Applications Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 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, Avaya Aura® Session 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® Session Manager 6.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.0.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise is the point of connection between Avaya Aura® Session Manager and the AT&T IP 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

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

Avaya Aura® Session Manager 6.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.0.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Avaya SBCE is the point of connection between Avaya Aura® Session Manager and the AT&T IP 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/PNT[1] transport.

Note that these Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service. That solution is described in the document *Application Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1, and Avaya Session Border Controller for Enterprise AT&T IP Transfer Connect Service – Issue 1.0.*

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya phones, fax machines (Ventafax application), Avaya Session Border Controller, 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 Session Manager, Communication Manager, the Session Border Controller, 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. The following features were tested as part of this effort:

- SIP trunking.

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

- 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 the 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 are 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. If Communication Manager receives an SDP offer with multiple codecs, where at least two of the codecs are supported in the codec set provisioned on Communication Manager, then Communication Manager selects a codec according to the priority order specified in the Communication Manager codec set, not the priority order specified in the SDP offer. For example, if the AT&T IP Toll Free service offers G.711, G.729A, and G.729B in that order, but the Communication Manager codec set contains G.729B, G729A, and G.711 in that order, then Communication Manager selects G.729A, not G.711. The practical resolution is to provision the Communication Manager codec set to match the expected codec priority order in AT&T IP Toll Free SDP offers.
2. G.711 faxing is not supported between Avaya Aura® Communication Manager and the AT&T IP Toll Free service. Avaya Aura® Communication Manager does not support the protocol negotiation that AT&T requires to have G.711 fax calls work. T.38 faxing is supported, as is Group 3 and Super Group 3 fax. Fax speeds are limited to 9600 in the configuration tested. In addition, Fax Error Correction Mode (ECM) is not supported by Avaya Aura® Communication Manager in this configuration.

3. G.726 codec is not supported between Communication Manager and the AT&T IP Toll Free service.

4. Avaya A175 SIP endpoints use a fixed RTP packet interval of 20ms. This may cause higher bandwidth utilization in AVPN transport configurations.

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:

- Session Manager provides core SIP routing and integration services that enables communication between disparate SIP-enabled entities, e.g. PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.
- System Manager provides a common administration interface for centralized management of all Session Manager instances in an enterprise.
- Communication Manager provides the voice communication's services for a particular enterprise site. In the reference configuration, Communication Manager runs on an Avaya S8800 Server in a Processor Ethernet (Procr) configuration. This solution is extensible to other Avaya S8xxx Servers.
- The Avaya Media Gateway provides the physical interfaces and resources for Communication Manager. In the reference configuration, an Avaya G450 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya desk telephones are represented with Avaya A175 (SIP), 1603(H.323), 960x Series IP Telephones (running H.323 or SIP firmware), and 96x1 Series IP Telephones (running H.323 or SIP firmware), Avaya 6211 Series Analog Telephones, as well as Avaya one-X® Agent. Note that all agent telephones (hardware and software based) are H.323.
- The Avaya Session Border Controller 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[2]. UDP transport protocol is used between the Avaya SBCE and the AT&T IP Toll Free service.

[2] 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. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Avaya SBCE and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Avaya SBCE and Communication Manager.

- An existing Avaya Aura® Messaging system provides the corporate voice messaging capabilities in the reference configuration. The provisioning of Avaya Aura® Messaging is beyond the scope of this document.
- Inbound calls were placed from the PSTN via the AT&T IP Toll Free service, through the Avaya SBCE to Session Manager, which routed the call to Communication Manager. Communication Manager terminated the call to the appropriate agent/phone or fax extension. The H.323 telephones on the enterprise side register to the Communication Manager Procr interface. The SIP telephones register to Session Manager.

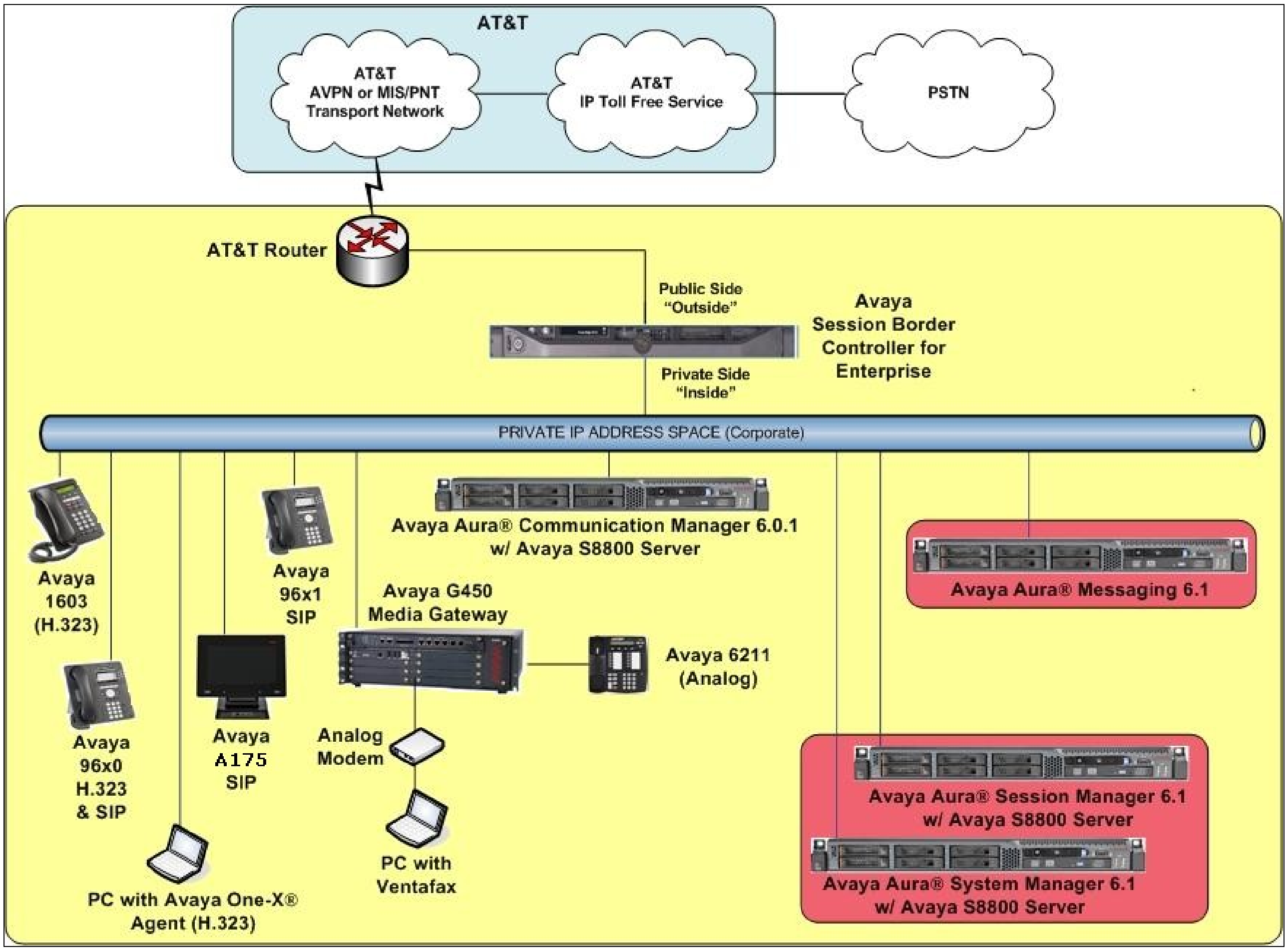

AT&T
AT&T AVPN or MIS/PNT Transport Network
AT&T IP Toll Free Service
PSTN
AT&T Router
Public Side "Outside"
Avaya Session Border Controller for Enterprise
Private Side "Inside"
PRIVATE IP ADDRESS SPACE (Corporate)
Avaya Aura® Communication Manager 6.0.1 w/ Avaya S8800 Server
Avaya Aura® Messaging 6.1
Avaya 1603 (H.323)
Avaya 96x1 SIP
Avaya G450 Media Gateway
Avaya 6211 (Analog)
Avaya 96x0 H.323 & SIP
Avaya A175 SIP
Analog Modem
PC with Ventafax
PC with Avaya One-X® Agent (H.323)
Avaya Aura® Session Manager 6.1 w/ Avaya S8800 Server
Avaya Aura® System Manager 6.1 w/ Avaya S8800 Server

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.

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.

Component	Illustrative Value in these Application Notes
Avaya Aura® System Manager	
Management IP Address	192.168.67.207
Avaya Aura® Session Manager	
Management IP Address	192.168.67.209
Network IP Address	192.168.67.210
Avaya Aura® Communication Manager	
Procr IP Address	192.168.67.202
Avaya Aura® Communication Manager extensions	40xxx = H323 and Analog 41xxx = SIP
Voice Messaging Pilot Extension	36000
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Outside (Public) Interface (connected to AT&T Access Router/IP Toll Free Service)	192.168.64.130
IP Address of Inside (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.67.120
Avaya Aura Messaging	
Messaging Application Server (MAS) IP Address	192.168.67.147
Messaging Mailboxes	4xxxx
AT&T IP Toll Free Service	
Border Element IP Address	135.25.29.74
AT&T Access router interface (to Avaya Aura® outside)	192.168.64.254
AT&T Access Router NAT address (Avaya Aura® outside address)	135.16.170.55

Table 1: Illustrative Values Used in these Application Notes

3.2. Call Flows

To understand how inbound AT&T IP Toll Free service calls are handled by Session Manager, Communication Manager, and the Avaya SBCE, 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 on Session Manager and is subsequently routed to 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 Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. 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.

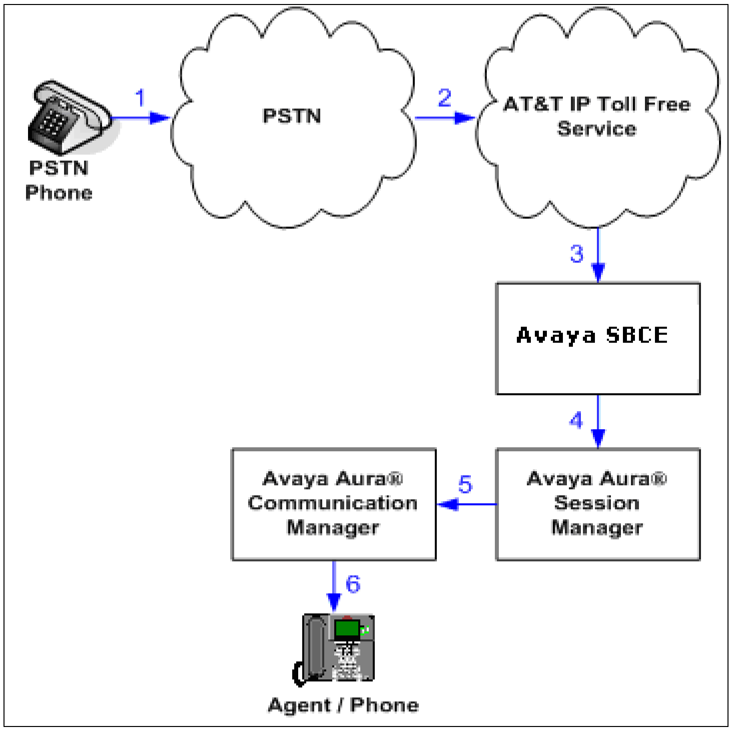

PSTN Phone
1
PSTN
2
AT&T IP Toll Free Service
3
Avaya SBCE
4
Avaya Aura® Session Manager
5
Avaya Aura® Communication Manager
6
Agent / Phone

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 Session Manager. The Avaya Aura® Messaging system is in MultiSite mode.

1. Same as the **Steps 1-5** and **Step 6b** 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 Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Avaya Aura® Messaging. Avaya Aura® Messaging answers the call and connects the caller to the called agent's or telephone's voice mailbox. Note that the call continues to go through Communication Manager.

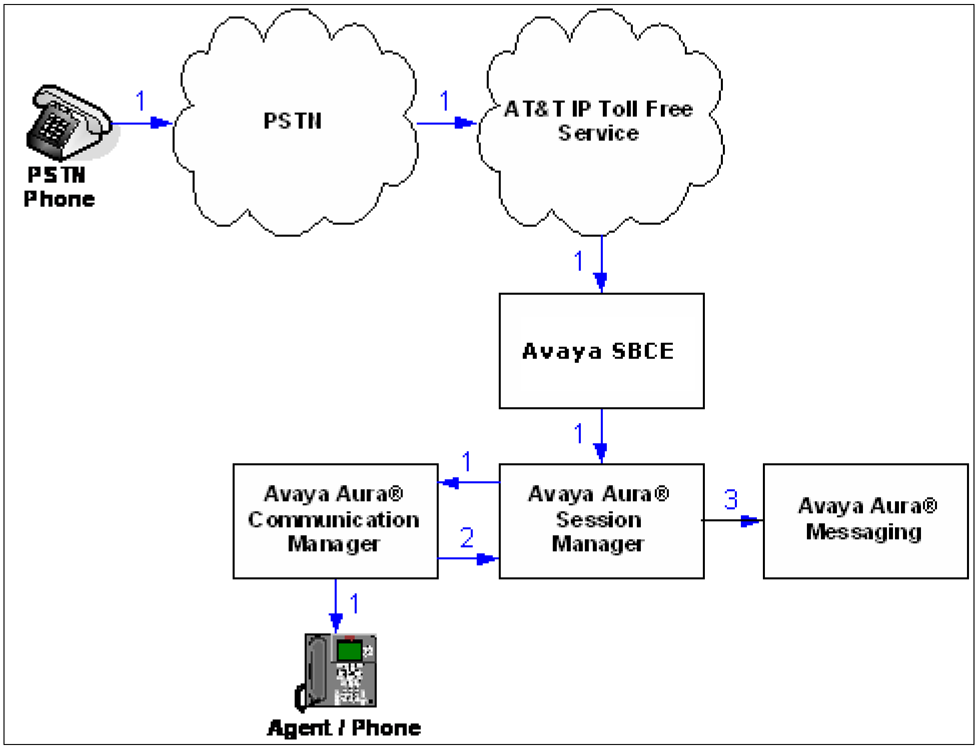

PSTN Phone
1
PSTN
1
AT&T IP Toll Free Service
1
Avaya SBCE
1
1
Avaya Aura® Communication Manager
2
Avaya Aura® Session Manager
3
Avaya Aura® Messaging
1
Agent / Phone

Figure 3: Inbound AT&T IP Toll Free Service Call to Agent / Telephone 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.

Component	Version
Avaya S8800 Server	Avaya Aura® System Manager 6.1 SP6 (System Manager 6.1.5.0 Build Number 6.1.0.0.7345 Patch 6.1.5.606 Build Number 6.1.10.1.1774) System Platform 6.0.3.6.3
Avaya S8800 Server	Avaya Aura® Session Manager 6.1 (6.1.6.0.616008)
Avaya S8800 Server	Avaya Aura® Communication Manager 6.0.1 SP7 (R016x.00.1.510.1-19528) System Platform 6.0.3.6.3
Dell R610	Avaya Aura® Messaging 6.1 with SP0 (00.1.510.1-115_0006) System Platform 6.0.3.6.3
Avaya G450 Media Gateway	31.20.1
MM711 Analog card	HW31 FW094
Dell R310	Avaya Session Border Controller for Enterprise 4.0.5.Q02
Avaya 9630 IP Telephone	H.323 Version S3.103S (ha96xxua3_1_03_S.bin) SIP Version 2.6.6 (SIP96xx_2_6_6_0.bin)
Avaya 9621 IP Telephone	SIP Version 6.0.1 (S96x1_SALBR6_0_3_V470)
Avaya A175 Flare™ Desktop Video Device (SIP telephone function)	SIP Version 1.1.0 (SIP_A175_1_1_0_012004)
Avaya one-X® Agent	2.5.00467.0
Avaya 1603 IP Telephone	H323 (ha1603ua1_3100.bin)
Avaya 6211 Analog telephone	-
Fax device	Ventafax Home Version 6.1.59.144
AT&T IP Toll Free Service using AVPN/MIS-PNT transport service connection	VNI 21

Table 2: Equipment and Software Versions

5. Configure Avaya Aura® Session Manager Release 6.1

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

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [1] through [4] for further details if necessary.

