning for Coverage to Avaya Aura® Messaging.....	28
5.13.1.	Hunt Group for Station Coverage to Avaya Aura® Messaging	28
5.13.2.	Coverage Path for Station Coverage to Avaya Aura® Messaging	29
5.13.3.	Station Coverage Path to Avaya Aura® Messaging	30
5.14.	Call Center Provisioning	31
6.	Avaya Aura® Messaging.....	32
7.	Configure Avaya Session Border Controller for Enterprise	33
7.1.	Initial Installation/Provisioning.....	33
7.2.	Advanced Configuration	33
7.3.	Global Profiles.....	34
7.3.1.	Server Interworking – Avaya Side.....	34
7.3.2.	Server Interworking – AT&T Side	35
7.3.3.	Routing – Avaya Side	36

7.3.4.	Routing – AT&T Side.....	36
7.3.5.	Server Configuration – To Avaya Communication Manager	37
7.3.6.	Server Configuration – To AT&T	38
7.3.7.	Topology Hiding – Avaya Side	39
7.3.8.	Topology Hiding – AT&T Side.....	41
7.3.9.	Signaling Manipulation.....	41
7.4.	Domain Policies	41
7.4.1.	Application Rules.....	41
7.4.2.	Media Rules	42
7.4.3.	Signaling Rules	43
7.4.4.	Endpoint Policy Groups – Avaya	48
7.4.5.	Endpoint Policy Groups – AT&T	49
7.5.	Device Specific Settings.....	50
7.5.1.	Network Management.....	50
7.5.2.	Media Interfaces.....	51
7.5.3.	Signaling Interface	51
7.5.4.	Endpoint Flows – To Avaya Communication Manager	52
7.5.5.	Endpoint Flows – To AT&T.....	52
7.6.	Troubleshooting Port Ranges	53
8.	Verification Steps.....	54
8.1.	General	54
8.2.	Avaya Aura® Communication Manager	54
8.3.	Protocol Traces.....	55
8.4.	Avaya Session Border Controller for Enterprise Verification	56
9.	Conclusion	57
10.	References.....	58
11.	Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements.....	59

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Communication 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 Toll Free service using **AVPN** or **MIS/PNT** transport connections.

Avaya Aura® Communication Manager 6.2 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya SBCE. An Avaya SBCE is the point of connection between Avaya Aura® Communication Manager and the AT&T IP Toll Free 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 IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks utilizing AVPN or MIS/PNT¹ transport.

Note – These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. See the document *Application Notes for Avaya Aura® Communication Manager 6.2 and Avaya Session Border Controller for Enterprise with AT&T IP Transfer Connect Service – Issue 1.0* for information on the AT&T IP Transfer Connect Solution.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Communication Manager, Avaya phones, fax machines (Ventafax application), Avaya SBCE, and Avaya Aura® Messaging.
- A laboratory version of the AT&T IP Toll Free service, to which the simulated enterprise was connected via AVPN transport.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound call flows (see **Section 3.2** for examples) between Communication Manager, Avaya SBCE, and the AT&T IP Toll Free 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 from the PSTN across the AT&T IP Toll Free service network.

¹ MIS/PNT transport does not support compressed RTP (cRTP), however AVPN transport does support cRTP.

The following features were tested as part of this effort:

- SIP trunking.
- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.
- PBX and AT&T IP Toll Free service features such as hold, resume, conference and transfer.
- AT&T IP Toll Free features such as Legacy Transfer Connect and Alternate Destination Routing were also tested.

2.2. Test Results

The main test objectives were to verify the following features and functionality:

- Inbound AT&T IP Toll Free service calls to Communication Manager telephones and VDNs/Vectors/Agents.
- Call and two-way talk path establishment between PSTN and Communication Manager telephones/Agents via the AT&T Toll Free service.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729 and G.711 codecs.
- T.38 fax calls from the AT&T IP Toll Free service/PSTN to Communication Manager G3 and SG3 fax endpoints.
- DTMF tone transmission using RFC 2833 between Communication Manager and the AT&T IP Toll Free service/PSTN automated access systems.
- Inbound AT&T IP Toll Free service calls to Communication Manager that is directly routed to stations, and if unanswered, can be covered to Avaya Aura® Messaging.
- Long duration calls.

The test objectives stated in **Section 2.1** with limitations as noted in **Section 2.2.1**, were verified.

2.2.1. Known Limitations

1. **G.711 Fax support** - G.711 faxing is not supported between Communication Manager and the AT&T IP Toll Free service. Fax speeds are limited to 9600 in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Communication Manager in the reference configuration.
2. **G.726 codec support** - G.726 codec is not supported between Communication Manager and the AT&T IP Toll Free service.
3. **Call transfer connection issue with Avaya one-X® Agent in “Other Phone” mode** – There is a known intermittent loss of audio issue during call transfer scenarios with Avaya one-X® Agent operating in “Other Phone” mode, in conjunction with Communication Manager 6.2. This issue is under investigation by Avaya. Therefore the use of Avaya one-X® Agent operating in “Other Phone” mode with Communication Manager 6.2 is not recommended.
 - This issue is scheduled to be fixed in Communication Manager SP4.

2.3. Support

AT&T customers may obtain support for the AT&T IP Toll Free service by calling (800) 325-5555.

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. Customers may also use specific numbers (provided on <http://support.avaya.com>) to directly access specific support and consultation services based upon their Avaya support agreements.

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. The solution described in these application notes is extensible to other Communication Manager 6.2 implementations.
- 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 1603(H.323), 960x Series IP Telephones (running H.323 firmware), and 96x1 Series IP Telephones (running H.323 firmware), Avaya 6421 Analog Telephones, as well as Avaya one-X® Agent soft phone (H323). Note that without Avaya Session Manager, SIP telephones are not supported.
- The Avaya SBCE provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Toll Free service and the enterprise internal network.
- The AT&T IP Toll Free service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Avaya SBCE in this sample configuration. Communication Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, (e.g., Avaya SBCE or Avaya Aura® Messaging). In the reference configuration Communication Manager uses SIP over TCP to communicate with the Avaya SBCE. UDP transport protocol is used between the Avaya SBCE and the AT&T IP Toll Free 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.
- Inbound calls were placed from PSTN via the AT&T IP Toll Free service, through the Avaya SBCE to Communication Manager. Communication Manager terminates the call to

the appropriate agent/phone or fax extension. The Avaya H.323 telephones in the enterprise register to the Communication Manager Processor Ethernet (Procr) interface.

Note – Documents used to provision the reference configuration are listed in **Section 10**. Specific references to these documents are indicated in the following sections by the notation [x], where x is the document reference number.

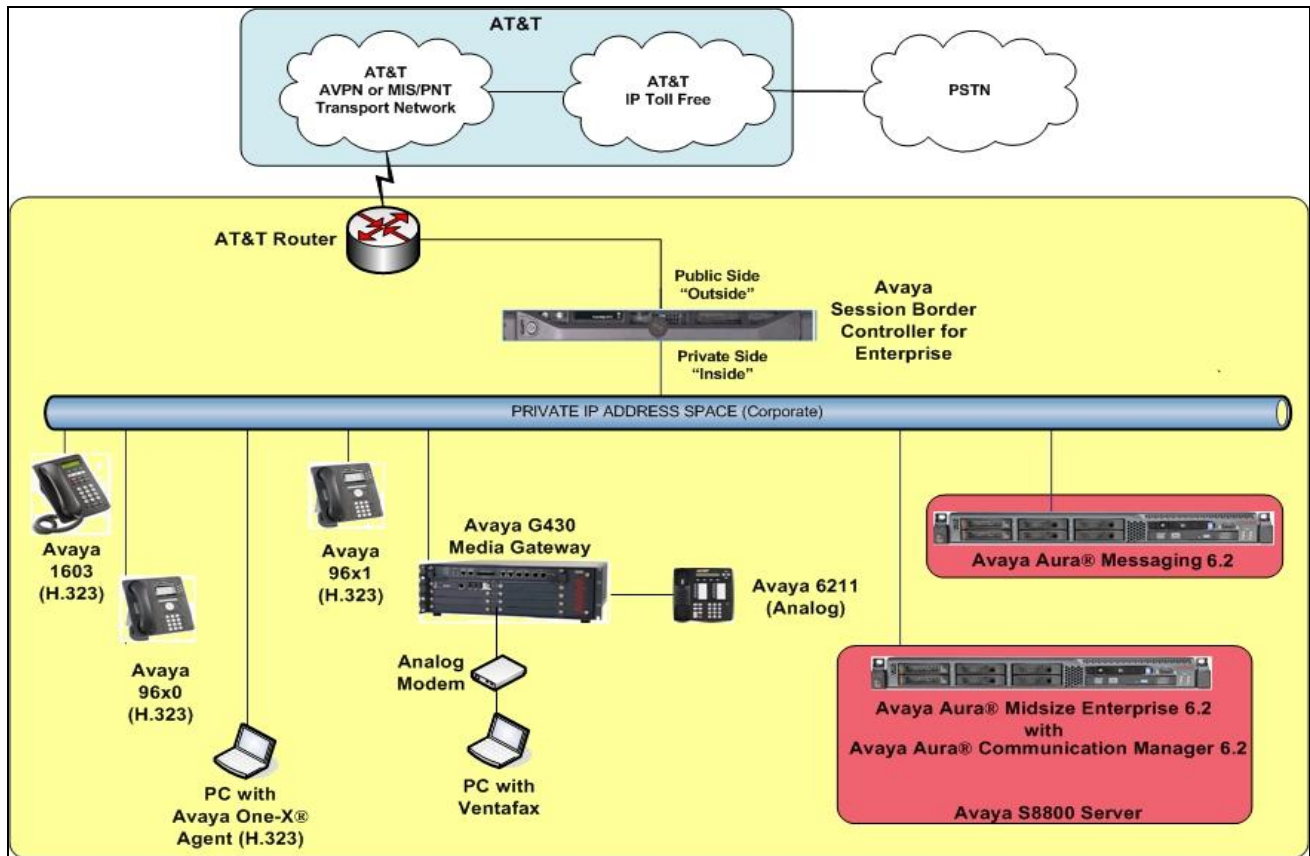


Figure 1: Reference configuration

3.1. Illustrative Configuration Information

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

Component	Illustrative Value in these Application Notes
Avaya Aura® Communication Manager	
Processor Ethernet (Procr) interface	192.168.67.44
Avaya Aura® Communication Manager extensions, Agents, and VDNs	19xxx, 44xxx, 47xxx
Voice Messaging Pilot Extension	36000
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Outside (Public) Interface	192.168.64.130
IP Address of Inside (Private) Interface	192.168.67.120
Avaya Aura Messaging	
IP Address	192.168.67.147
AT&T IP Toll Free Service	
Border Element IP Address	135.25.29.74

Table 1: Illustrative Values Used in these Application Notes

Note - The AT&T IP Toll Free service Border Element IP address and DNIS digits, (destination digits specified in the SIP Request URIs sent by the AT&T Toll Free service) are shown in this document as examples. AT&T Customer Care will provide the actual IP addresses and DNIS digits as part of the IP Toll Free provisioning process.

3.2. Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled by Communication Manager, two general call flows are described in this section. The first call scenario illustrated in **Figure 2** is an inbound AT&T IP Toll Free service call that arrives at Communication Manager.

1. A PSTN telephone originates a call to an AT&T IP Toll Free service number.
2. The PSTN routes the call to the AT&T IP Toll Free service network.
3. The AT&T IP Toll Free 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 Communication Manager.
5. Depending on the called number, Communication Manager routes the call to a) a vector, which in turn, routes the call to an agent, or b) directly to an agent or telephone.