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

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

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

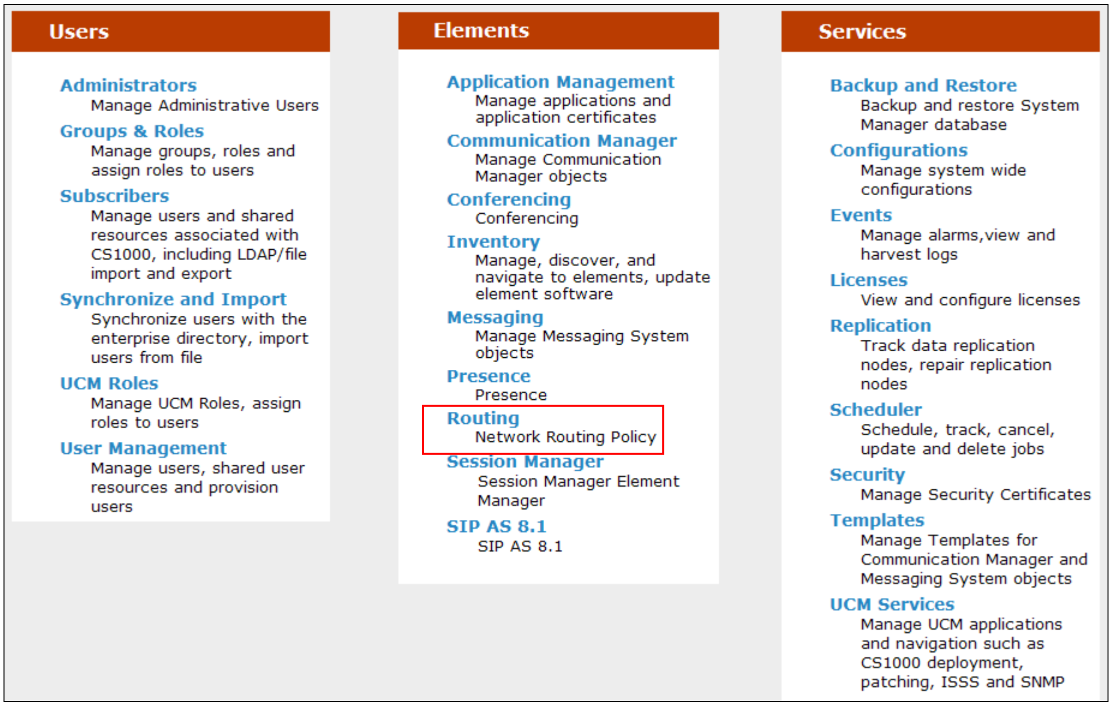
The following administration activities will be described:

- Define SIP Domain(s)
- Define Locations for Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Define SIP Entities corresponding to Communication Manager, the Avaya SBCE, and Avaya Aura® Messaging.
- Define Entity Links describing the SIP trunk between Communication Manager and Session Manager, the SIP Trunk between Session Manager and the Avaya SBCE, and the SIP trunk between Session Manager and Avaya Aura® Messaging.

- Define Routing Policies associated with Communication Manager, the Avaya SBCE and Avaya Aura® Messaging.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

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

In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.



Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Subscribers
Manage users and shared resources associated with CS1000, including LDAP/file import and export

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

UCM Roles
Manage UCM Roles, assign roles to users

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

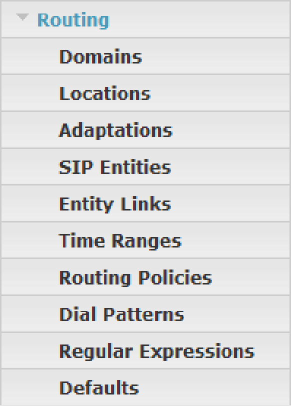
Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

The screen shown below shows the various sub-headings of the left navigation menu that will be referenced in this section.

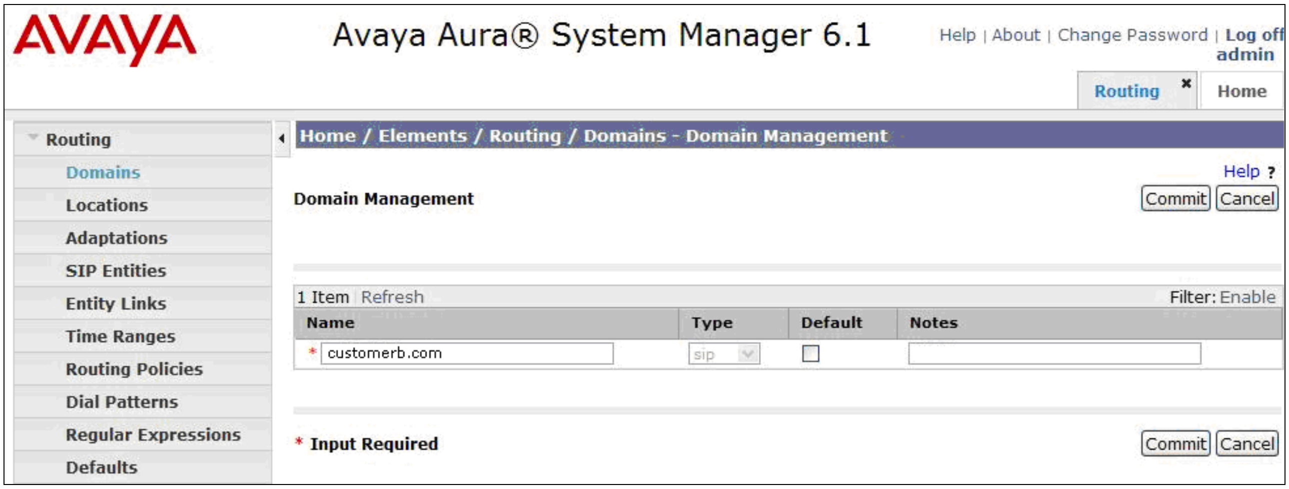


5.1. SIP Domain

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

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

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



Domain Management

Name	Type	Default	Notes
* customerb.com	sip	□	

* Input Required

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

Note - Multiple SIP Domains may be defined if required.

5.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g., 192.168.67.x for all devices on a particular subnet), or individual devices (e.g., 192.168.67.202 for a device's specific IP address). In the reference configuration, Communication Manager, Avaya Aura® Messaging, and the Avaya SBCE were each defined as individual Locations.

5.2.1. Location for Avaya Aura® Communication Manager

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

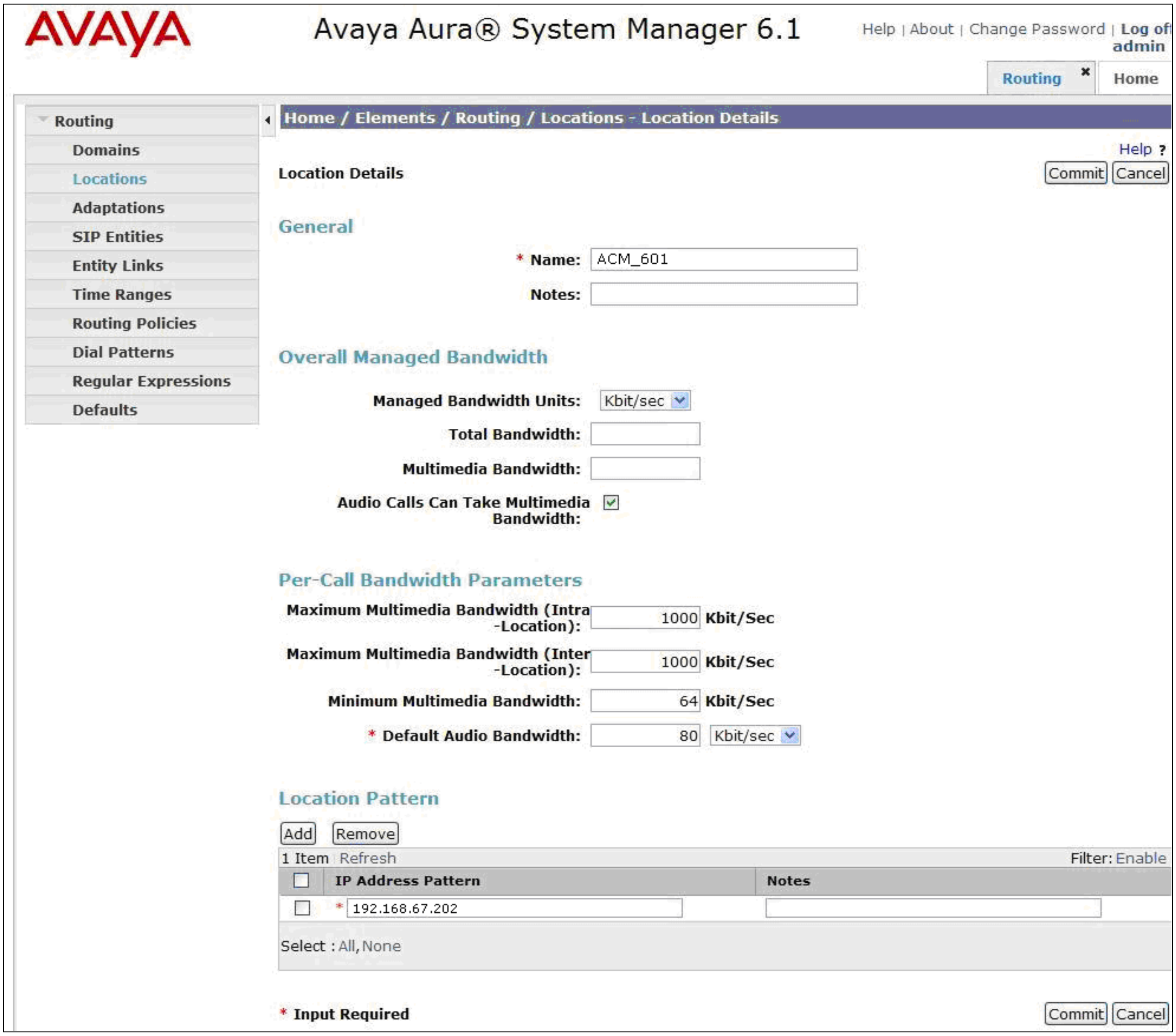
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

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

- **IP Address Pattern:** Enter the IP Address used to identify the Communication Manager location (e.g., **192.168.67.202**).
- **Notes:** Add a brief description. [Optional]

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

The screen below shows the Location Details defined for Communication Manager.



Home / Elements / Routing / Locations - Location Details

Location Details

General

* Name:	ACM_601
Notes:	

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):	1000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	1000 Kbit/Sec
Minimum Multimedia Bandwidth:	64 Kbit/Sec
* Default Audio Bandwidth:	80 Kbit/sec

Location Pattern

□	IP Address Pattern	Notes
□	* 192.168.67.202	

* Input Required

5.2.2. Location for the Avaya Session Border Controller for Enterprise

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

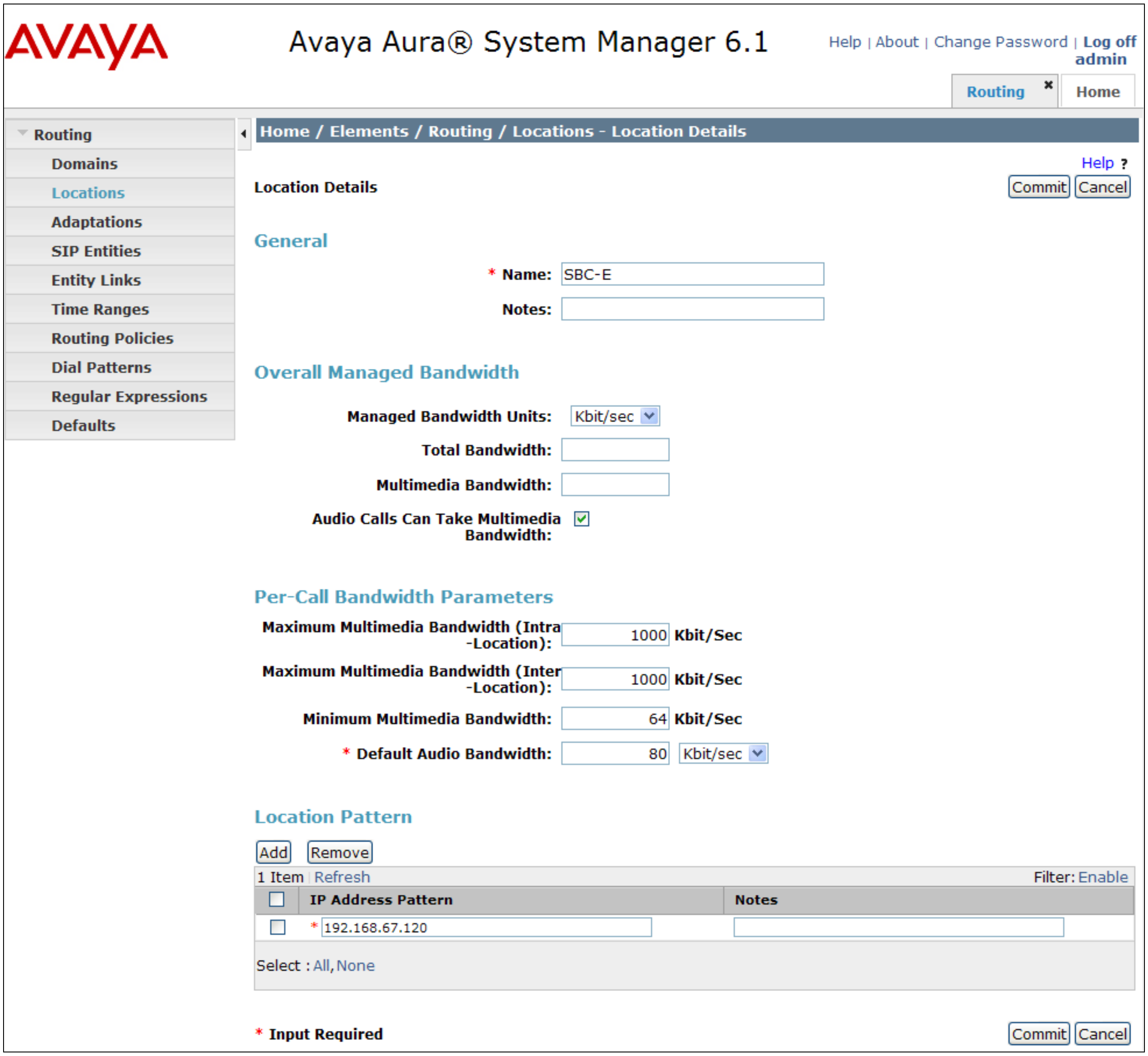
- **Name:** Enter a descriptive name for the location.

- **Notes:** Add a brief description. [Optional]

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

- **IP Address Pattern:** Enter the IP Address or IP Address pattern used to identify the Avaya SBCE location (e.g., **192.168.67.120**).
- **Notes:** Add a brief description. [Optional]

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



Location Details

General

* Name: SBC-E

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

1 Item | Refresh Filter: Enable

□	IP Address Pattern	Notes
□	* 192.168.67.120	

Select : All, None

* Input Required

Commit Cancel

5.2.3. Location for Avaya Aura® Messaging

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

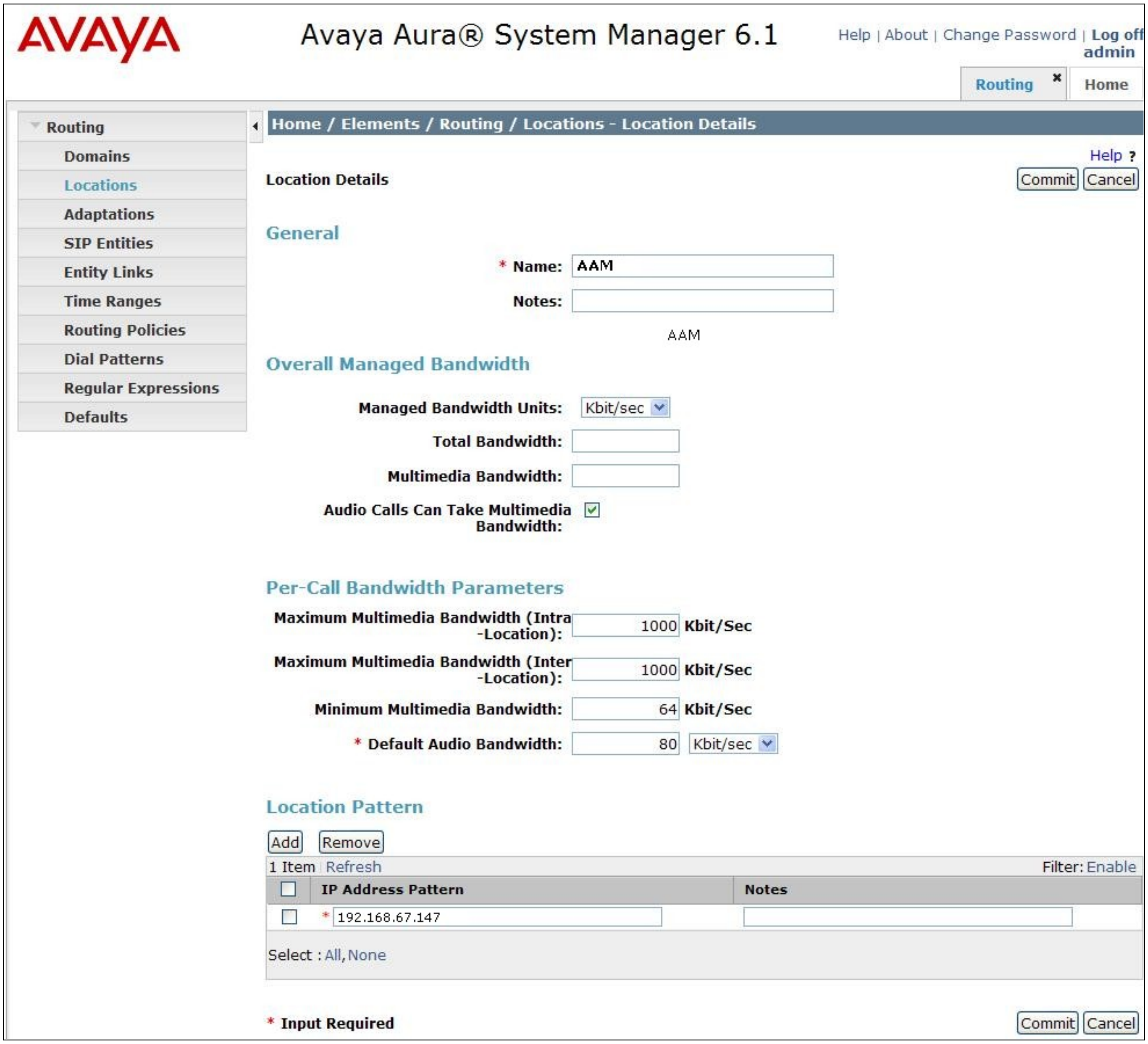
- **Name:** Enter a descriptive name for the location (e.g., **AAM**).

- **Notes:** Add a brief description. [Optional]

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

- **IP Address Pattern:** Enter the IP Address used to identify the Avaya Aura® Messaging location (e.g., **192.168.67.147**).
- **Notes:** Add a brief description. [Optional]

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



Location Details

General

* Name:	AAM
Notes:	

AAM

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):	1000	Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	1000	Kbit/Sec
Minimum Multimedia Bandwidth:	64	Kbit/Sec
* Default Audio Bandwidth:	80	Kbit/sec

Location Pattern

□	IP Address Pattern	Notes
□	* 192.168.67.147	

* Input Required

5.2.4. Location for Other CPE Devices

The location **main** is used as a wild card for any other CPE devices that may source traffic to Session Manager (e.g., SIP telephones registered to Session Manager). In the Reference configuration Session Manager was assigned to this location. Note that a specific location like those described in the previous section could have been used as well.

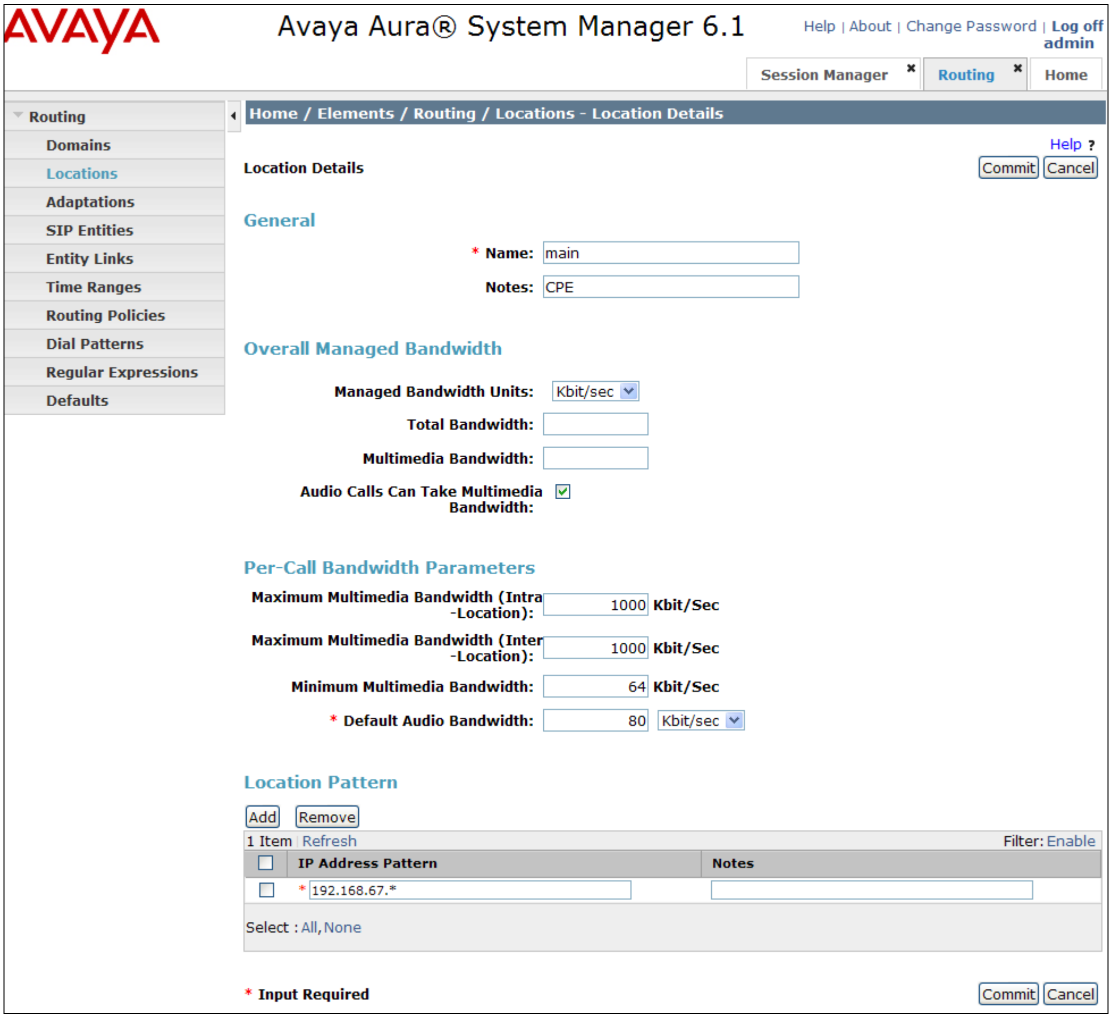
Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

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

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

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



Location Details

General

* Name: main

Notes: CPE

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

□	IP Address Pattern	Notes
□	* 192.168.67.*	

5.3. Configure Adaptations

Session Manager can be configured to use Adaptation Modules to convert SIP headers in messages sent by AT&T, before those messages are routed to Communication Manager, and for messages between Communication Manager and Avaya Aura® Messaging. In the reference configuration the following adaptations were used.

In the reference configuration, Adaptations are administered for the following purposes:

- Calls from AT&T (**Section 5.3.1**) - Modification of SIP messages sent to Communication Manager.
    - The IP address of Session Manager (192.168.67.210) is replaced with the Avaya CPE SIP domain (**customerb.com**) in the Request URI.
    - The AT&T called number digit strings in the Request URI are replaced with their associated Communication Manager extensions/VDNs.

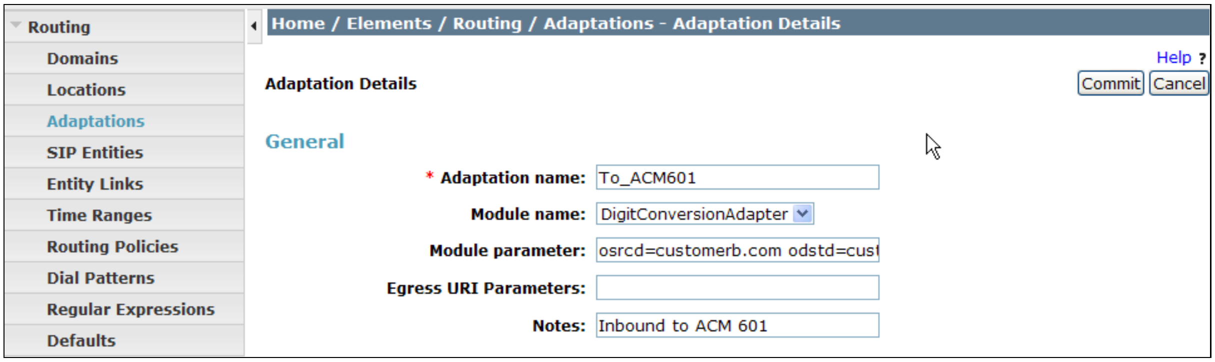
5.3.1. Adaptation for calls to Avaya Aura® Communication Manager

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager from AT&T.

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

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

- A descriptive **Name**, (e.g., **To_ACM601**).
- Select **DigitConversionAdapter** from the **Module Name** drop down menu (if no module name is present, select <click to add module> and enter **DigitConversionAdapter**).
- In the **Module parameter** field enter **odstd=customerb.com osrcd=customerb.com.** The odstd parameter will replace the IP address of Session Manager (*192.168.67.210*) with *customerb.com* in the *inbound* Request URI, and the osrcd parameter will replace the AT&T border element IP address (*135.25.29.74*) with *customerb.com* in the PAI header.



Adaptation Details

General

* Adaptation name: To_ACM601

Module name: DigitConversionAdapter

Module parameter: osrcd=customerb.com odstd=cust

Egress URI Parameters:

Notes: Inbound to ACM 601

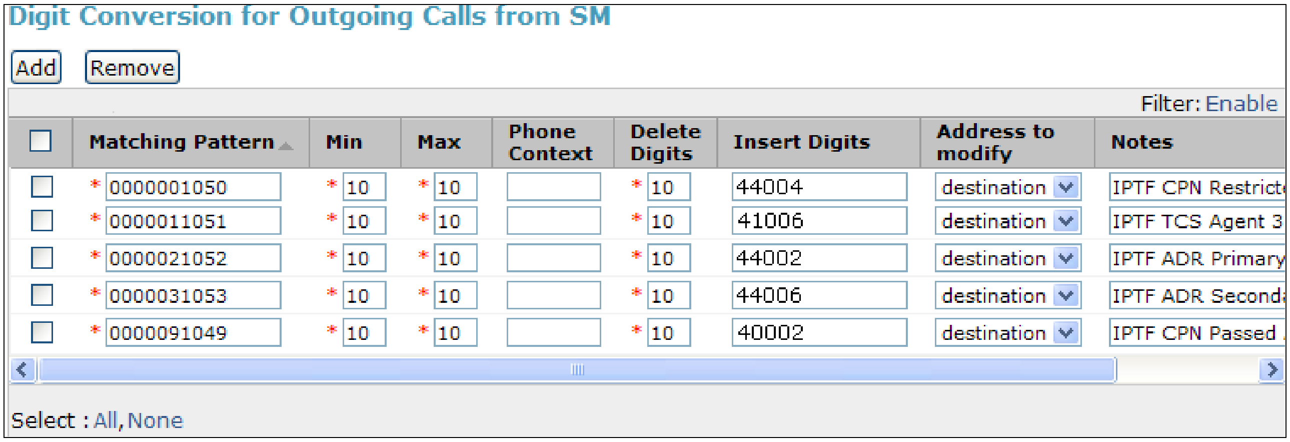
Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* digits from AT&T that need to be replaced with their associated Communication Manager extensions before being sent to Communication Manager).

- Example: 0000091049 is a digit string sent in the Request URI by AT&T Toll Free service that is associated with Communication Manager extension 40002.
  - Enter **0000091049** in the **Matching Pattern** column.
  - Enter **10** in the **Min/Max** columns.
  - Enter **10** in the **Delete Digits** column.
  - Enter **40002** string in the **Insert Digits** column.
  - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
  - Enter any desired notes.

Step 4 – Repeat **Step 3** for all additional AT&T DID numbers.

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

Note - In the reference configuration no **Digit Conversion for Incoming Calls to SM** were required.



Digit Conversion for Outgoing Calls from SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
□	* 0000001050	* 10	* 10		* 10	44004	destination	IPTF CPN Restrict
□	* 0000011051	* 10	* 10		* 10	41006	destination	IPTF TCS Agent 3
□	* 0000021052	* 10	* 10		* 10	44002	destination	IPTF ADR Primary
□	* 0000031053	* 10	* 10		* 10	44006	destination	IPTF ADR Second
□	* 0000091049	* 10	* 10		* 10	40002	destination	IPTF CPN Passed

5.4. SIP Entities

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

- Session Manager (**Section 5.4.1**).
- Communication Manager, Local and Public access. Two entities are defined to allow two different SIP trunks (public and private) to be defined on Communication Manager. This permits different numbering plans to be administered on each so that the assigned AT&T IP Toll Free DID numbers are presented in the called number fields on the public trunk to AT&T, and local extensions are presented in the called number fields on the local trunk (e.g., coverage to Avaya Aura® Messaging. See **Section 6.7** for the associated Communication Manager trunk provisioning). In addition, SIP telephones will use the local trunk for intra site calls as well as status signaling to Session Manager. In order to differentiate between these two trunks, TCP port 5080 was defined for the public trunk and TCP port 5060 was defined for the local trunk. These ports are defined for Session Manager here and in **Section 5.5 Entity Links**.