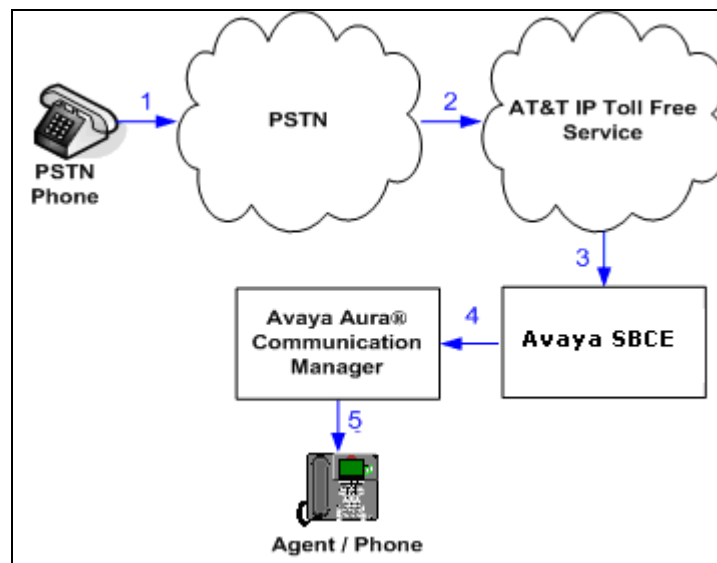


Figure 2: Inbound AT&T IP Toll Free Service Call to VDN/Agent/Telephone

The second call scenario illustrated in **Figure 3** is an inbound call that is covered to voicemail. In this scenario, the voicemail system is an Avaya Aura® Messaging system connected to Communication Manager via a SIP trunk.

1. Same as the **Steps 1-5** from the first call scenario.
2. The called Communication Manager agent or telephone does not answer the call, and the call covers to the agent's or telephone's voicemail. Communication Manager forwards the call to Avaya Aura® Messaging.
3. Avaya Aura® Messaging answers the call and connects the caller to the called agent's or telephone's voice mailbox.

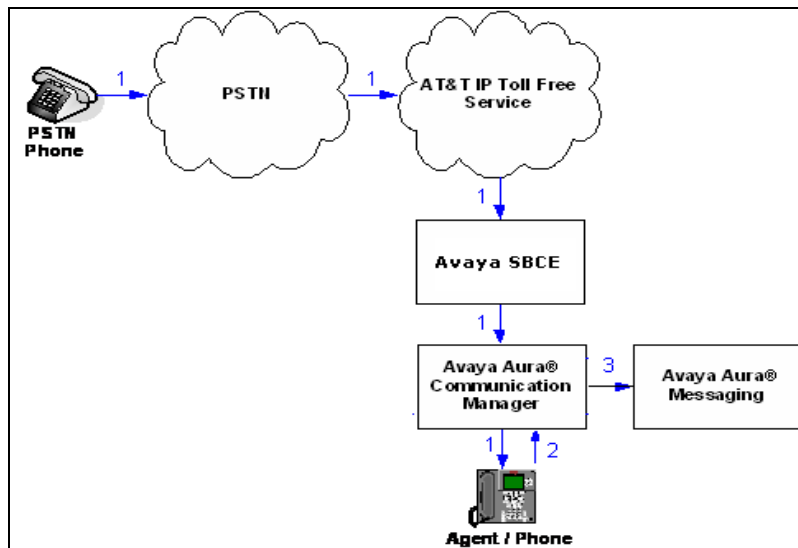


Figure 3: Inbound AT&T IP Toll Free Service Call Covered to Avaya Aura® Messaging

4. Equipment and Software Validated

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

Equipment		Software Release/Version
HP Proliant DL360 G7 server		<ul style="list-style-type: none">• System Platform 6.2.1.0.9• Avaya Aura® Communication Manager 6.2 SP3 (02.0.823.0-20001)
Dell R610		<ul style="list-style-type: none">• System Platform 6.2.1.0.9• Avaya Aura® Messaging 6.2 SP1 (MSG-02.0.823.0-109_0102)
Avaya G430 Media Gateway		31.20.0
	MM711 Analog card	HW31 FW094
	MM712 Digital card	HW07 FW011
Dell R210		Avaya Session Border Controller for Enterprise 4.0.5.Q19
Avaya 96x0 IP Telephone		H.323 Version S3.105S
Avaya 96x1 IP Telephone		H.323 Version S6.020S
Avaya one-X® Agent		2.5 SP1 Patch 1 (2.5.1072.11082)
Avaya 1603 IP Telephone		H323 (ha1603ua1_3200.bin)
Avaya 6424 Digital telephone		
Windows XP PC		Ventafax Home Version (Fax device) 6.1.59.144
AT&T IP Toll Free service using AVPN/MIS-PNT transport service connection.		VNI 26

Table 2: Equipment and Software Versions

5. Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult documents [1] and [2] 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.

5.1. 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 **Enhanced EC500?** , **IP Stations?**, **ISDN-PRI?**, and **IP Trunks?** 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		

5.2. 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).
 2. The digit **1** (Local extensions for Communication Manager Agents and VDNs).
 3. 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 5.12**).

change dialplan analysis			DIAL PLAN ANALYSIS TABLE			Page	1 of 12
			Location: all			Percent Full: 2	
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length
1	5	ext					
3	5	ext					
4	5	ext					
8	1	fac					
*	3	dac					

5.3. 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 do the following:

- Verify the Processor Ethernet node name and IP Address (**procr** & **192.168.67.44**). These appear automatically based on the address defined during installation.
- Add a node for the Avaya SBCE (e.g., **SBCE**) with SBCE Internal Interface IP address **192.168.67.120** (see **Section 7.5.1**).
- Add a node for the Avaya Aura® Messaging (e.g., **AAM**) with IP address **192.168.67.147**

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AAM	192.168.67.147	
default	0.0.0.0	
procr	192.168.67.44	
procr6	::	
SBCE	192.168.67.120	

5.4. 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		
Enable Interface? y		Target socket load: 1700
Network Region: 3		Allow H.323 Endpoints? y
		Allow H.248 Gateways? y
		Gatekeeper Priority: 5
IPV4 PARAMETERS		
Node Name: procr		IP Address: 192.168.67.44
Subnet Mask: /24		

5.5. 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.

5.5.1. 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. Provision the form with the following values:

- Enter a descriptive name (e.g., **Local**).
- Enter **sip.customerc.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.customerc.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 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 1												all	
4 2 y NoLimit										n			t