- Communication Manager for AT&T access (**Section 5.4.2**) – This entity, and its associated Entity Link (using port 5080), is for calls from AT&T to Communication Manager via the Avaya SBCE. Note that port 5080 is only used between Communication Manager and Session Manager.
- Communication Manager for local access (**Section 5.4.3**) – This entity, and its associated Entity Link (using port 5060), is for communication between Avaya SIP telephones and Communication Manager.
- Avaya SBCE (**Section 5.4.4**) - This entity, and its associated Entity Link (using port 5060), is for inbound calls from the AT&T IP Toll Free service via the Avaya SBCE.
- Avaya Aura® Messaging (**Section 5.4.5**) – This entity, and its associated Entity Link (using port 5060), is for local calls from Avaya Aura® Messaging to Communication Manager**.**

Note – In the reference configuration, TCP is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis, however, Avaya best practices call for TLS (port 5061) to be used as the transport protocol when possible.

5.4.1. Avaya Aura® Session Manager SIP Entity

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

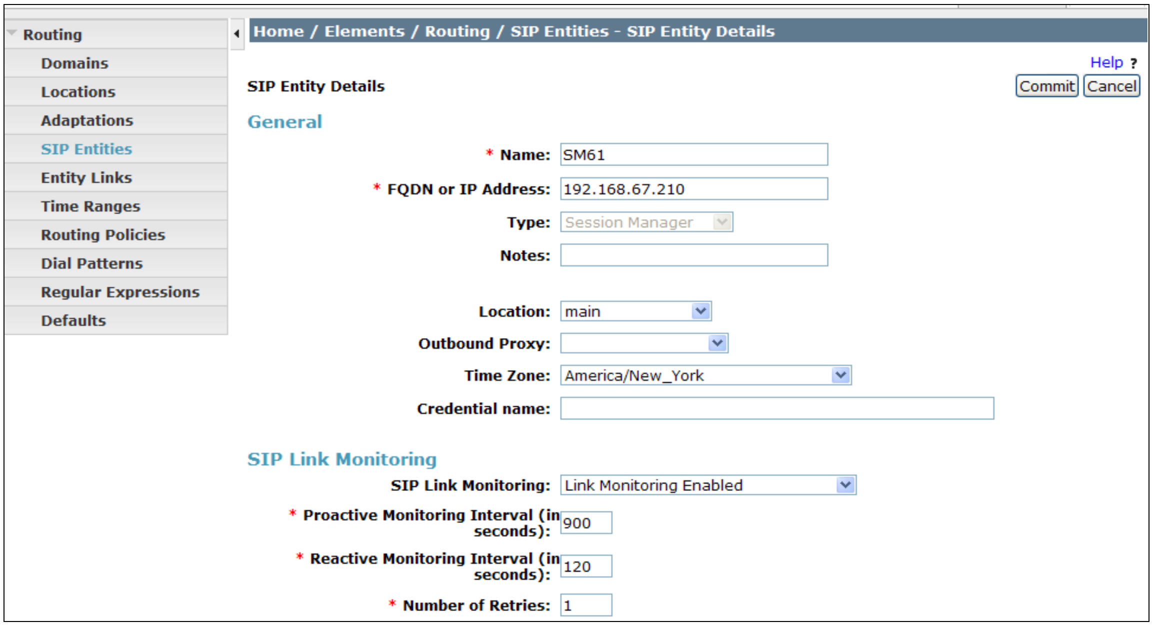
Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name for Session Manager (e.g., **SM61**).
- **FQDN or IP Address –** Enter the IP address of the Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **192.168.67.210**).
- **Type –** Verify **Session Manager** is selected.
- **Location** – Select location **main** (**Section 5.2.4)**.
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides.

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

- Select **Link Monitoring Enabled** for **SIP Link Monitoring** field.
- Use the default values for the remaining parameters.

These entries enable Session Manager to accept SIP requests on the specified ports/protocols. In addition, Session Manager will accept SIP requests containing the IP address of Session Manager (192.168.67.210) in the host part of the Request-URI.



Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

General

* Name: SM61

* FQDN or IP Address: 192.168.67.210

Type: Session Manager

Notes:

Location: main

Outbound Proxy:

Time Zone: America/New_York

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

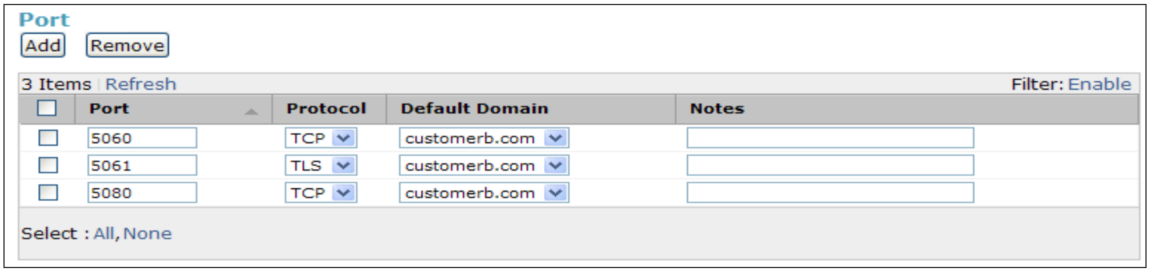
Step 4 - In the **Port** section of the **SIP Entity Details** page, click on **Add** and provision an entry as follows:

- **Port** – Enter **5080** (see note above).
- **Protocol** – Select **TCP** (see note above).
- **Default Domain** – (Optional) Select a SIP domain administered in **Section 5.1** for the selected **Default Domain** field (e.g., **customerb.com**)

Step 5 - Repeat **Step 4** to provision another entry, with **5060** for **Port** and **TCP** for **Protocol**. This is for local calls from the Avaya SIP telephones (and Avaya Aura® Messaging), to Communication Manager.

Step 6 – Repeat **Step 4** to provision another entry, with **5061** for **Port** and **TLS** for **Protocol.** Although TLS was not used in the reference configuration (see the note at the beginning of this section), the addition of TLS is shown for completeness.

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



Port

3 Items

□	Port	Protocol	Default Domain	Notes
□	5060	TCP	customerb.com	
□	5061	TLS	customerb.com	
□	5080	TCP	customerb.com	

Select : All, None

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

5.4.2. Avaya Aura® Communication Manager SIP Entity - Public

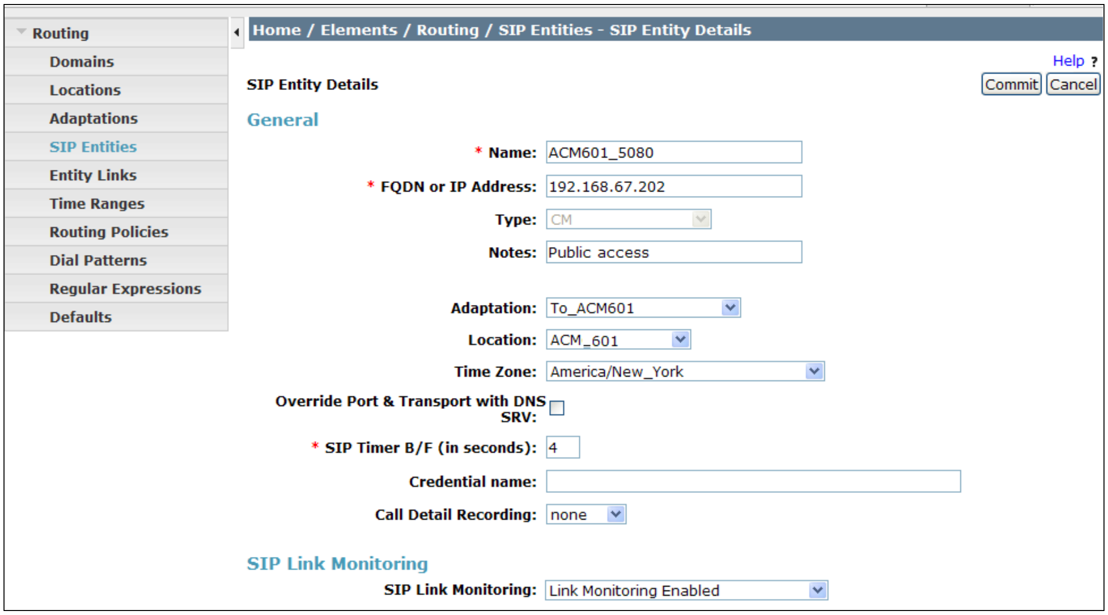
Step 1 - In the **SIP Entities** page, click on **New** (not shown).

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

- **Name** – Enter a descriptive name for the Communication Manager public trunk (e.g. **ACM601_5080**).
- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.3** (e.g. **192.168.67.202**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation administered in **Section 5.3.1**.
- **Location** – Select a Location administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page select:
  - Select **Link Monitoring Enabled** for **SIP Link Monitoring** field.
  - Use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

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



SIP Entity Details

General

* Name:	ACM601_5080
* FQDN or IP Address:	192.168.67.202
Type:	CM
Notes:	Public access
Adaptation:	To_ACM601
Location:	ACM_601
Time Zone:	America/New_York
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Enabled

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

Configuration for this entity is similar to the entity configured in **Section 5.4.2**.

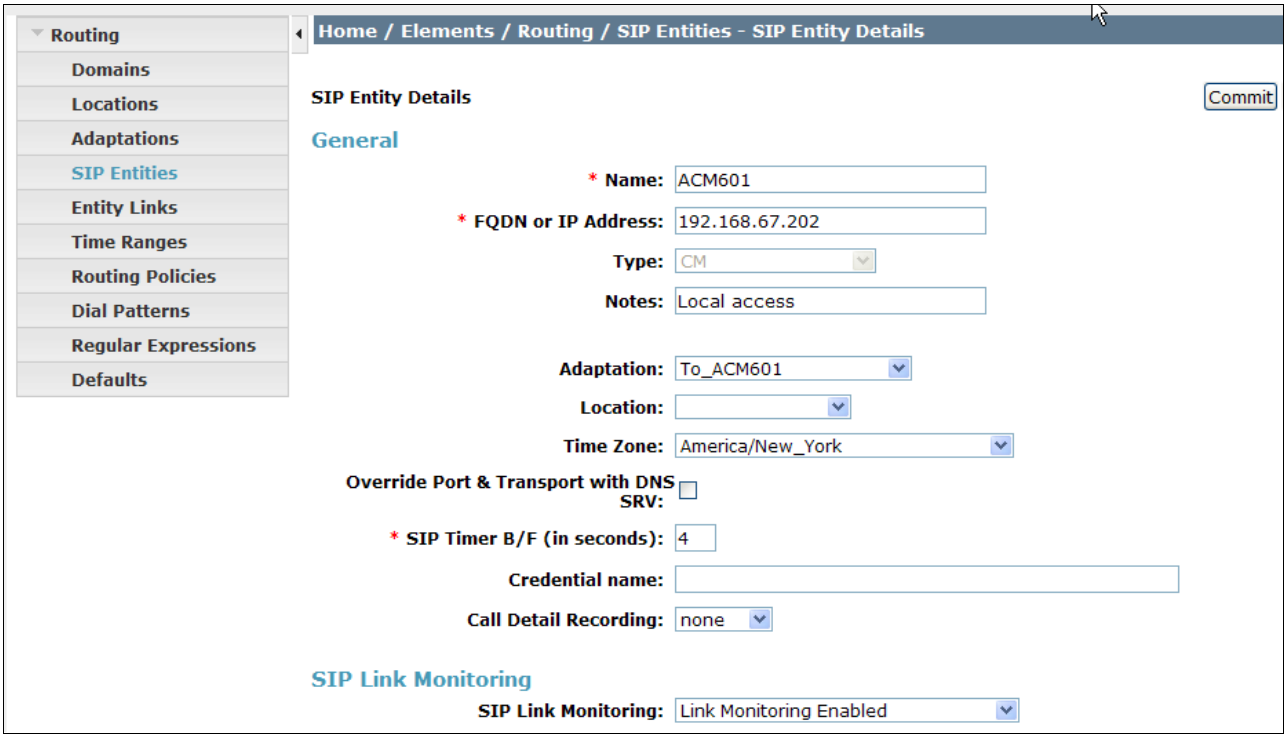
Step 1 - In the **SIP Entities** page, click on **New** (not shown).

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

- **Name** – Enter a descriptive name for the Communication Manager local trunk.
- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) provisioned in **Section 6.3** (e.g. **192.168.67.202**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation administered in **Section 5.3.1**.
- **Location** – Select a Location administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** pageprovision the following:
  - Select **Link Monitoring Enabled** for **SIP Link Monitoring** field.
  - Use the default values for the remaining parameters.

Step 3 - Click on **Commit**.

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



SIP Entity Details

General

* Name:	ACM601
* FQDN or IP Address:	192.168.67.202
Type:	CM
Notes:	Local access
Adaptation:	To_ACM601
Location:	
Time Zone:	America/New_York
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Link Monitoring Enabled

5.4.4. Avaya Session Border Controller for Enterprise SIP Entity

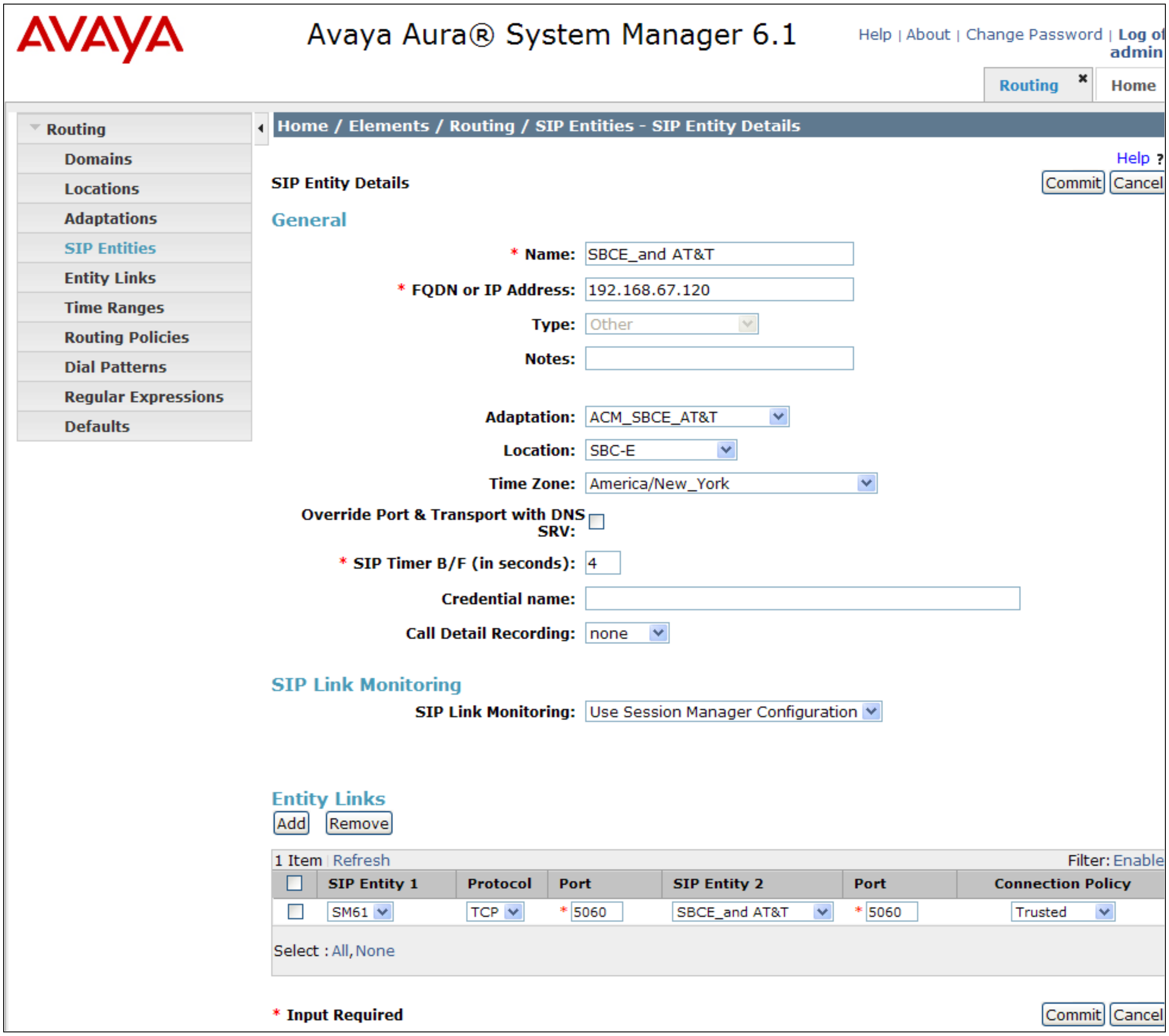
To configure the Avaya SBCE entity, repeat the steps in **Section 5.4.2** with the following changes:

- The F**QDN or IP Address** field is populated with the IP address of the private (inside) Avaya SBCE interface configured in **Section 8** (e.g., **192.168.67.120**).
- The **Type** field is set to **Other**.
- **Adaptation** – Select the Adaptation administered in **Section 5.3.1**.

- **Location** – Select the Location administered in **Section 5.2.2**.

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

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



SIP Entity Details

General

* Name:	SBCE_and AT&T
* FQDN or IP Address:	192.168.67.120
Type:	Other
Notes:	
Adaptation:	ACM_SBCE_AT&T
Location:	SBC-E
Time Zone:	America/New_York
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

Entity Links

1 Item | Refresh Filter: Enable

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	SM61	TCP	* 5060	SBCE_and AT&T	* 5060	Trusted

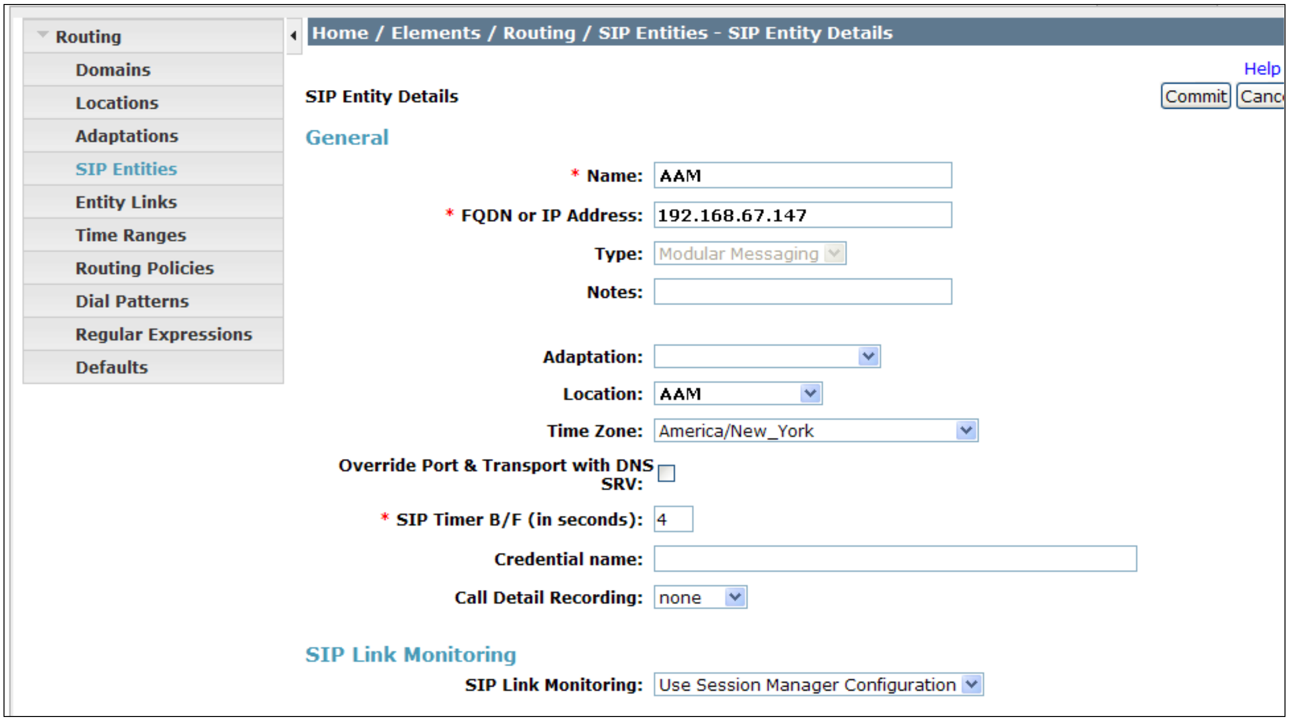
Select : All, None

* Input Required

5.4.5. Avaya Aura® Messaging SIP Entity

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

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



SIP Entity Details

General

* Name:	AAM
* FQDN or IP Address:	192.168.67.147
Type:	Modular Messaging
Notes:	
Adaptation:	
Location:	AAM
Time Zone:	America/New_York
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

5.5. Entity Links

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

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

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

Note – In the reference configuration, TCP (using ports 5060 and 5080) is used as the transport protocol between Session Manager and all the SIP Entities, including Communication Manager. This was done to facilitate protocol trace analysis, however, Avaya best practices call for TLS (port 5061) to be used as transport protocol when possible.

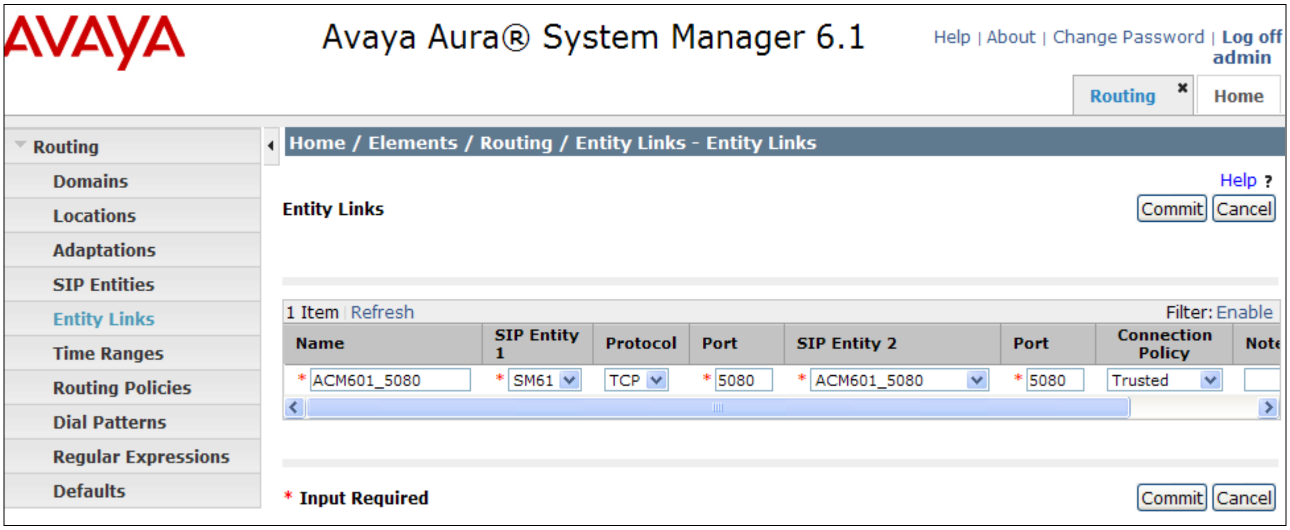
5.5.1. Entity Link to Avaya Aura® Communication Manager - Public

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

Step 2 - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **ACM601_5080**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager. SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter **5080**.
- **SIP Entity 2** –Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public entity.
- **SIP Entity 2 Port** - Enter **5080**.
- **Trusted** – Select **Trusted**.
- **Protocol** – Select **TCP**.

Step 3 - Click on **Commit**.



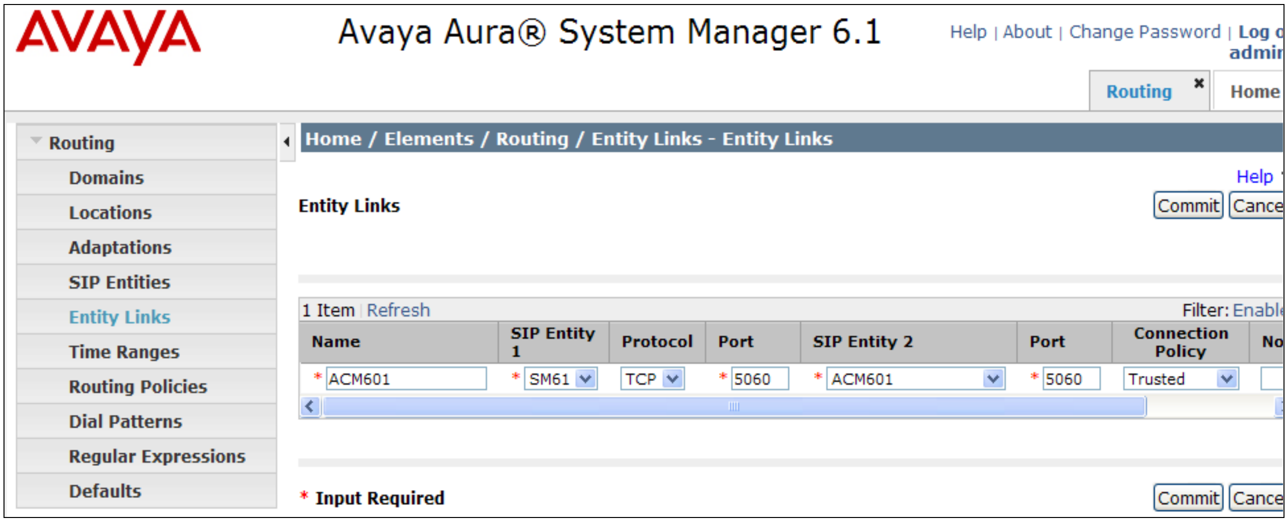
Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Note
* ACM601_5080	* SM61	TCP	* 5080	* ACM601_5080	* 5080	Trusted	

* Input Required

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

To configure this entity link, repeat the steps in **Section 5.5.1**. The **SIP Entity 2** field is populated with the SIP Entity configured in **Section 5.4.3** for the Communication Manager local Entity (e.g., **ACM601**). Note that the **Port** fields are populated with **5060**. See the figure below for the values used in the reference configuration.



Entity Links

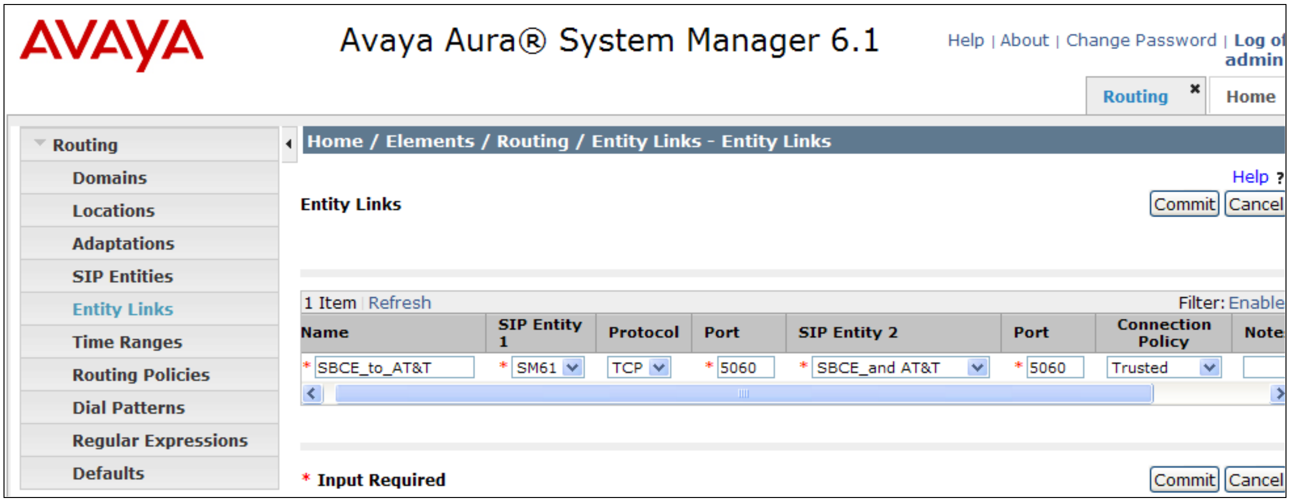
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	No
* ACM601	* SM61	TCP	* 5060	* ACM601	* 5060	Trusted	

* Input Required

5.5.3. Entity Link for the AT&T IP Toll Free Service via the Avaya SBCE

Repeat the steps in **Section 5.5.1** with the following differences:

- **Name** – Enter a descriptive name for the link for the AT&T IP Toll Free service, by way of the Avaya SBCE.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.4** for the Avaya SBCE.



Entity Links

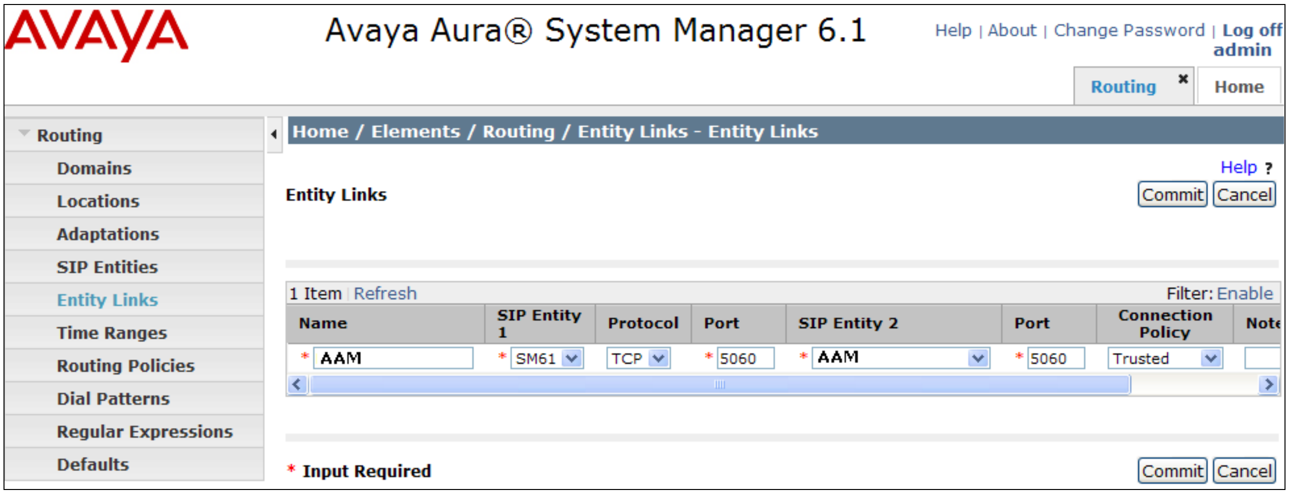
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Note
* SBCE_to_AT&T	* SM61	TCP	* 5060	* SBCE_and AT&T	* 5060	Trusted	

* Input Required

5.5.4. Entity Link to Avaya Aura® Messaging

Repeat the steps in **5.5.1** with the following differences:

- **Name** – Enter a descriptive name for the link to Avaya Aura® Messaging (e.g., **AAM**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.5** for Avaya Aura® Messaging.



Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Note
* AAM	* SM61	TCP	* 5060	* AAM	* 5060	Trusted	

* Input Required

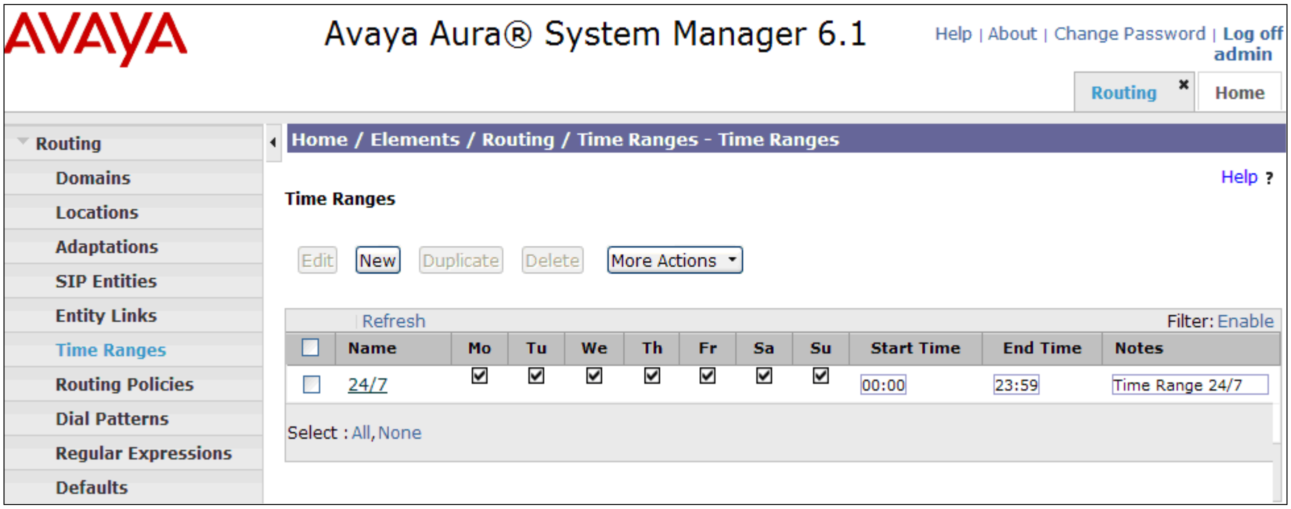
5.6. Time Ranges

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

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

Step 3 - Click on **Commit**.

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



Home / Elements / Routing / Time Ranges - Time Ranges

Time Ranges

□	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
□	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

5.7. Routing Policies

In this section, the following Routing Policies are administered:

- AT&T calls to Avaya Aura® Communication Manager (**Section 5.7.1**).
- Avaya Aura® Messaging MWI notification to Avaya Aura® Communication Manager (**Section 5.7.2**).
- Avaya Aura® Communication Manager calls to Avaya Aura® Messaging for call coverage (**Section 5.7.3**)

Note: Since the AT&T IP Toll Free service is inbound only, no outbound routing is provisioned.

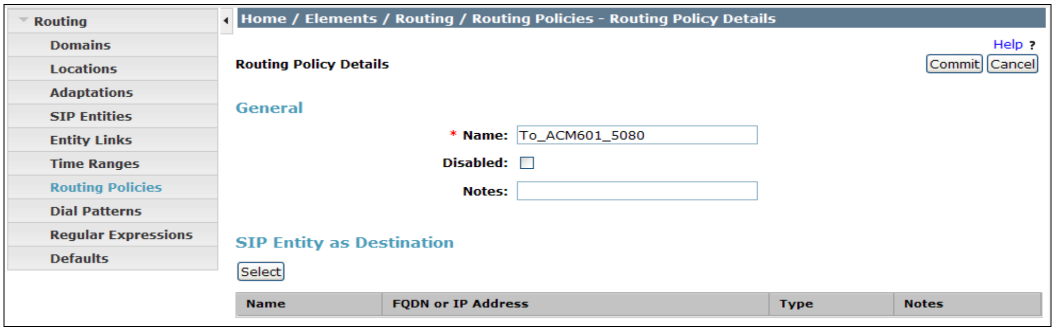
5.7.1. Routing Policy for Routing to Avaya Aura® Communication Manager from AT&T

Note that this routing policy will use the public Communication Manager SIP Entity **ACM601_5080**.

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

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing AT&T calls to Communication Manager (e.g., **To_ACM601_5080**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

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



Routing Policy Details

General

* Name: To_ACM601_5080

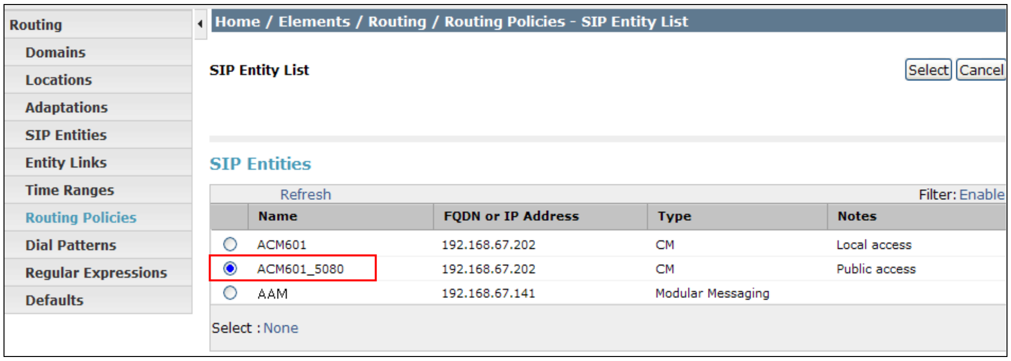
Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes

Step 4 - In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for the Communication Manager public SIP Entity (**ACM601_5080**), and click on **Select**.



SIP Entity List

SIP Entities

	Name	FQDN or IP Address	Type	Notes
○	ACM601	192.168.67.202	CM	Local access
●	ACM601_5080	192.168.67.202	CM	Public access
○	AAM	192.168.67.141	Modular Messaging	

Select : None

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

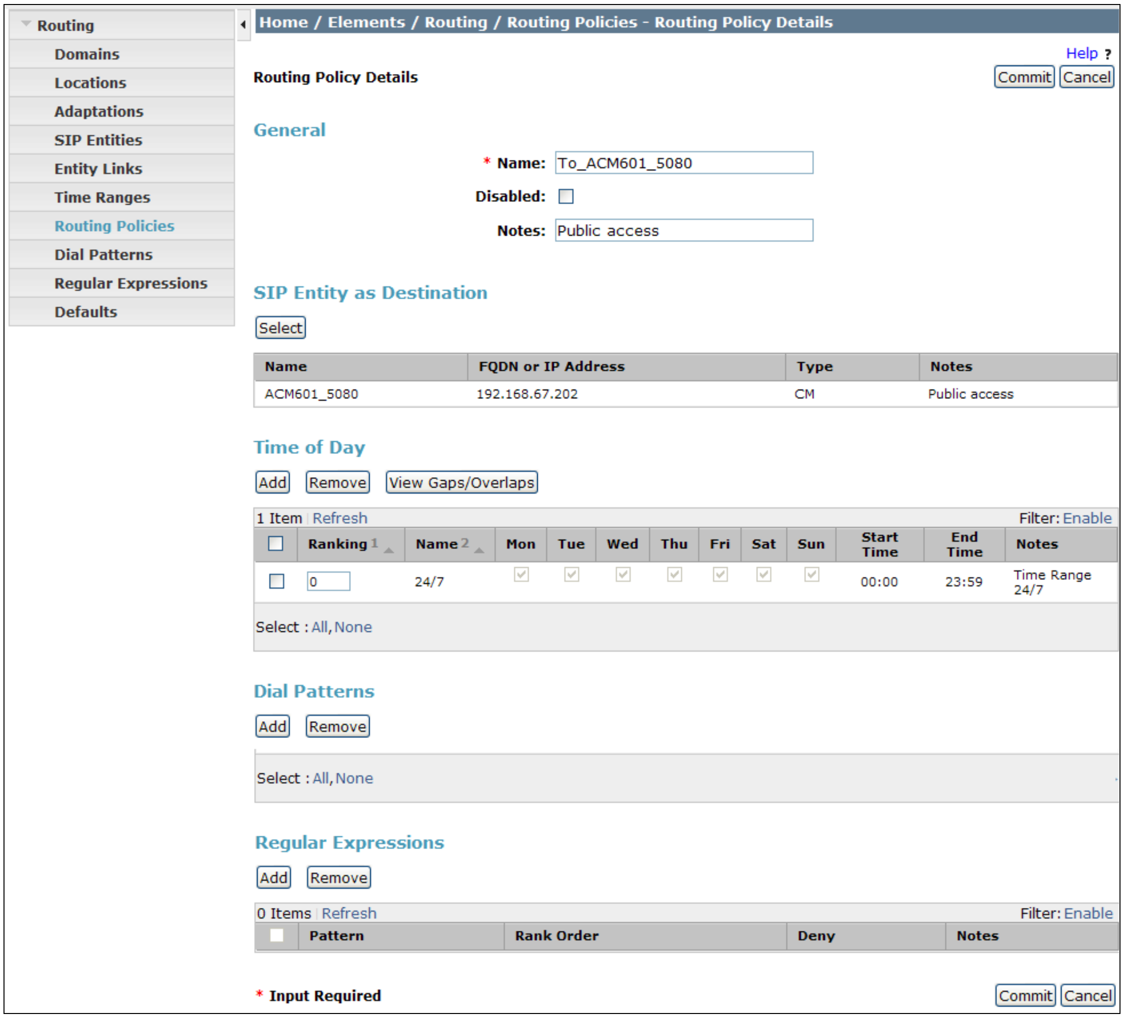
Step 6 - In the **Time Range List** page (not shown), check the checkbox(es) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on **Select**.

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

Step 8 - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.

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

Step 10 - Click on **Commit**.



Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

General

* Name: To_ACM601_5080

Disabled: □

Notes: Public access

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ACM601_5080	192.168.67.202	CM	Public access

Time of Day

1 Item | Refresh Filter: Enable

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Select : All, None

Regular Expressions

0 Items | Refresh Filter: Enable

□	Pattern	Rank Order	Deny	Notes

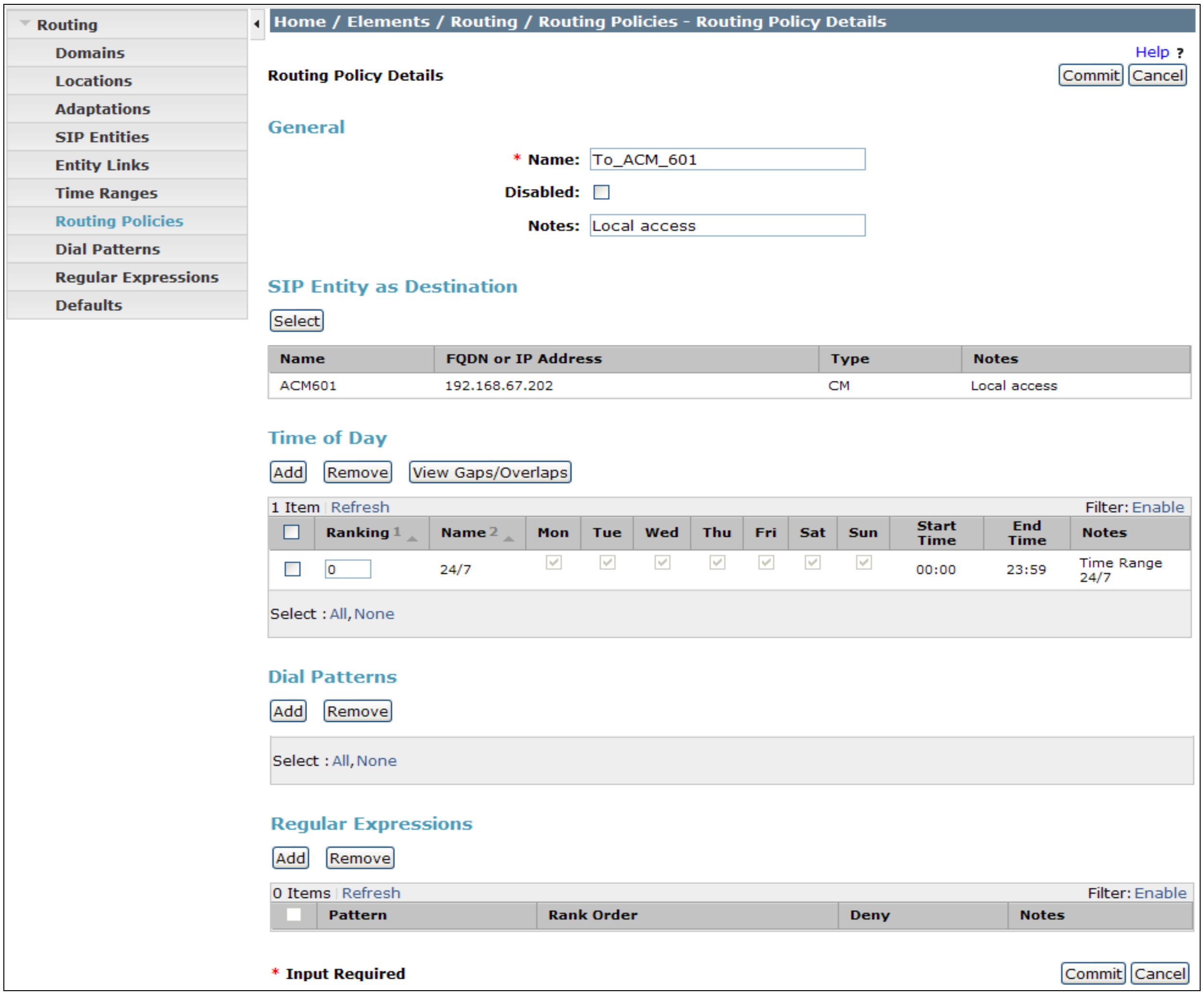
* Input Required

5.7.2. Routing Policy for Local Routing to Avaya Aura® Communication Manager

Note that this routing policy will use the local Communication Manager SIP Entity **ACM601**.

Repeat the steps in **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing local calls to Communication Manager (e.g. **To_ACM_601**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.3** for the Communication Manager local SIP Entity (e.g. **ACM601**), and click on **Select**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.