5.5.2. 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 5.5.1** 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
                                AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                RSVP Enabled? n
    H.323 Link Bounce Recovery? y
    Idle Traffic Interval (sec): 20
    Keep-Alive Interval (sec): 5
    Keep-Alive Count: 5

```

Step 2 – On Page 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 rgn	codec set	direct	WAN Units	WAN-BW-limits	Video	Intervening		Dyn	A	G	c	
				Total Norm	Prio Shr	Regions		CAC	R	L	e	
1												
2												
3	2	y	NoLimit						n		t	
4	2									all		
5												

5.6. IP Codec Parameters

5.6.1. 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**, and **G.729A** are specified in the codec list in the order shown. Note that the packet interval size will default to 20ms. Optionally G.729B can be selected instead of G.729A.

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:							

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			

5.6.2. 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 AT&T IP Toll Free calls. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown. Optionally G.729B may be specified instead of G.729A. For G729A or G729B set **3** for the **Frames Per Pkt**. This will automatically populate **30** for the Packet Size (ms). Let G711MU default to **20**.

change ip-codec-set 2				Page 1 of 2
IP Codec Set				
Codec Set: 2				
Audio	Silence	Frames	Packet	
Codec	Suppression	Per Pkt	Size (ms)	
1: G.729A	n	3	30	
2: G.711MU	n	2	20	
3:				

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		

5.7. 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.
- Local for Avaya Aura® Messaging access – SIP Trunk 3
 - Note that this trunk will use TLS port 5060.

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

Note – In the reference configuration, TCP (port 5060) is used as the transport protocol on the Communication Manager public and local SIP trunks. This was done to facilitate protocol trace analysis. Note that Avaya best practices call for TLS to be used as the transport protocol in customer environments whenever possible. The transport protocol used between the Avaya SBCE and the AT&T IP Toll Free service is UDP.

5.7.1. SIP Trunk for AT&T IP Toll Free calls

This section describes the steps for administering the SIP trunk used for inbound AT&T IP Toll Free calls.

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**.
- Set **Peer Detection Enabled?** to **n**, and set **Peer Server:** to **Others**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.3**.
- **Far-end Node Name** – Set to the node name of the Avaya SBCE as administered in **Section 5.3** (e.g., **SBCE**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5060**
- **Far-end Network Region** – Set the IP network region to **4**, as set in **Section 5.5.2**.
- **Far-end Domain** – Enter **sip.customerarc.com** (see **Sections 5.5.1** and **5.5.2**).
- **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 the Avaya SBCE to provide link status.

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? n	Peer Server: Others	
Near-end Node Name: procr	Far-end Node Name: SBCE	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 4	
	Far-end Secondary Node Name:	
Far-end Domain: sip.customerarc.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 **incoming**.
- **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	TAC: *04
Direction: incoming	Outgoing Display? n		
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			
	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 **public**.

add trunk-group 4	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none Maintenance Tests? y
Numbering Format: public	UI 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 **Support Request History?** to **n**.

Note – The AT&T IP Toll Free service does not support History Info header. By default, this header is enabled by Communication Manager. In the reference configuration, the History Info header is disabled in the trunk form. Alternatively, History Info may be removed by the Avaya SBCE (see **Section 7.4.3.1**).

- Set **Telephone Event Payload Type** to the RTP payload type required by the AT&T IP Toll Free service (e.g., **100**).

add trunk-group 4	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? n	
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	

5.7.2. Local SIP Trunk (Avaya Aura® Messaging access)

This section describes the steps for administering the local SIP trunk to Avaya Aura® Messaging.

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 5.7.1** with the following changes:

- **Far-end Network Region** – Set to the IP network region **3**, as defined in **Section 5.5.1**.

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? n	Peer Server: Others	
Near-end Node Name: procr	Far-end Node Name: AAM	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
Far-end Domain: sip.customercc.com	Far-end Network Region: 3	
	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 5.7.1** 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**).
- **Direction** – Set to **two-way**
- **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
Direction: two-way	Outgoing Display? n	TAC: *03
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 5.7.1**.

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

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

add trunk-group 3	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: internal
	Maintenance Tests? y
Numbering Format: private	UI 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 **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	

5.8. Incoming Call Handling

Communication Manager must convert the incoming DNIS numbers sent by the AT&T IP Toll Free service, to their associated Communication Manager extensions.

Step 1 - Using the **change inc-call-handling-trmt trunk-group 4** command, (trunk 4 is the public SIP trunk to AT&T), enter the following:

- **Service/Feature** – Enter **public-ntwrk**.
- **Number Len** – Enter the number of DNIS digits sent by the IP Toll Free service (e.g., **10**)
- **Number Digits** – Enter a DNIS digit string (e.g., **0000001050**).
- **Del** – Enter the number of DNIS digits to delete (e.g., **10**).
- **Insert** – Enter the associated Communication Manager extension (e.g., Skill VDN extension **44002**).

Step 2 – Repeat **Step 1** for any additional DNIS/extension associations.

change inc-call-handling-trmt trunk-group 4				Page	1 of 30
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	10	0000001050	10	44002	
public-ntwrk	10	0000001051	10	44003	
public-ntwrk	10	0000001052	10	44003	
public-ntwrk	10	0000001053	10	19011	

5.9. Public Unknown Numbering

In the reference configuration, the public-unknown-numbering form is used to convert Communication Manager local extensions to AT&T IP Toll Free DNIS numbers, (previously identified by AT&T), for inclusion in Contact and PAI SIP headers directed to the AT&T IP Toll Free service via the public trunk (e.g., **4**) defined in **Section 5.7.1**.

Step 1 - Using the **change public-unknown-numbering 0** command, enter the following:

- **Ext Len** – Enter the total number of digits in the extension range (e.g., **5**).
- **Ext Code** – Enter a Communication Manager extension (e.g., **44002**) assigned to a VDN used by an Agent/Skill (see **Section 5.14**).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g., **4**).
- **CPN Prefix** – Enter the associated AT&T IP Toll Free DNIS number (e.g., **0000001050**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 2 – Repeat **Step 1** for any additional VDNs used for Agent/Skill access.

Step 3 – If there are any Communication Manager station extensions that are called directly, enter those as well:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).

- **Ext Code** – Enter the Communication Manager station extension (e.g., **19011**).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g., **4**).
- **CPN Prefix** – Enter the corresponding AT&T IP Toll Free DNIS number (e.g., **0000001053**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 4 – Repeat **Step 3** for any additional station extensions accessed directly.

change public-unknown-numbering 0					Page 1 of 2
					NUMBERING - PUBLIC/UNKNOWN FORMAT
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	19011	6	0000001053	10	Total Administered: 4
5	44002	6	0000001050	10	Maximum Entries: 9999
5	44003	6	0000001051	10	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	44004	6	0000001052	10	

5.10. Private Numbering

In the reference configuration, the private-numbering form is used to direct local extensions to Avaya Aura® Messaging (call coverage/retrieval) via the local trunk (e.g., **3**) defined in **Section 5.7.2**.

Step 1 - Using the **change private-numbering 0** command, enter the following:

- **Ext Len** – Enter the total number of digits in the extension range (e.g., **5**).
- **Ext Code** – Enter a Communication Manager station extension pattern (e.g., **1**, to represent 1xxx station extensions).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **3**).
- **Private Prefix** – Leave blank.
- **Total Len** – Enter the total number of digits in the extension (e.g., **5**).

Step 2 – Repeat **Step 1** for any Agent extensions, with the following changes:

- **Ext Code** – Enter a Communication Manager Agent extension pattern (e.g., **4**, to represent 4xxx Agent 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: 2
5	4	3		5	Maximum Entries: 540
5	4	3		5	

5.11. Route Patterns

5.11.1. Route Pattern for Calls to Avaya Aura® Messaging

This form defines the local SIP trunk, based on the route-pattern selected by the AAR table in **Section 5.12** (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 the local SIP trunk.
- In the **FRL** column enter **0** (zero).

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	n	rest						none								
2:	y	y	y	y	y	n	n	rest						none								
3:	y	y	y	y	y	n	n	rest						none								
4:	y	y	y	y	y	n	n	rest						none								
5:	y	y	y	y	y	n	n	rest						none								

5.12. Automatic Alternate Routing (AAR) Dialing

Automatic Alternate Routing (AAR) is used to direct coverage calls for Avaya Aura® Messaging (36000) to the route pattern defined in **Section 5.11.1**.

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		

5.13. Provisioning for Coverage to Avaya Aura® Messaging

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

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

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

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

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

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

- **Message Center** – Enter **sip-adjunct**.
- **Voice Mail Number** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Voice Mail Handle** – Enter the Avaya Aura® Messaging pilot number (e.g., **36000**).
- **Routing Digits** – Enter the AAR access code defined in **Section 5.2** (e.g., **8**).

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

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

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

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

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

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

5.13.3. 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 5.13.2**. 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	

5.14. Call Center Provisioning

The administration of Communication Manager Call Center elements – agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult [3] for further details, if necessary. The samples that follow are provided for reference purposes only.

- Agent form – **Page 1**

display agent-loginID 47002	Page 1 of 3
AGENT LOGINID	
Login ID: 47002	AAS? n
Name: Agent2	AUDIX? n
TN: 1	LWC Reception: spe
COR: 1	LWC Log External Calls? n
Coverage Path: 1	AUDIX Name for Messaging:
Security Code:	LoginID for ISDN/SIP Display? n
	Password: 2580
	Password (enter again): 2580
	Auto Answer: station
	MIA Across Skills: system
	ACW Agent Considered Idle: system
	Aux Work Reason Code Type: system
	Logout Reason Code Type: system
	Maximum time agent in ACW before logout (sec): system
	Forced Agent Logout Time: :

- Agent form – **Page 2**

display agent-loginID 47002	Page 2 of 3
AGENT LOGINID	
Direct Agent Skill:	Service Objective? n
Call Handling Preference: skill-level	Local Call Preference? n
SN RL SL SN RL SL SN RL SL SN RL SL	
1: 2 1	
2:	

- Skill 2 Hunt Group form – **Page 1**

display hunt-group 2	Page 1 of 4
HUNT GROUP	
Group Number: 2	ACD? y
Group Name: Skill2	Queue? y
Group Extension: 43002	Vector? y
Group Type: ead-mia	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display:	
Queue Limit: unlimited	
Calls Warning Threshold: Port:	
Time Warning Threshold: Port :	

- Skill 2 VDN form – **Page 1**

display vdn 44002		Page 1 of 3
VECTOR DIRECTORY NUMBER		
Extension: 44002		
Name*: Skill2		
Destination: Vector Number	2	
Attendant Vectoring? n		
Meet-me Conferencing? n		
Allow VDN Override? n		
COR: 1		
TN*: 1		
Measured: none		
VDN of Origin Annc. Extension*:		
1st Skill*:		
2nd Skill*:		
3rd Skill*:		
* Follows VDN Override Rules		

- Skill 2 Vector form – **Page 1**

display vector 2		Page 1 of 6
CALL VECTOR		
Number: 2	Name: Skill2	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n Lock? n
Basic? y	EAS? y G3V4 Enhanced? y	ANI/II-Digits? y ASAI Routing? y
Prompting? y	LAI? y G3V4 Adv Route? y	CINFO? y BSR? y Holidays? y
Variables? y	3.0 Enhanced? y	
01 wait-time	2 secs hearing ringback	
02 announcement	42002	
03 queue-to	skill 2 pri m	
04 wait-time	10 secs hearing music	
05 announcement	42005	
06 goto step	3 if unconditionally	
07 stop		
08		

6. 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 documents [4] and [5] for further details.

7. Configure Avaya Session Border Controller for Enterprise

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

7.1. Initial Installation/Provisioning

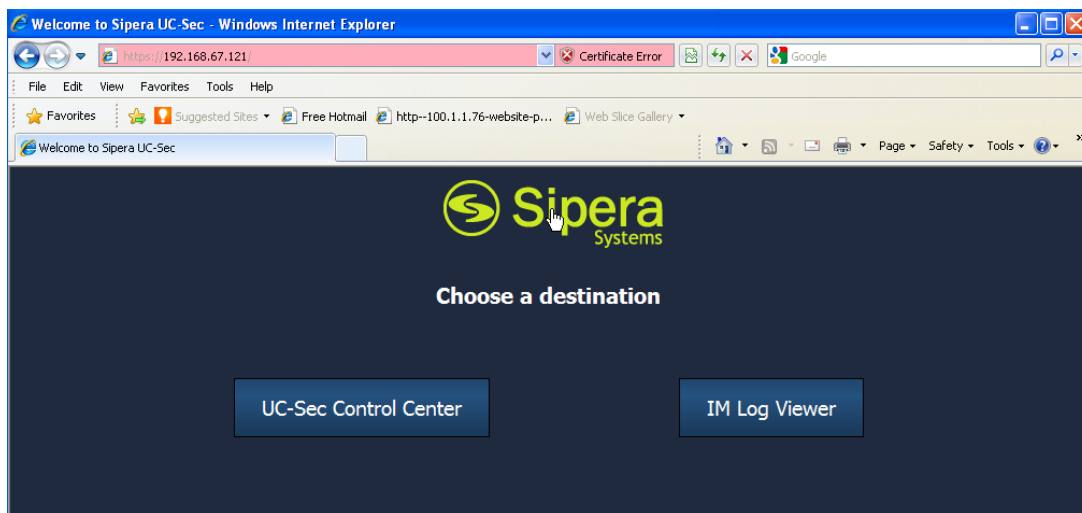
Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document. Refer to documents [6] and [7] for additional information.

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 have this resolved.

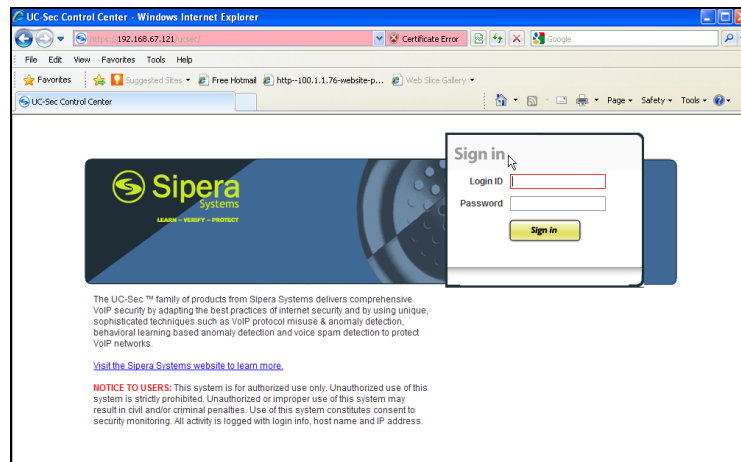
7.2. Advanced Configuration

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

1. Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP of the Avaya SBCE).
2. Select **UC-SEC Control Center**.



3. Enter the login ID and password



7.3. Global Profiles

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

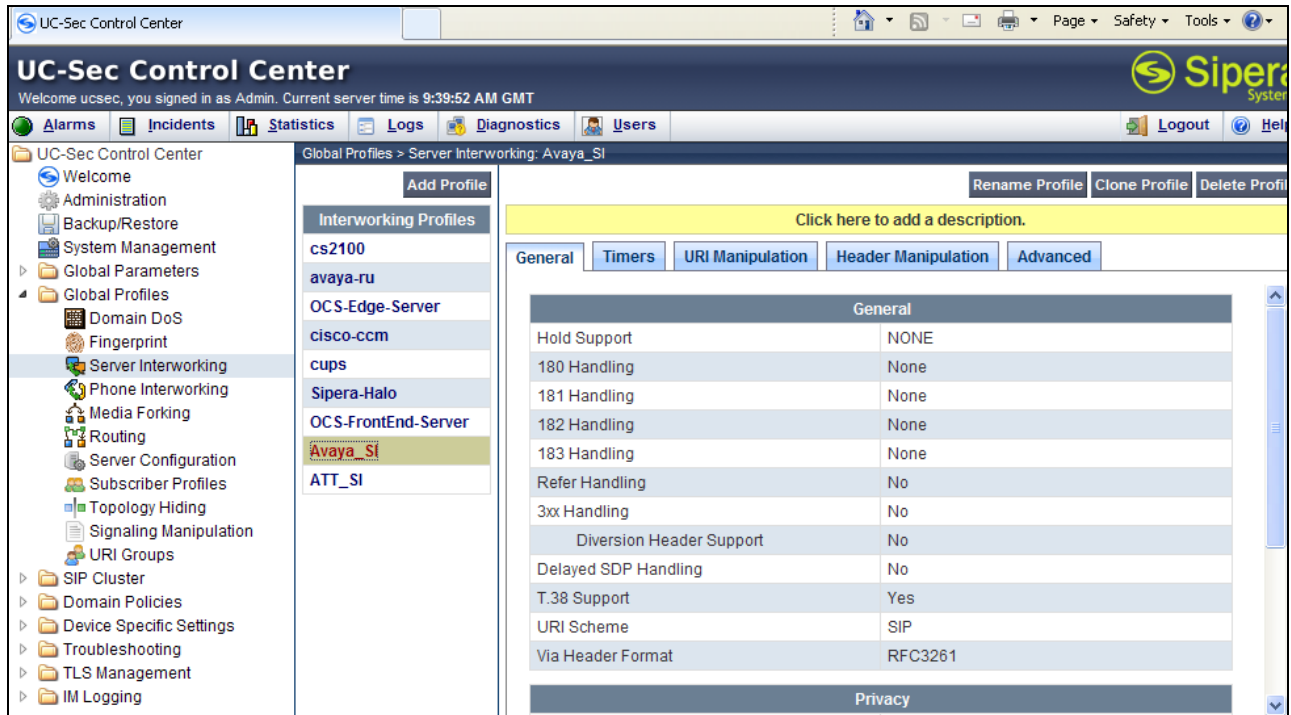
7.3.1. Server Interworking – Avaya Side

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 (not shown)
2. Select the **Server Interworking** (not shown)
3. Select **Add Profile** (not shown)
4. The following information is entered (and stored in the **General Tab**):
 - a. Enter profile name: **Avaya_SI** (not shown), and select **Next**.
 - b. Check **T38 Support** → **Yes**
 - c. Leave all other options at default, and select **Next**.

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

- On the **Privacy/DTMF** window (not shown), select **Next** to accept default values.
- On the **SIP Timers/Transport Timers** window (not shown), select **Next** to accept the remaining default values for the General Tab.
- Accept default values for all remaining tabs, and click **Finish.(Not Shown)**



7.3.2. Server Interworking – AT&T Side

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

- Select **Global Profiles** from the menu on the left-hand side
- Select the **Server Internetworking**
- Select **Add Profile**
- The following information is entered on the **General** Tab:
 - Enter a profile name: (e.g., **ATT**)
 - Select **Next**
 - Check **T38 Support**
 - All other options on the General Tab can be left at default.
 - Select **Next**
 - At the **Privacy/DTMF** sections select **Next** to accept the remaining default values for the General Tab.
- Accept the default values for all remaining tabs and select **Finish.**

7.3.3. 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. (not shown)
2. Select the **Routing** tab (not shown).
3. Select **Add Profile** (not shown).
4. Enter Profile Name: (e.g., **To_Avaya**). (not shown)
5. Click **Next** and enter:
 - a. **Next Hop Server 1: 192.168.67.44** (Communication Manager Processor Ethernet IP address, **Section 5.4**)
 - b. Select **Routing Priority Based on Next Hop Server**
 - c. **Outgoing Transport: TCP**
 - d. Use defaults for all other values.
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 section titled 'Next Hop Routing'. It contains a table with two rows: 'Next Hop Server 1' with the value '192.168.67.44' and 'Next Hop Server 2' which is empty. Both rows have a placeholder text 'IP, IP:Port, Domain, or Domain:Port'. Below the table 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 two radio buttons for 'NAPTR' and 'SRV', both unchecked. At the bottom, there is a section for 'Outgoing Transport' with three radio buttons: 'TLS' (unchecked), 'TCP' (checked), and 'UDP' (unchecked). At the very bottom are 'Back' and 'Finish' buttons.