Routing Policy Details

General

* Name: To_ACM_601

Disabled: □

Notes: Local access

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACM601	192.168.67.202	CM	Local access

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

Select : All, None

Regular Expressions

Add Remove

0 Items | Refresh Filter: Enable

□	Pattern	Rank Order	Deny	Notes

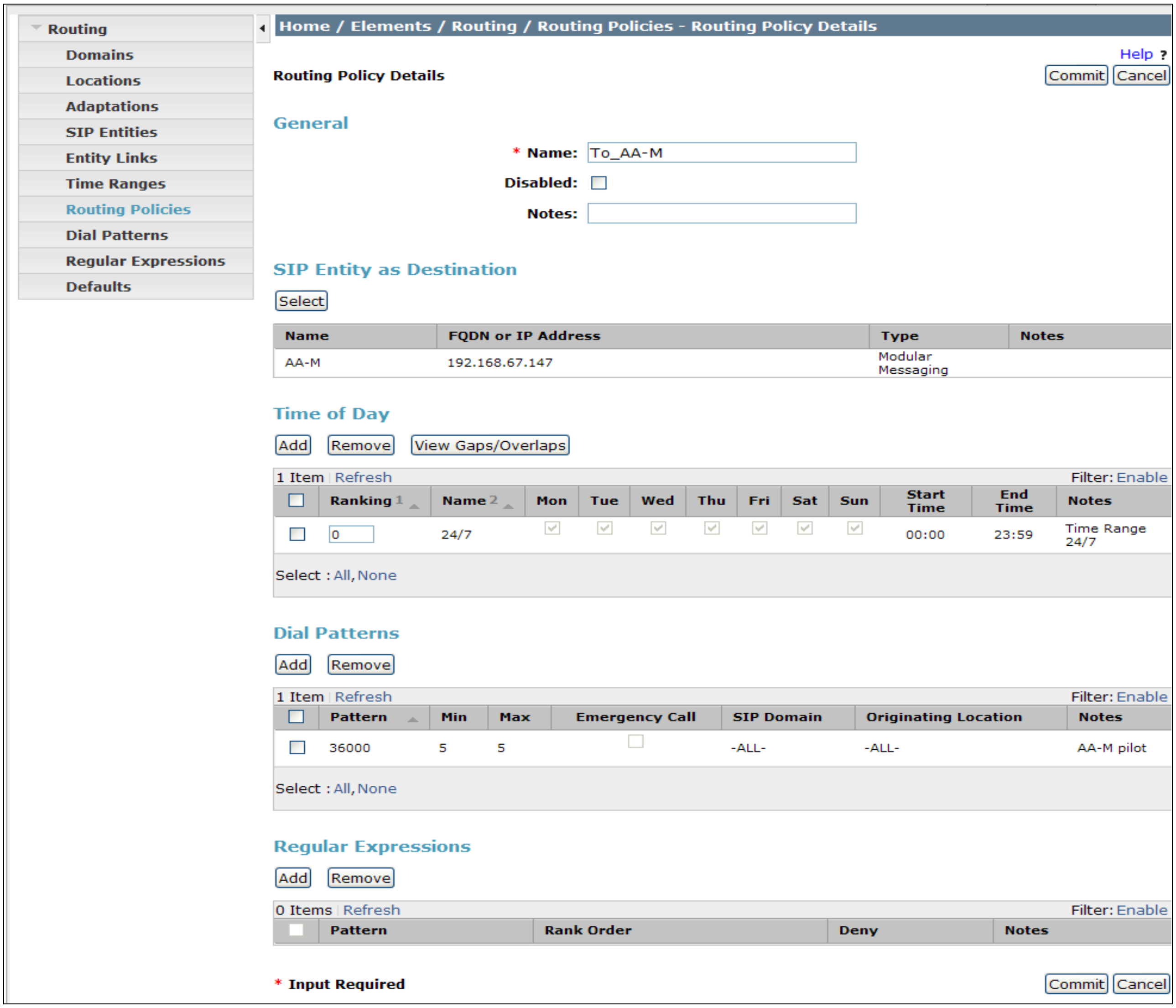
* Input Required

Commit Cancel

5.7.3. Routing Policy for Routing to Avaya Aura® Messaging (Call Coverage) from Avaya Aura® Communication Manager

Repeat **Section 5.7.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Avaya Aura® Messaging (e.g. **AAM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.5** for Avaya Aura® Messaging (e.g. **AAM**), and click on **Select**.
- Note that once the **Dial Patterns** are defined (**Section 5.8**), they will appear in the **Dial Pattern** section.



Routing Policy Details

General

* Name: To_AA-M

Disabled: □

Notes:

SIP Entity as Destination

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

Time of Day

1 Item | Refresh Filter: Enable

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

1 Item | Refresh Filter: Enable

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	36000	5	5	□	-ALL-	-ALL-	AA-M pilot

Select : All, None

Regular Expressions

0 Items | Refresh Filter: Enable

□	Pattern	Rank Order	Deny	Notes

* Input Required

5.8. Dial Patterns

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

- Inbound PSTN calls via AT&T IP Toll Free service to Communication Manager.
- Call Coverage/retrieval to Avaya Aura® Messaging from Communication Manager to the Avaya Aura® Messaging pilot number.
- Notifications from Avaya Aura® Messaging (MWI) to Communication Manager 5 digit local extensions.

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

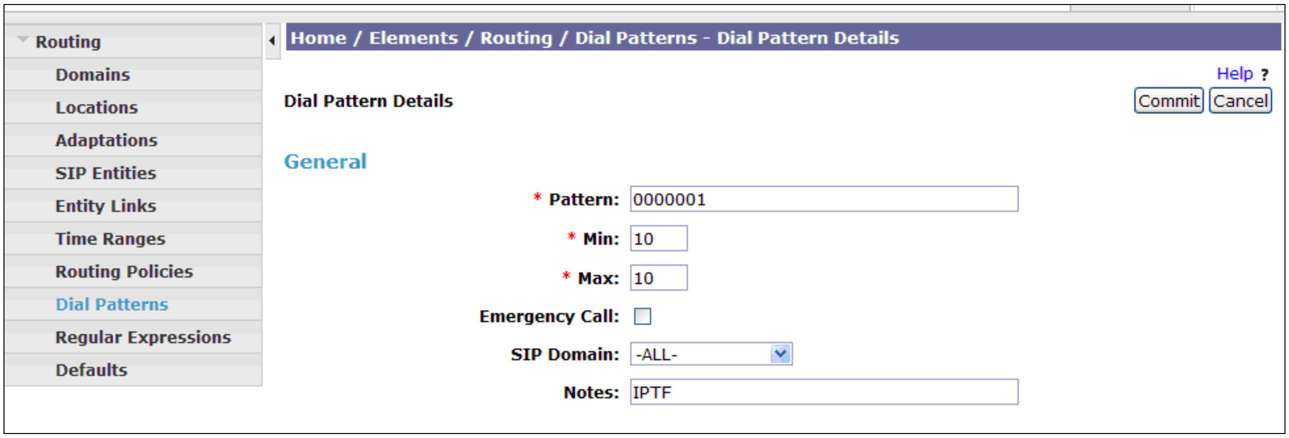
In the reference configuration inbound calls from the AT&T IP Toll Free service used the called digit pattern 0000001xxx in the SIP Request URI. This pattern is matched for further call processing.

Note – Be sure to match on the digit string specified in the Request URI, not the digit string that was dialed. They may be different.

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

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

- **Pattern** – In the reference configuration, AT&T sends a 10 digit number in the Request URI with the format 0000001xxx. Enter **0000001**. Note - The adaptation defined for Communication Manager in **Section 5.3.1** will convert the various 0000001xxx numbers into their corresponding extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select one of the SIP Domains defined in **Section 5.1** or **-ALL-**, to select all of the administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if **-ALL-** is selected) can match this Dial Pattern.



Dial Pattern Details

General

* Pattern: 0000001

* Min: 10

* Max: 10

Emergency Call: □

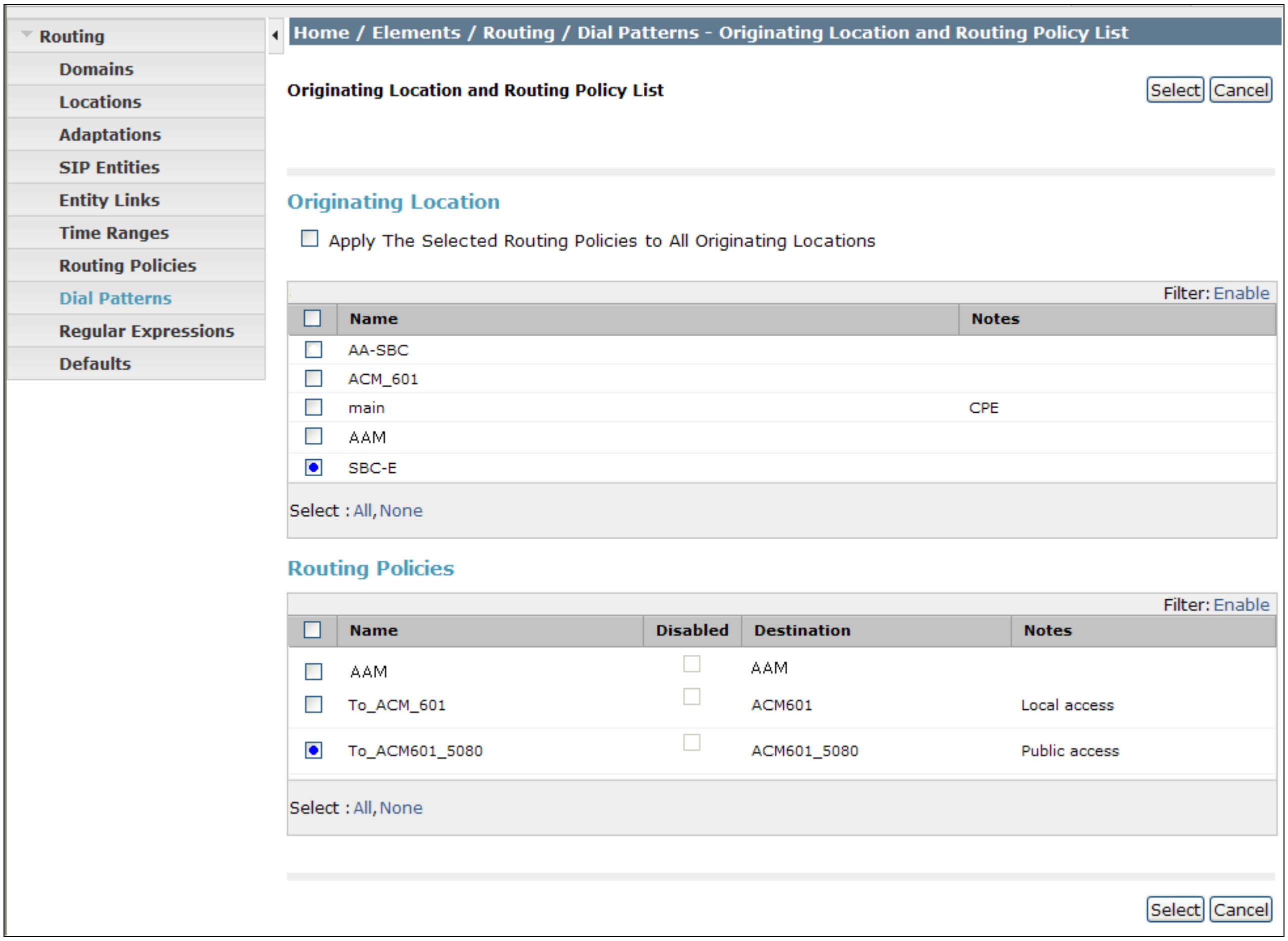
SIP Domain: -ALL-

Notes: IPTF

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

Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **SBC-E** see **Section 5.2.2**). Note that only those calls that originate from the selected Location(s), or all administered Locations if **-ALL-** is selected, can match this Dial Pattern.

Step 5 - In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager public trunk in **Section 5.7.1**.



Originating Location and Routing Policy List

Originating Location

□ Apply The Selected Routing Policies to All Originating Locations

Filter: Enable

□	Name	Notes
□	AA-SBC	
□	ACM_601	
□	main	CPE
□	AAM	
☑	SBC-E	

Select : All, None

Routing Policies

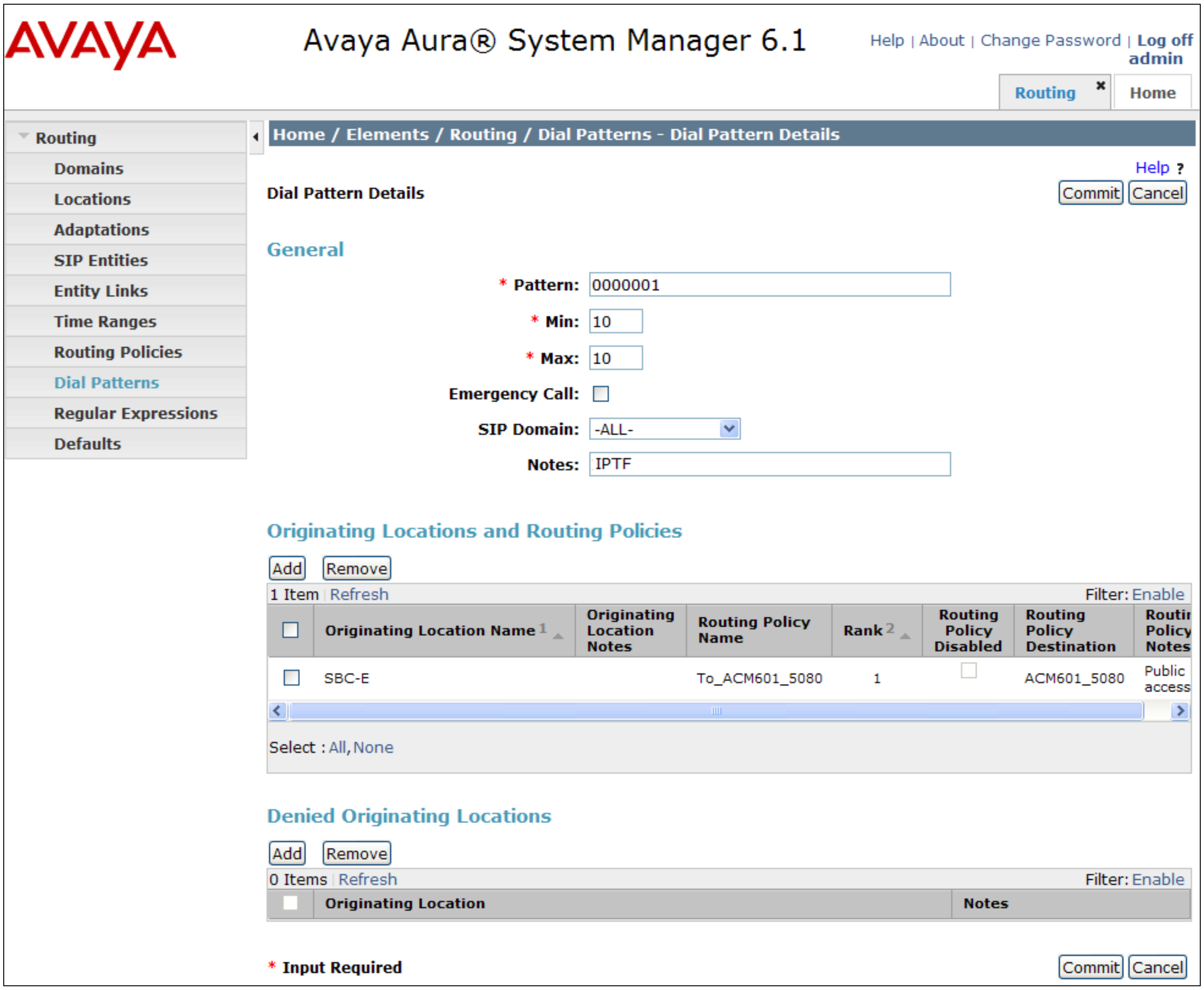
Filter: Enable

□	Name	Disabled	Destination	Notes
□	AAM	□	AAM	
□	To_ACM_601	□	ACM601	Local access
☑	To_ACM601_5080	□	ACM601_5080	Public access

Select : All, None

Step 6 - In the **Originating Location and Routing Policy List** page, click on **Select**.