Next Hop Routing	
URI Group	*
Next Hop Server 1	192.168.67.44
Next Hop Server 2	

☒ 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**

7.3.4. Routing – AT&T Side

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

1. Select **Global Profiles** from the menu on the left-hand side (not shown).
2. Select the **Routing** tab (not shown).
3. Select **Add Profile** (not shown).
4. Enter Profile Name: (e.g., **To_ATT**) (not shown).
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**
 - a. **Outgoing Transport: UDP**
 - b. Use defaults for all other values.

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: 135.25.29.74 (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

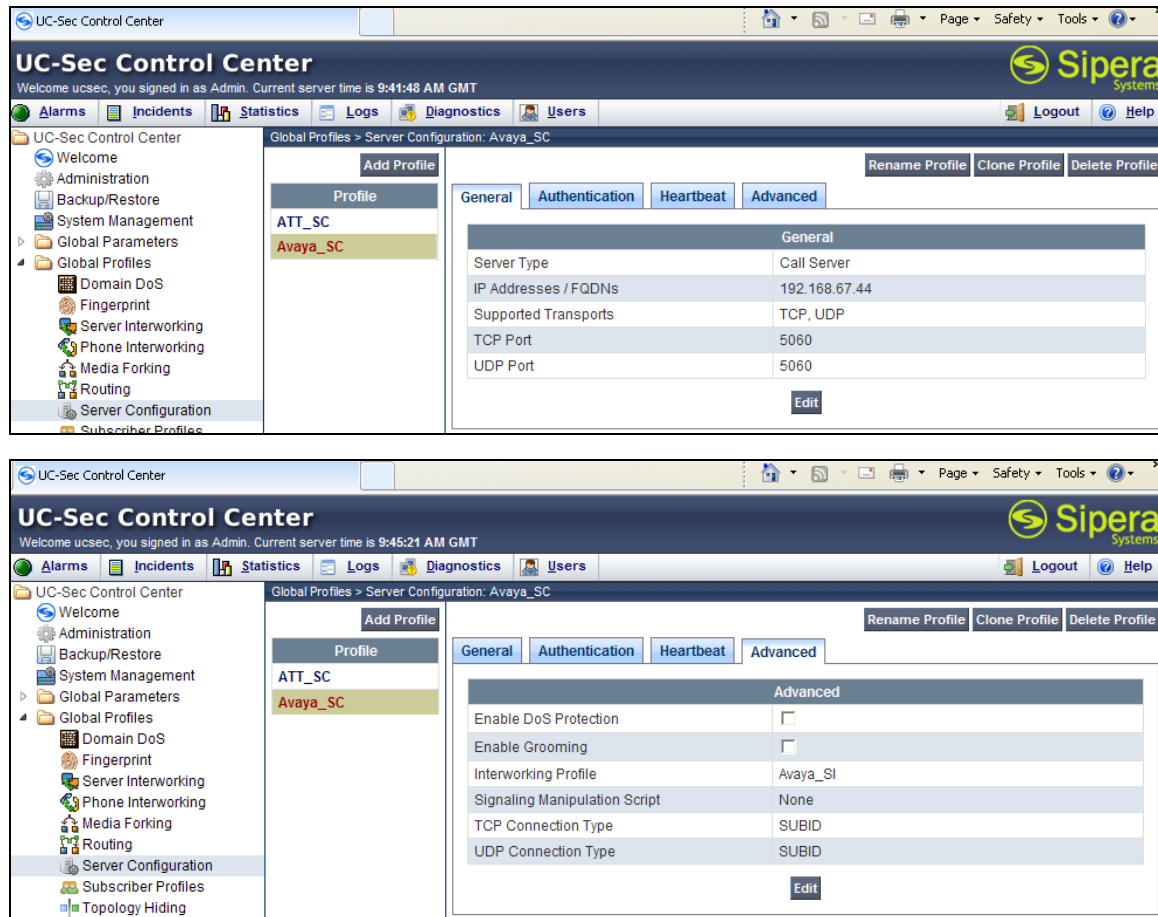
Back Finish

7.3.5. Server Configuration – To Avaya Communication 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_SC**) and select **Next**.
4. The **Add Server Configuration Profile - General** window will open (not shown).
 - a. Select Server Type: **Call Server**
 - b. **IP Address: 192.168.67.44** (Communication 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 **Avaya_SI** for **Interworking Profile** (created in **Section 7.3.1**).
 - b. In the **Signaling Manipulation Script** field select **None** (default).
 - c. Select **Finish**.

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



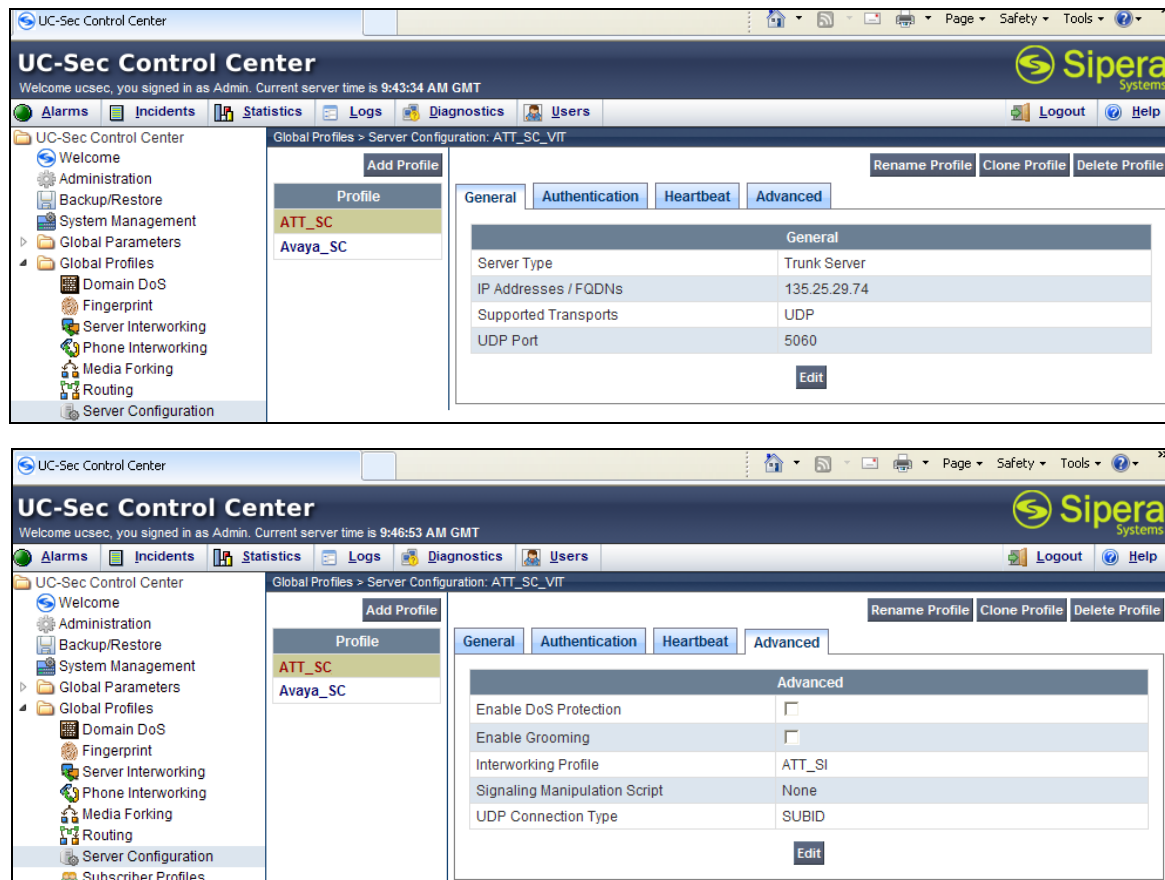
7.3.6. Server Configuration – To AT&T

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

1. Select **Global Profiles** from the menu on the left-hand side.
2. Select **Server Configuration**.
3. Select **Add Profile** and the **Profile Name** window will open (not shown). Enter a Profile Name (e.g., **ATT_SC**) 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.
 - d. Select **ATT_SI** for **Interworking Profile** (created in **Section 7.3.2**).
 - e. In the **Signaling Manipulation Script** field select **None** (default).
 - a. Select **Finish**.

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



7.3.7. 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_TH**).

5. For the Header **To**,
 - a. In the **Criteria** column select **IP/Domain**
 - b. In the **Replace Action** column select: **Overwrite**
 - c. In the **Overwrite Value** column: **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**
8. Click **Finish**.

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	
Record-Route	IP/Domain	Auto	
From	IP/Domain	Overwrite	sip.customerbc.com
To	IP/Domain	Overwrite	sip.customerbc.com
SDP	IP/Domain	Auto	
Request-Line	IP/Domain	Overwrite	sip.customerbc.com

Finish

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 9:48:39 AM GMT

Global Profiles > Topology Hiding: Avaya_TH

Click here to add a description.

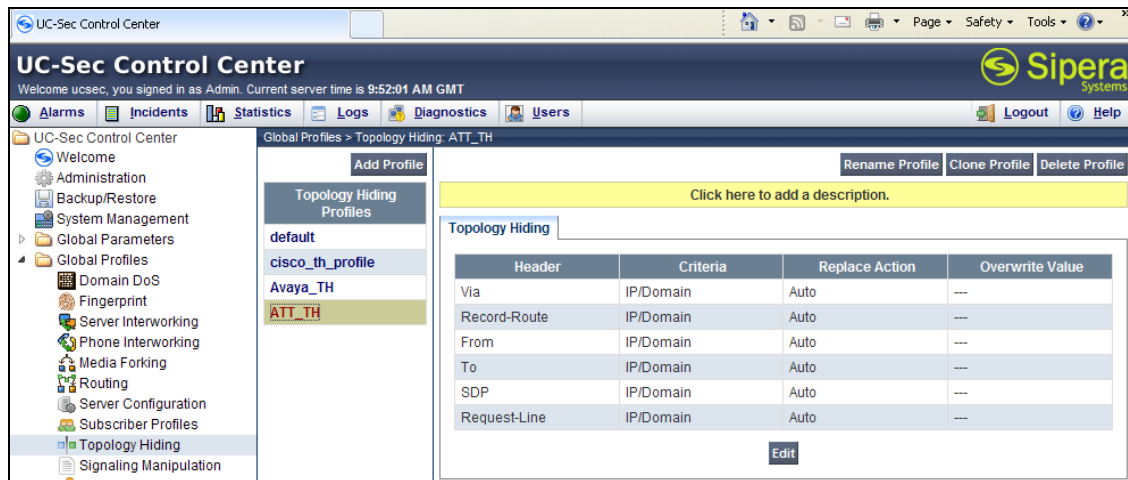
Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sip.customerbc.com
To	IP/Domain	Overwrite	sip.customerbc.com
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sip.customerbc.com

Edit

7.3.8. Topology Hiding – AT&T Side

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

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



7.3.9. Signaling Manipulation

The Avaya SBCE can manipulate or remove inbound and outbound SIP headers, however no SIP header manipulations were required in the reference configuration.

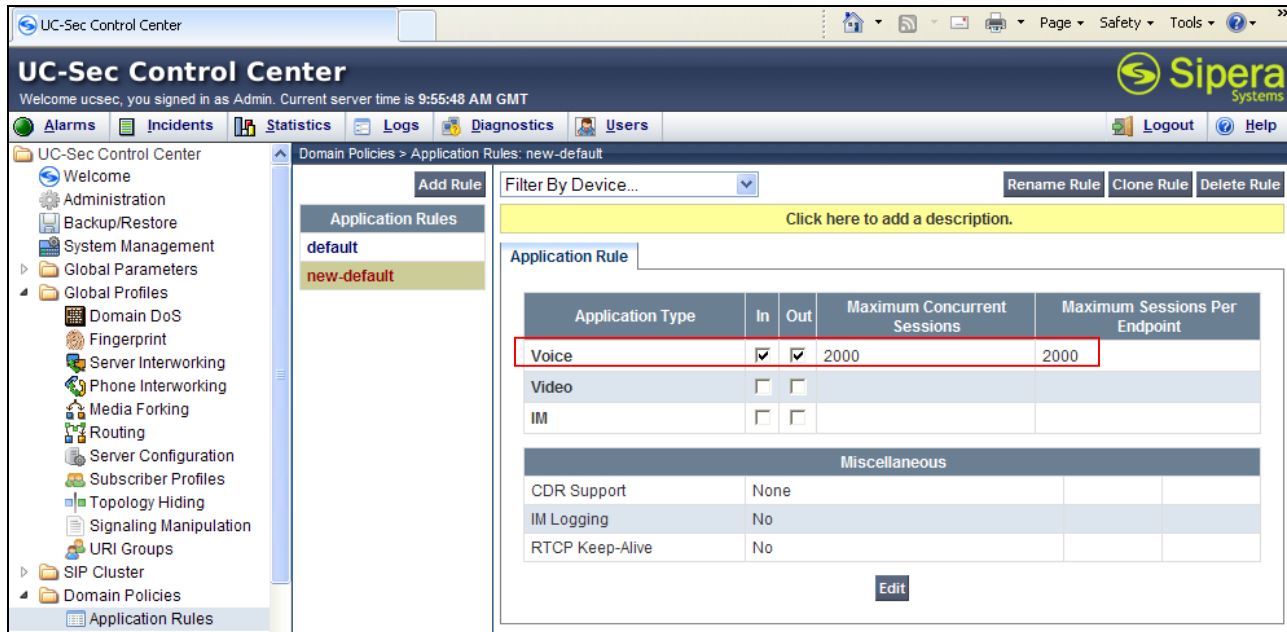
7.4. Domain Policies

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.

7.4.1. 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 **2000**
 - ii. Change the **Maximum Sessions per Endpoint** to **2000**

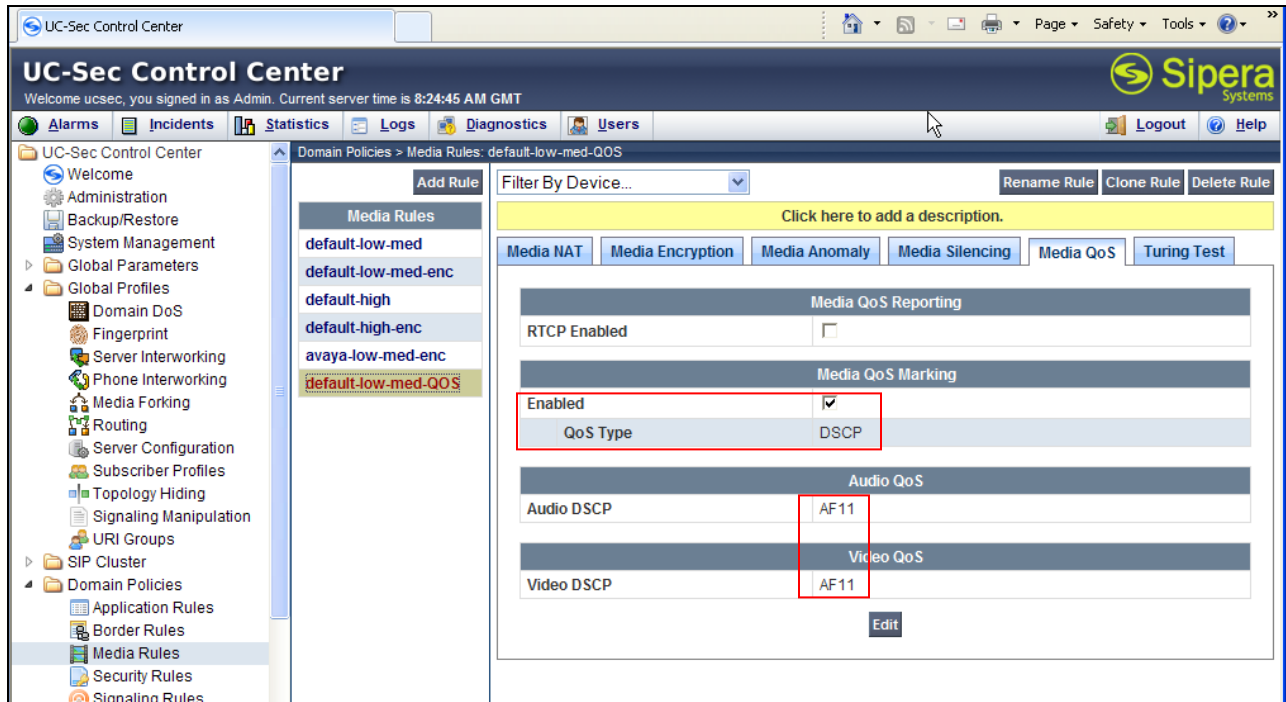


7.4.2. Media Rules

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

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Media Rules (not shown)**.
3. 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: **default-low-med-QOS**
 - a. Select the **Media QOS** tab
 - b. Click the **Edit** button
 - c. Check the **Media QOS Marking Enabled**
 - d. Check the **DSCP** box
 - e. **Audio**: Select **AF11** from the drop-down
 - f. **Video**: Select **AF11** from the drop-down

6. Click **Finish** (not shown). The following screenshot shows the completed form.



7.4.3. Signaling Rules

Signaling Rules may be used to remove or block various SIP headers as well as setting signaling QoS parameters.

Note – SIP headers may also be removed by defining scripts in the Global profiles → Signaling Manipulation function. However, Signaling Rules are a more efficient use of Avaya SBCE resources.

7.4.3.1 Avaya - Requests

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

Note – In the reference configuration the History-Info header is removed by Communication Manager (see **Section 5.7.1, Step 5**). Using the Signaling Rules to remove History-Info is included here for informational purposes.

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

Edit Header Control	
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
<div>486 Busy Here</div>	
Finish	

7. **OPTIONAL** (see note above), repeat **Steps 5** and **6** to create a rule to remove the History-Info header.

Edit Header Control	
Proprietary Request Header?	<input type="checkbox"/>
Header Name	History-Info
Method Name	INVITE
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional
Presence Action	Remove header
<div>486 Busy Here</div>	
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	History-Info	INVITE	Forbidden	Remove Header	No	IN	 

7.4.3.2 Avaya - Responses

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

Note – In the reference configuration the History-Info header is removed by Communication Manager (see **Section 5.7.1, Step 5**). Using the Signaling Rules to remove History-Info is included here for informational purposes.

- Highlight the **Avaya_SR** rule created in **Section 7.4.3.1** and enter the following:
 - Select the **Response Headers** tab (not shown).
 - Click the **Edit** button and the **Edit Header Control** window will open.
 - Verify the **Proprietary Request Header** box is unchecked.
 - From the **Header Name** menu select **History-Info**.
 - From the **Response Code** menu select **1xx**.
 - From the **Method Name** menu select **Invite**.
 - For **Header Criteria** select **Forbidden**.
 - From the **Presence Action** menu select **Remove Header**.
- Click **Finish**

Edit Header Control ✕

Proprietary Response Header?	<input type="checkbox"/>
Header Name	<div style="border: 1px solid #ccc; padding: 2px;">History-Info ▼</div>
Response Code	<div style="border: 1px solid #ccc; padding: 2px;">1XX ▼</div>
Method Name	<div style="border: 1px solid #ccc; padding: 2px;">INVITE ▼</div>
Header Criteria	<input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional
Presence Action	<div style="border: 1px solid #ccc; padding: 2px;">Remove header ▼</div> <div style="display: inline-block; border: 1px solid #ccc; padding: 2px; margin-left: 5px;">488</div> <div style="display: inline-block; border: 1px solid #ccc; padding: 2px; margin-left: 5px; background-color: #eee;">Busy Here</div>
<div style="background-color: #333; color: white; padding: 5px 15px; cursor: pointer;">Finish</div>	

3. Repeating **Steps 1** and **2**, 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 **History-Info**.
 - 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”.

General Requests Responses Request Headers Response Headers Signaling QoS									
Add In Header Control Add Out Header Control									
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	History-Info	1XX	INVITE	Forbidden	Remove Header	No	IN		
2	History-Info	200	INVITE	Forbidden	Remove Header	No	IN		

7.4.3.3 Avaya – Signaling QoS

1. Highlight the **Avaya_SR** rule created in **Section 7.4.3.1** and enter the following:
 - Select the **Signaling QoS** tab (not shown).
 - Click the **Edit** button and the **Signaling QoS** window will open.
 - Select **DCSP**.
 - Select **Value = AF11**.
2. Click **Finish**

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

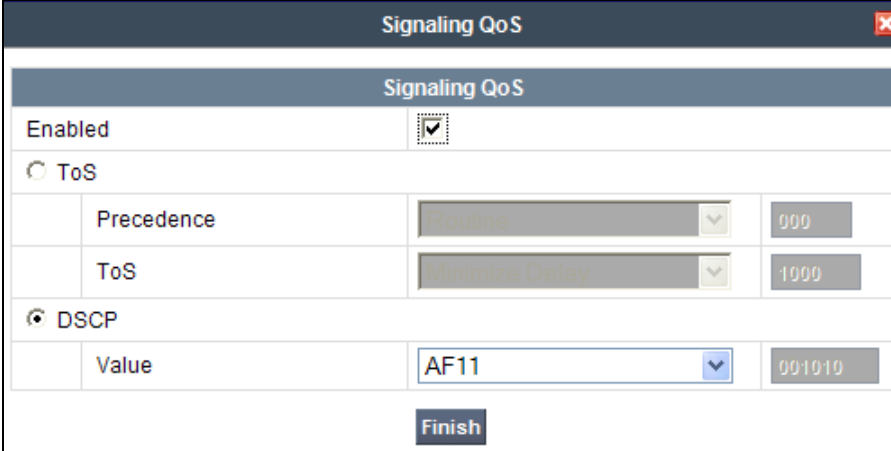
7.4.3.4 AT&T – Requests and Responses

No AT&T Request or Response Signaling Rules were required.

7.4.3.5 AT&T – Signaling QoS

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Signaling Rules** (not shown).
3. The Signaling Rules window will open (not shown). From the Signaling Rules menu, select the **default** rule.
4. Select **Clone Rule** button
 - Enter a name: **ATT_SR**
 - Click **Finish**
5. Highlight the **ATT_SR** signaling rule 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**.

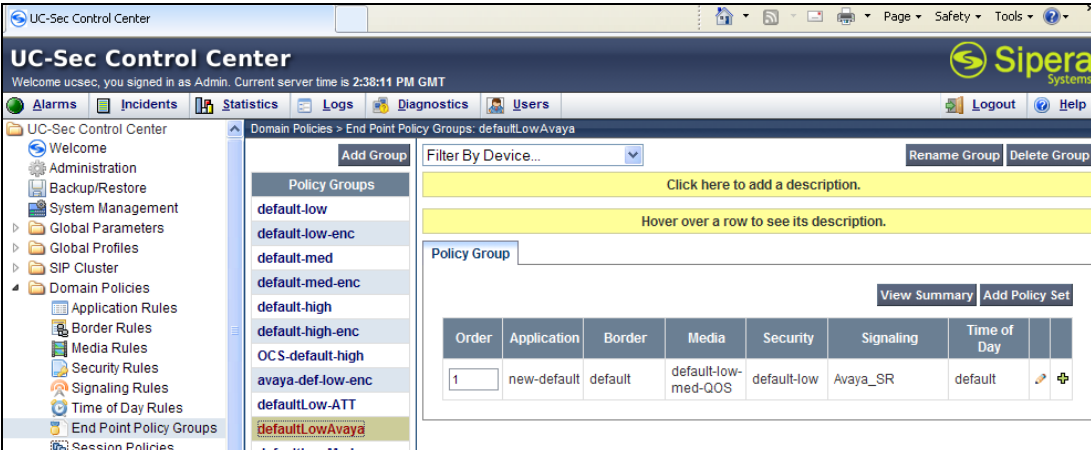
6. Click **Finish**



The image shows a 'Signaling QoS' configuration window. It has a title bar with the text 'Signaling QoS' and a close button. Below the title bar is a section header 'Signaling QoS'. There are two radio buttons: 'ToS' (unselected) and 'DSCP' (selected). Under 'ToS', there are two rows: 'Precedence' with a dropdown menu showing 'Priority' and a text box with '000', and 'ToS' with a dropdown menu showing 'Minimum Delay' and a text box with '1000'. Under 'DSCP', there is one row: 'Value' with a dropdown menu showing 'AF11' and a text box with '001010'. At the bottom right is a 'Finish' button.

7.4.4. Endpoint Policy Groups – Avaya

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
 - a) **Name:** defaultLowAvaya
 - b) **Application Rule:** new-default (created in Section 7.4.1).
 - c) **Border Rule:** default
 - d) **Media Rule:** default-low-med-QOS (created in Section 7.4.2).
 - e) **Security Rule:** default-low
 - f) **Signaling Rule:** Avaya_SR (created in Section 7.4.3.1).
 - g) **Time of Day:** default
4. Select **Finish** (not shown). The completed form is shown below.



The image is a screenshot of the UC-Sec Control Center web interface. The top navigation bar includes 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', and 'Users'. The main content area shows a tree view on the left with 'Domain Policies' expanded, and 'End Point Policy Groups' selected. A list of policy groups is shown, including 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'defaultLow-ATT', and 'defaultLowAvaya'. The 'defaultLowAvaya' group is highlighted. On the right, there is a 'Policy Group' configuration form with a table showing the selected rules for this group.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	new-default	default	default-low-med-QOS	default-low	Avaya_SR	default

7.4.5. Endpoint Policy Groups – AT&T

1. Select **Domain Policies** from the menu on the left-hand side
2. Select **End Point Policy Groups**
3. Select **Add Group**
 - a. **Name:** defaultLow-ATT
 - b. **Application Rule:** new-default (created in Section 7.4.1).
 - c. **Border Rule:** default
 - d. **Media Rule:** default-low-med-QOS (created in Section 7.4.2).
 - e. **Security Rule:** default-low
 - f. **Signaling Rule:** ATT_SR (created in Section 7.4.3.5).
 - g. **Time of Day:** default
4. Select **Finish** (not shown). The completed form is shown below.

The screenshot displays the UC-Sec Control Center web interface. The left-hand navigation pane shows the 'Domain Policies' menu expanded, with 'End Point Policy Groups' selected. The main content area shows the configuration for the 'defaultLow-ATT' policy group. The 'Policy Groups' list on the left includes 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', 'avaya-def-low-enc', 'defaultLow-ATT' (highlighted), 'defaultLowAvaya', and 'defaultLowMed'. The 'Add Group' button is visible. The 'Filter By Device...' dropdown is set to 'defaultLow-ATT'. The 'Click here to add a description.' button is present. The 'Hover over a row to see its description.' message is displayed. The 'Policy Group' section shows a table with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and Actions. The table contains one row with the following values: Order 1, Application new-default, Border default, Media default-low-med-QOS, Security default-low, Signaling ATT_SR, Time of Day default, and Actions (edit and delete icons). The 'View Summary' and 'Add Policy Set' buttons are also visible.

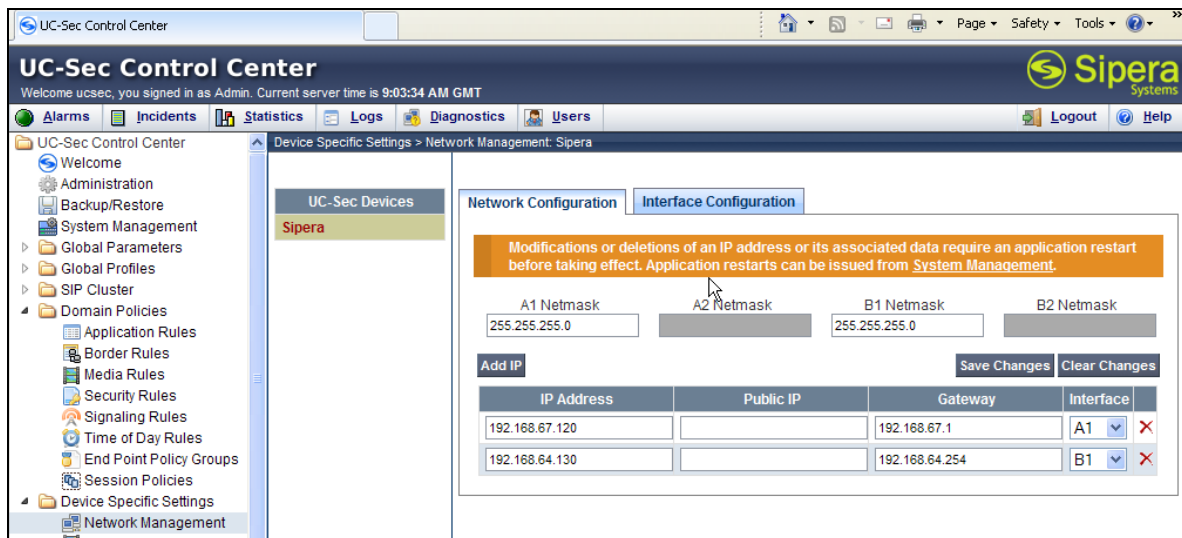
Order	Application	Border	Media	Security	Signaling	Time of Day	Actions
1	new-default	default	default-low-med-QOS	default-low	ATT_SR	default	

7.5. Device Specific Settings

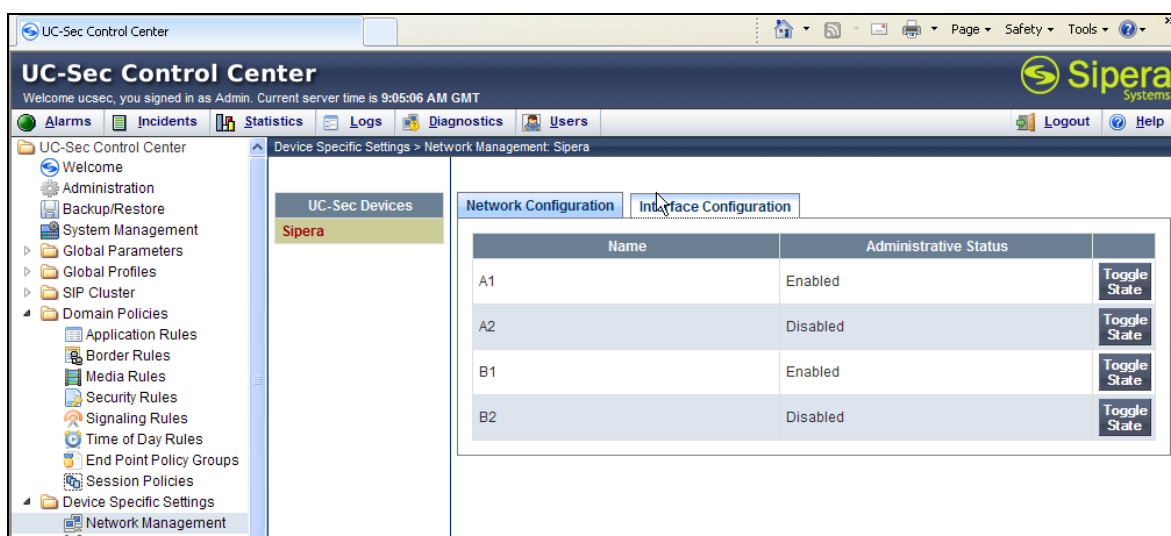
The **Device Specific Settings** feature for SIP allows you to view system information, and manage various device-specific network parameters such as port ranges.

7.5.1. Network Management

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



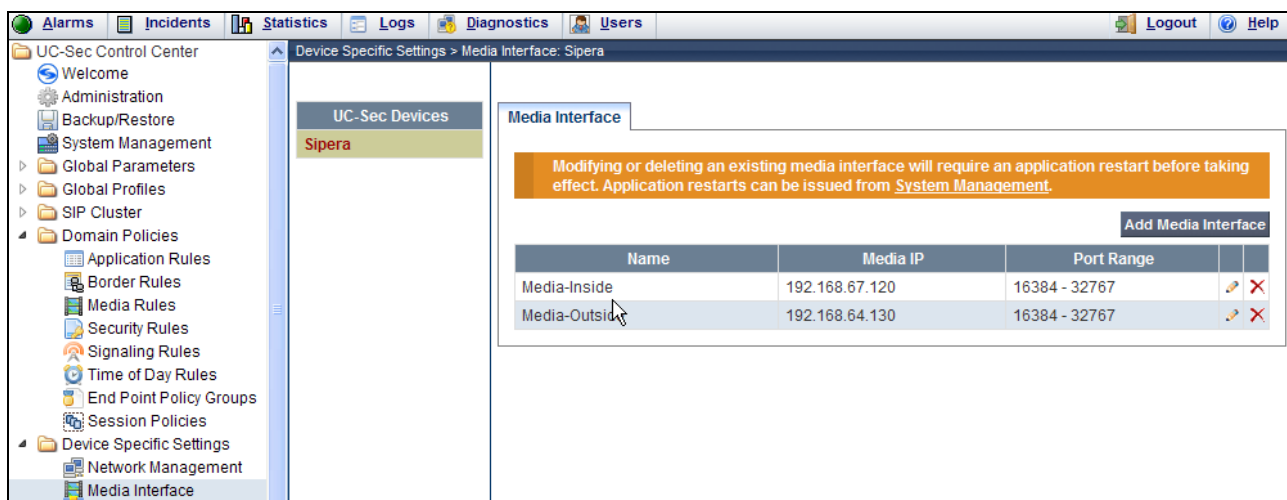
3. In addition, the provisioned interfaces may be enabled/disabled via the **Interface Configuration Tab**.
 - a) Toggle the State of the physical interfaces being used.



7.5.2. Media Interfaces

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

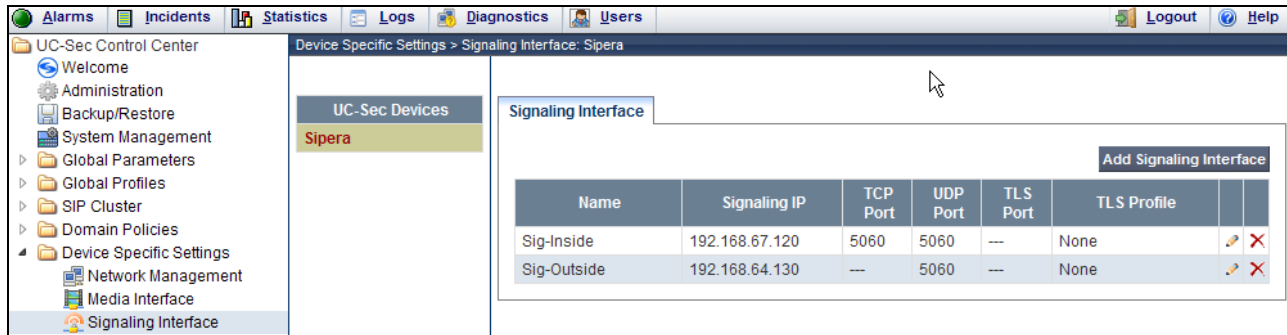
1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Media Interface**
3. Select **Add Media Interface**
 - a) **Name: Media-Inside**
 - b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Communication Manager)
 - c) **Port Range: 16384 - 32767**
4.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



7.5.3. Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Signaling Interface**
3. Select **Add Signaling Interface**
 - a) **Name: Sig-Inside**
 - b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Communication Manager)
 - c) **TCP Port: 5060**
 - d) **UDP Port: 5060**
4. Click **Finish** (not shown)
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** (not shown). The completed form is shown below.



7.5.4. Endpoint Flows – To Avaya Communication 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** (if not visible, scroll the screen to the right to find this button), and enter the following:
 - a) **Name: Avaya**
 - b) **Server Configuration: Avaya_SC**
 - c) **URI Group: ***
 - d) **Transport: ***
 - e) **Remote Subnet: ***
 - f) **Received Interface: Sig-Outside**
 - g) **Signaling Interface: Sig-Inside**
 - h) **Media Interface: Media-Inside**
 - i) **End Point Policy Group: defaultLowAvaya**
 - j) **Routing Profile: To_ATT**
 - k) **Topology Hiding Profile: Avaya_TH**
 - l) **File Transfer Profile: None**
5. Click **Finish** (not shown).

7.5.5. Endpoint Flows – To AT&T

1. Repeat Section 7.5.4, Steps 1 - 3.
2. Select **Add Flow** and enter the following:
 - a) **Name: ATT**
 - b) **Server Configuration: ATT_SC**
 - 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_TH**
 - l) **File Transfer Profile: None**
3. Click **Finish** (not shown). The completed form is shown below.

UC-Sec Control Center

Device Specific Settings > End Point Flows: A-SBCE

UC-Sec Devices

A-SBCE

Subscriber Flows | Server Flows

Server Configuration: ATT_SC

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

Server Configuration: Avaya_SC

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

7.6. Troubleshooting Port Ranges

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

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

Alarms | Incidents | Statistics | Logs | Diagnostics | Users | Logout | Help

UC-Sec Control Center

Troubleshooting > Advanced Options: Sipera

UC-Sec Devices

EMS

Sipera

Subsystem Logs | CDR Listing | Feature Control | SIP Options | Port Ranges | Active Registrations

Changes to the settings below require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Port Range Configuration

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

Save

8. Verification Steps

The following steps may be used to verify the configuration:

8.1. General

1. Place an inbound AT&T IP Toll Free call from PSTN, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, local transfer, and local conference.
3. Verify the use of DTMF signaling.
4. Place an inbound call to a telephone or agent, but do not answer the call. Verify that the call covers to Avaya Aura® Messaging voicemail. Retrieve the message from Avaya Aura® Messaging either locally or from PSTN.

8.2. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See documents [1] and [2] 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 Communication Manager has previously converted the AT&T IP Toll Free DNIS number included in the Request URI, to extension 19011, using the incoming-call-handling-treatment form shown in **Section 5.8**.

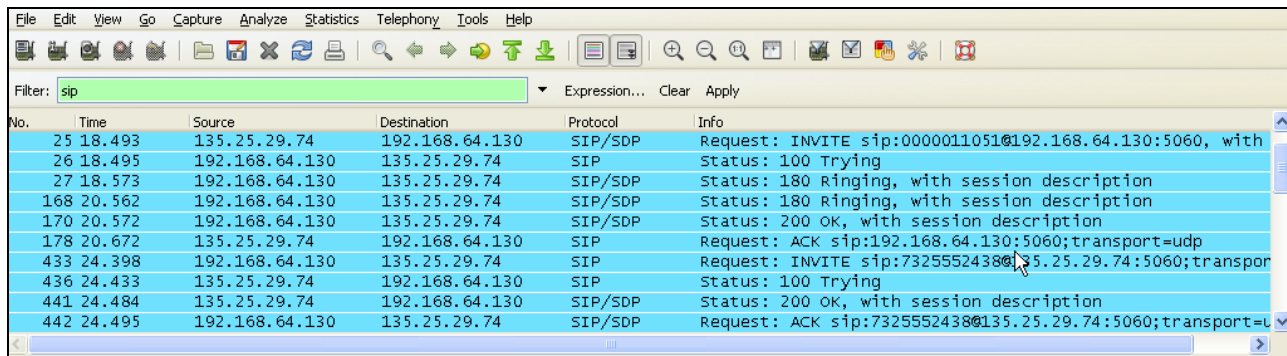
```
list trace tac *04                                     Page 1
                                                    LIST TRACE
time          data
09:05:40 TRACE STARTED 07/25/2012 CM Release String cold-02.0.823.0-19593
09:05:47 SIP<INVITE sip:19011@sip.customerc.com SIP/2.0
09:05:47      Call-ID: 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>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>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*.

8.3. Protocol Traces

Using a SIP protocol analyzer (e.g., Wireshark), monitor the SIP traffic at the Avaya SBCE public outside interface connection to the AT&T IP Toll Free service.

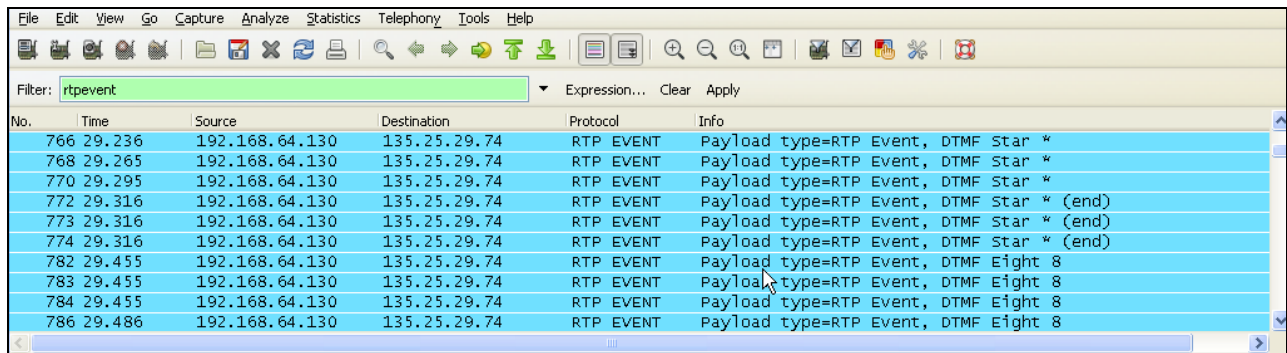
The following are examples of inbound calls filtering on the SIP protocol.



Filter: sip

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

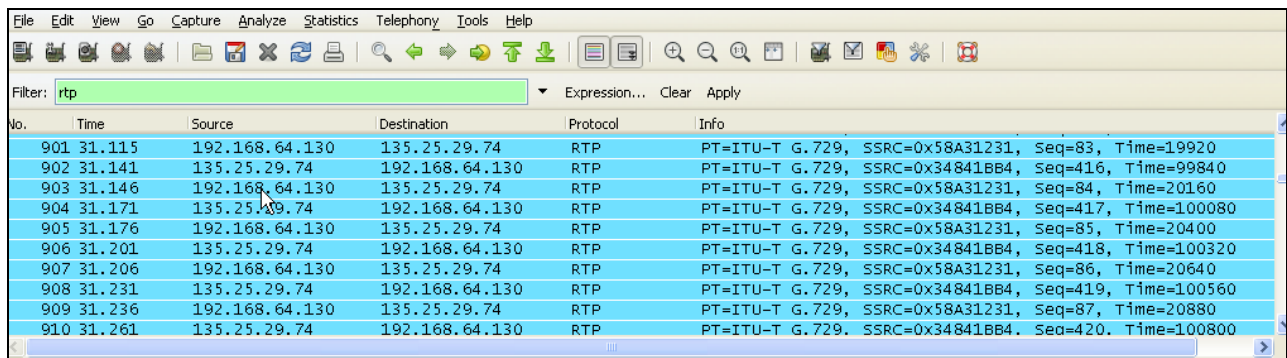
The following is an example of a call filtering on DTMF.



Filter: rtpevent

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

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

8.4. 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 screenshot shows the UC-Sec Control Center web interface. The left sidebar contains a navigation tree with 'Troubleshooting' expanded and 'Trace Settings' selected. The main content area is titled 'Troubleshooting > Trace Settings: Sipera'. It features four tabs: 'Packet Trace', 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is active, displaying the 'Packet Capture Configuration' form. The form includes the following fields: 'Currently capturing' (No), 'Interface' (B1), 'Local Address (ip:port)' (192.168.64.130), 'Remote Address (*, *:port, ip, ip:port)' (135.25.29.74), 'Protocol' (All), 'Maximum Number of Packets to Capture' (1000), and 'Capture Filename' (inbound_test_call.pcap). A note states: 'Existing captures with the same name will be overwritten'. At the bottom of the form are 'Start Capture' and 'Clear' buttons.

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

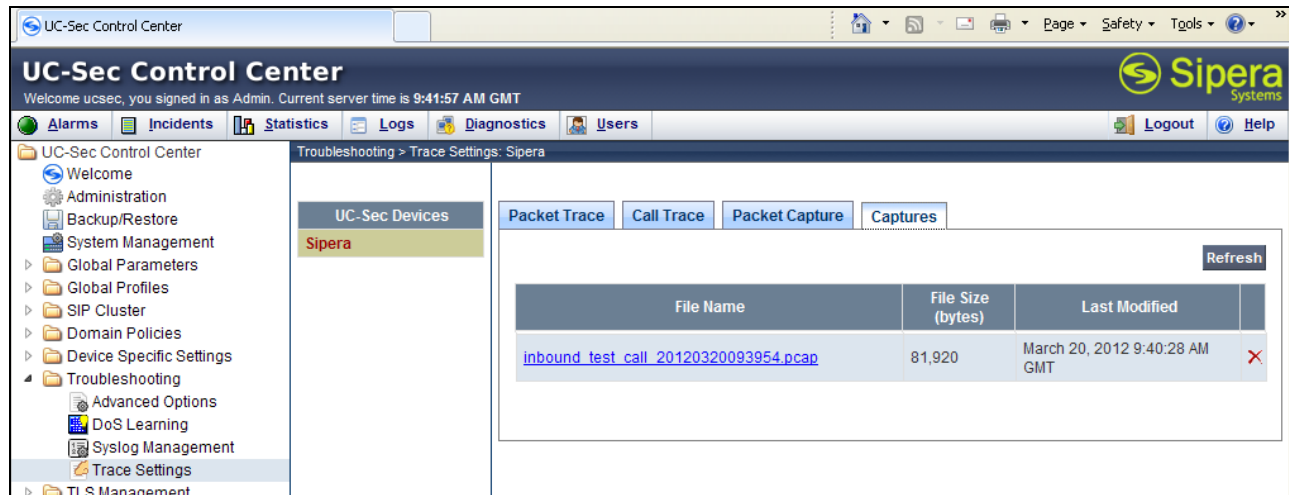
This screenshot shows the same UC-Sec Control Center interface as the previous one, but the 'Packet Capture' tab now displays a status message: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.' Below this message, the 'Packet Capture Configuration' form is shown with updated values: 'Currently capturing' (Yes), 'Interface' (B1), 'Local Address (ip:port)' (192.168.64.130), 'Remote Address (*, *:port, ip, ip:port)' (135.25.29.74), 'Protocol' (All), 'Maximum Number of Packets to Capture' (1000), and 'Capture Filename' (inbound_test_call.pcap). A 'Stop Capture' button is now visible at the bottom right of the configuration area.

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 a packet capture analysis application such as Wireshark to open the trace.



9. Conclusion

As illustrated in these Application Notes, 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 Toll Free service, within the limitations stated in **Section 2.2.1**.

This solution provides users of Avaya Aura® Communication Manager the ability to support inbound toll free calls over an AT&T IP Toll Free SIP trunk service connection.

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.

10. References

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

Avaya Aura® Communication Manager

- [1] *Administering Avaya Aura® Communication Manager* Release 6.2, 03-300509, Issue 7.0, July 2012
- [2] *Implementing Avaya Aura® Communication Manager*, 03-603558, Issue 3, Release 6.2, July 2012
- [3] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya Aura® Messaging

- [4] *Administering Avaya Aura® Messaging, 6.1*, CID: 151610, December 2011
- [5] *Implementing Avaya Aura® Messaging 6.1*, CID: 150976, October 2011

Avaya Session Border Controller for Enterprise

Product documentation for UC-Sec is provided on the installation CD provided with the device.

- [6] *E-SBC 1U Installation Guide, Release 4.0.5*, Part Number: 101-5225-405v1.00, Release Date: November 2011
- [7] *E-SBC Administration Guide, Release 4.0.5*, Part Number: 010-5424-405v1.00, Release Date: November 2011

Avaya Application Notes

- [8] Avaya application notes are available at:
<https://www.devconnectmarketplace.com/at-t/at-t-sip-trunking>, then select *Resources*.

AT&T IP Toll Free Service Descriptions:

- [9] AT&T IP Toll Free Service description -
<http://www.business.att.com/enterprise/Service/business-voip-enterprise/network-based-voip-enterprise/ip-toll-free-enterprise/>

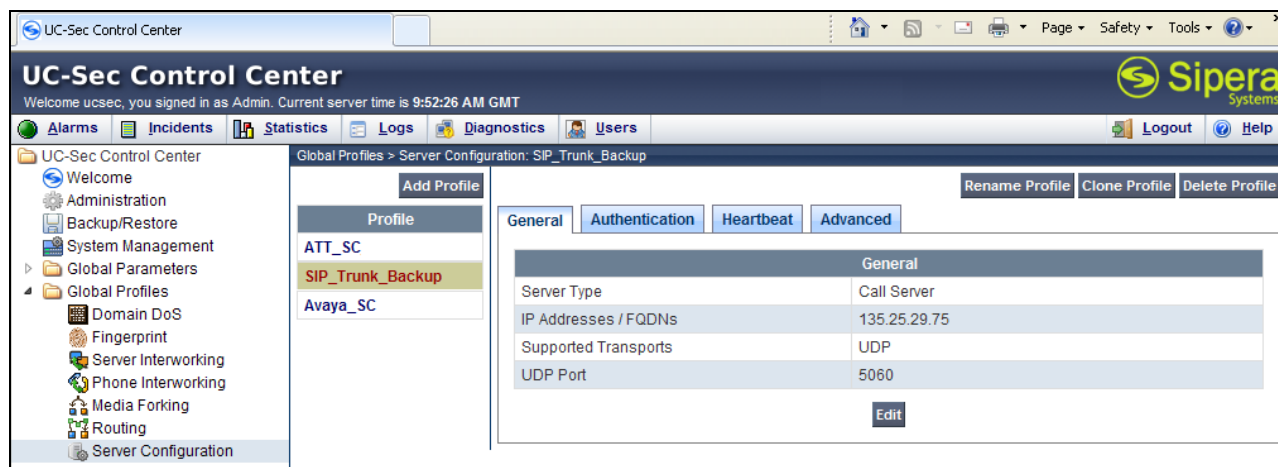
11. Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements

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 7.3.6**).

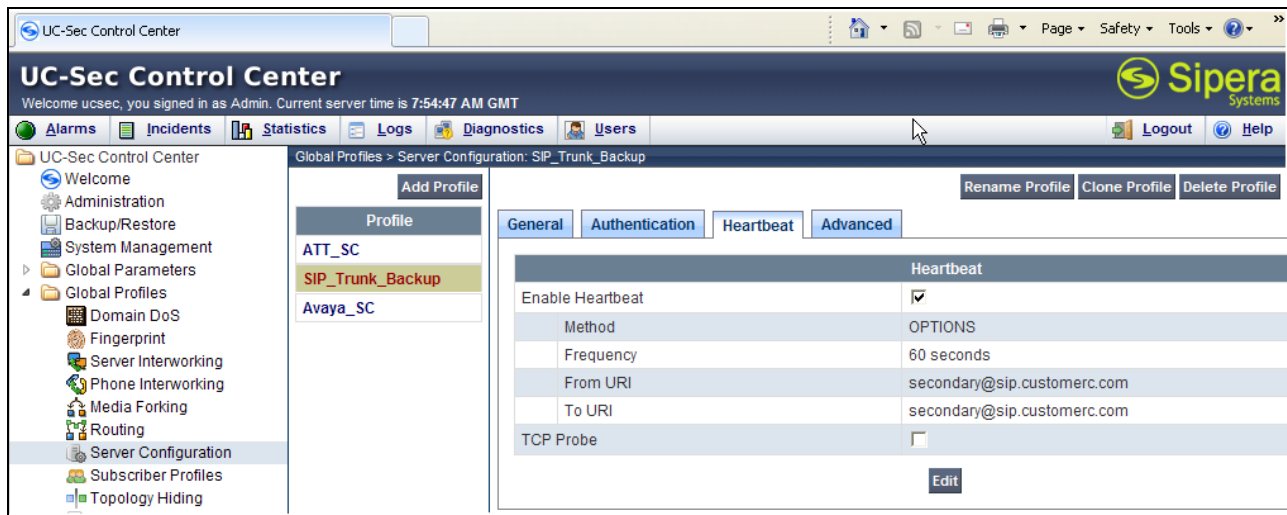
Step 1: Configure the Secondary Location in Server Configuration

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**
 - b) Select **Next** (not shown)
4. On the **Add Server Configuration Profile – General** tab:
 - a) Select **Server Type: Call 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)

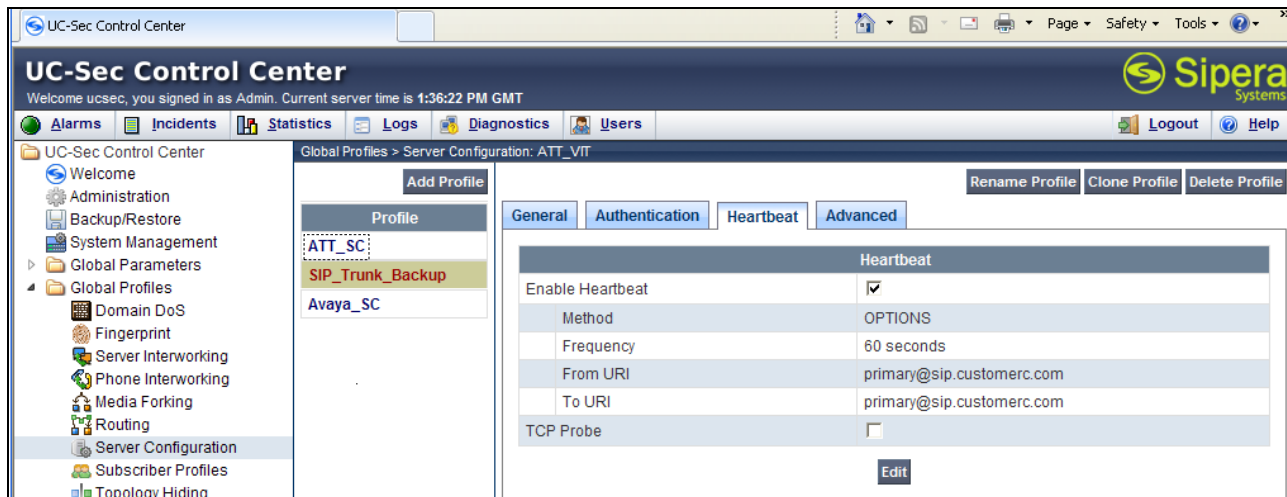


5. On the **Authentication** tab
 - a) Select **Next** (not shown)
6. On the **Heartbeat** tab (The Heartbeat must be enabled on the Primary trunk also)
 - a) Check **Enable Heartbeat**
 - b) **Method: OPTIONS**
 - c) **Frequency: 60 seconds**

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



Step 2: Add Secondary IP Address to Routing

1. Select **Global Profiles** from the menu on the left-hand side (not shown)
2. Select the **Routing** (not shown)

3. Select the profile created in **Section 7.3.4** (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**

Step 3: Configure End Point Flows – SIP_Trunk_backup

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown)
2. Select **Endpoint Flows** (not shown)
3. Select the **Server Flows** Tab (not shown)
4. Select **Add Flow** (not shown)
 - 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_TH**
 - l) **File Transfer Profile: None**

5. Click **Finish**

Add Flow	
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_TH
File Transfer Profile	None
Finish	

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

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® 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.