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



Avaya Aura® System Manager 6.1

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 0000001

* Min: 10

* Max: 10

Emergency Call: □

SIP Domain: -ALL-

Notes: IPTF

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routir Policy Notes
□	SBC-E		To_ACM601_5080	1	□	ACM601_5080	Public access

Select : All, None

Denied Originating Locations

□	Originating Location	Notes

* Input Required

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

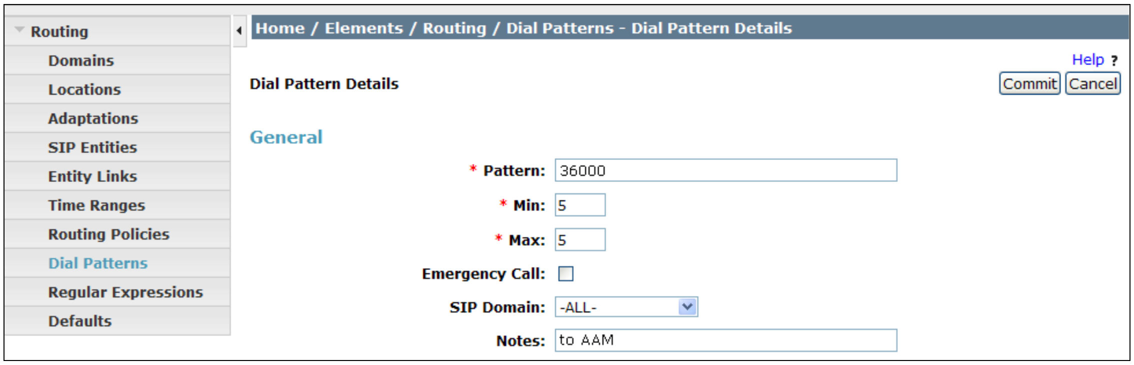
Communication Manager stations cover to Avaya Aura® Messaging using a pilot extension (36000 in the reference configuration). Additionally stations may dial this pilot extension to retrieve messages or modify mailbox settings.

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

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

- **Pattern** – Enter the Avaya Aura® Messaging pilot extension (e.g., **36000**)
- **Min** and **Max** – Enter **5**.
- **SIP Domain** – Select one of the SIP Domains defined in **Section 5.1** or **-ALL-**, to select all of the administered SIP Domains. Only those calls with the same domain

in the Request-URI as the selected SIP Domain (or all administered SIP Domains if **-ALL-** is selected) can match this Dial Pattern.



Dial Pattern Details

General

* Pattern: 36000

* Min: 5

* Max: 5

Emergency Call: □

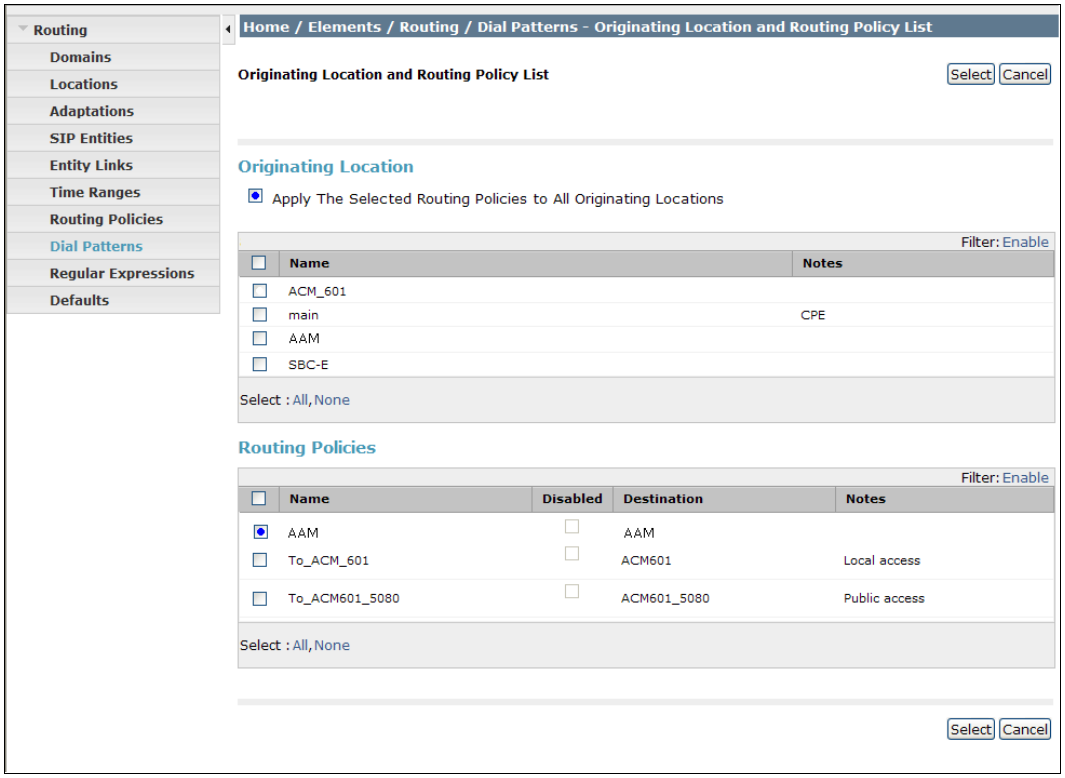
SIP Domain: -ALL-

Notes: to AAM

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

Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to "**Apply The Selected Routing Policies to All Originating Locations**".

Step 5 - In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **AAM** administered for routing calls to Avaya Aura® Messaging in **Section 5.7.3**.



Originating Location and Routing Policy List

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations

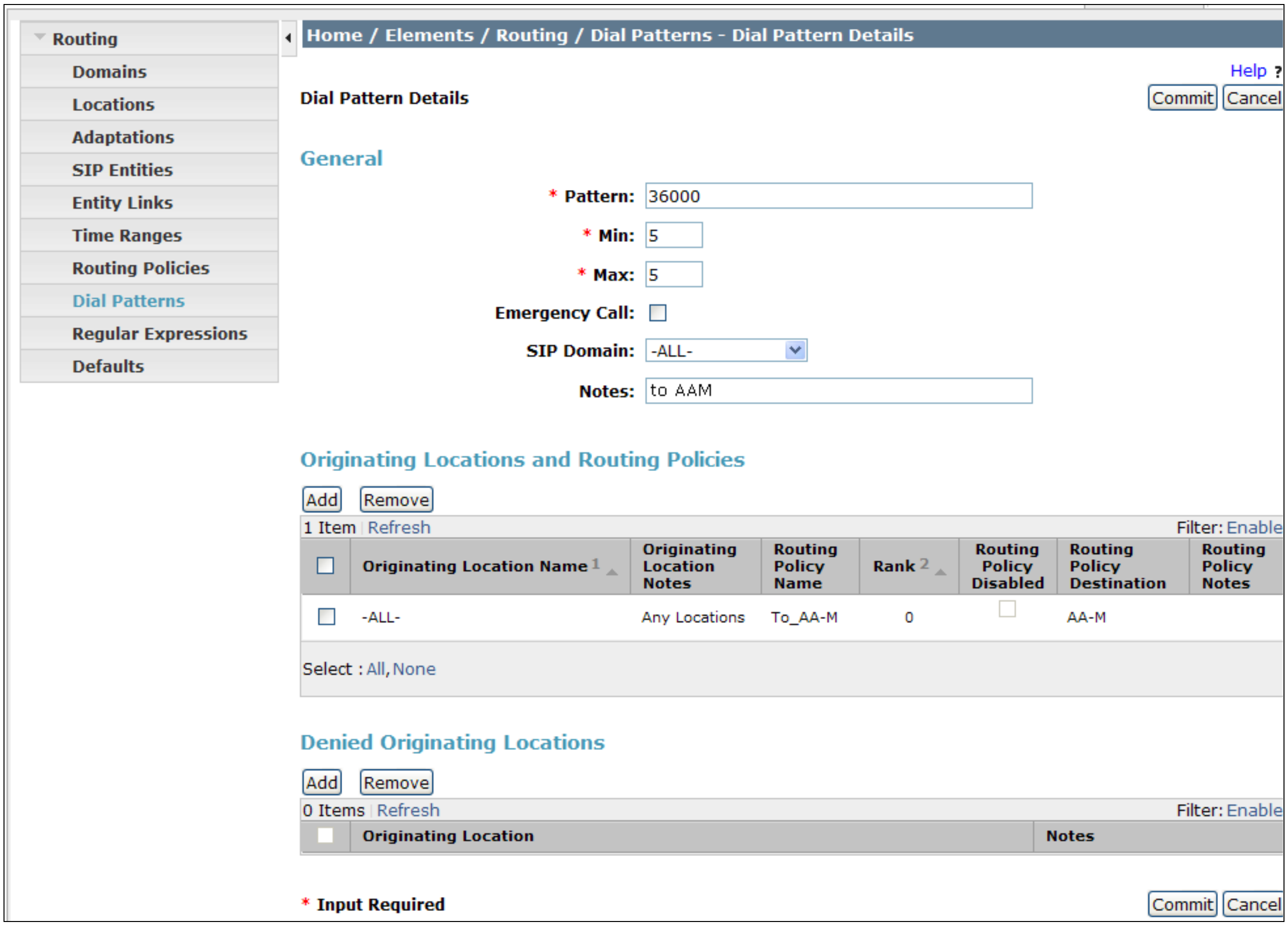
□	Name	Notes
□	ACM_601	
□	main	CPE
□	AAM	
□	SBC-E	

Routing Policies

□	Name	Disabled	Destination	Notes
☒	AAM	□	AAM	
□	To_ACM_601	□	ACM601	Local access
□	To_ACM601_5080	□	ACM601_5080	Public access

Step 6 - In the **Originating Location and Routing Policy List** page, click on **Select**.

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



Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 36000

* Min: 5

* Max: 5

Emergency Call: □

SIP Domain: -ALL-

Notes: to AAM

Originating Locations and Routing Policies

1 Item | Refresh

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	To_AA-M	0	□	AA-M	

Select : All, None

Denied Originating Locations

0 Items | Refresh

□	Originating Location	Notes

* Input Required

6. Avaya Aura® Communication Manager

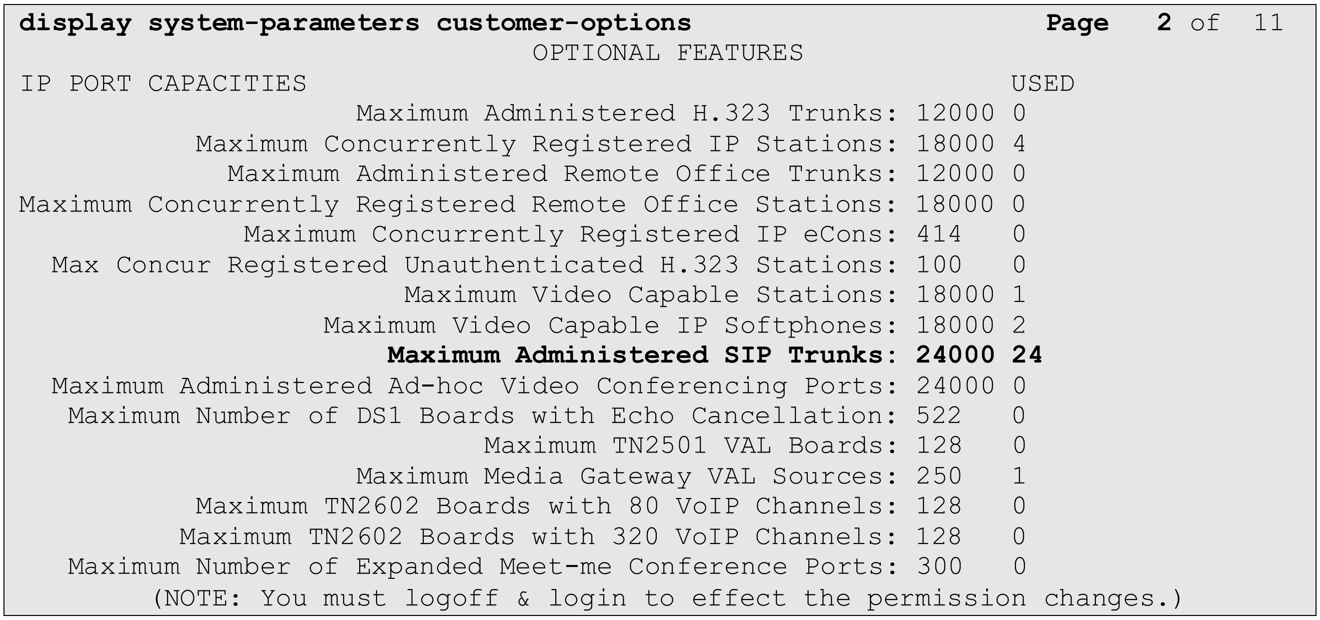
This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult [5], [6] and [7] for further details if necessary.

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

6.1. System Parameters

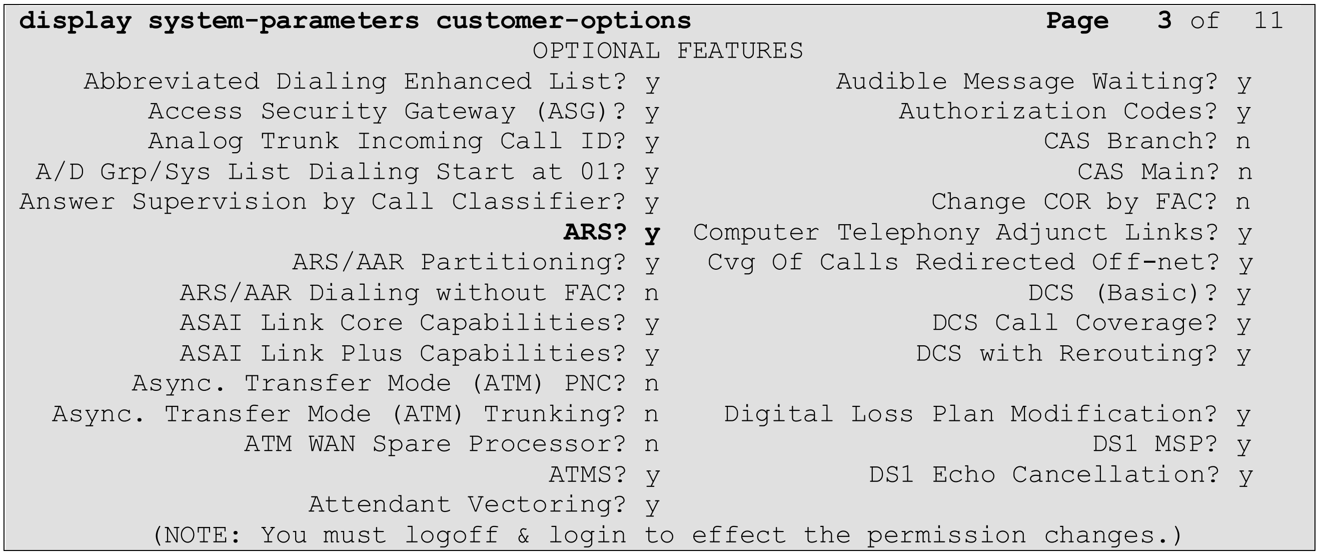
This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes. For required licenses that are not enabled in the steps that follow, contact an authorized Avaya account representative to obtain the licenses.

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.)
```

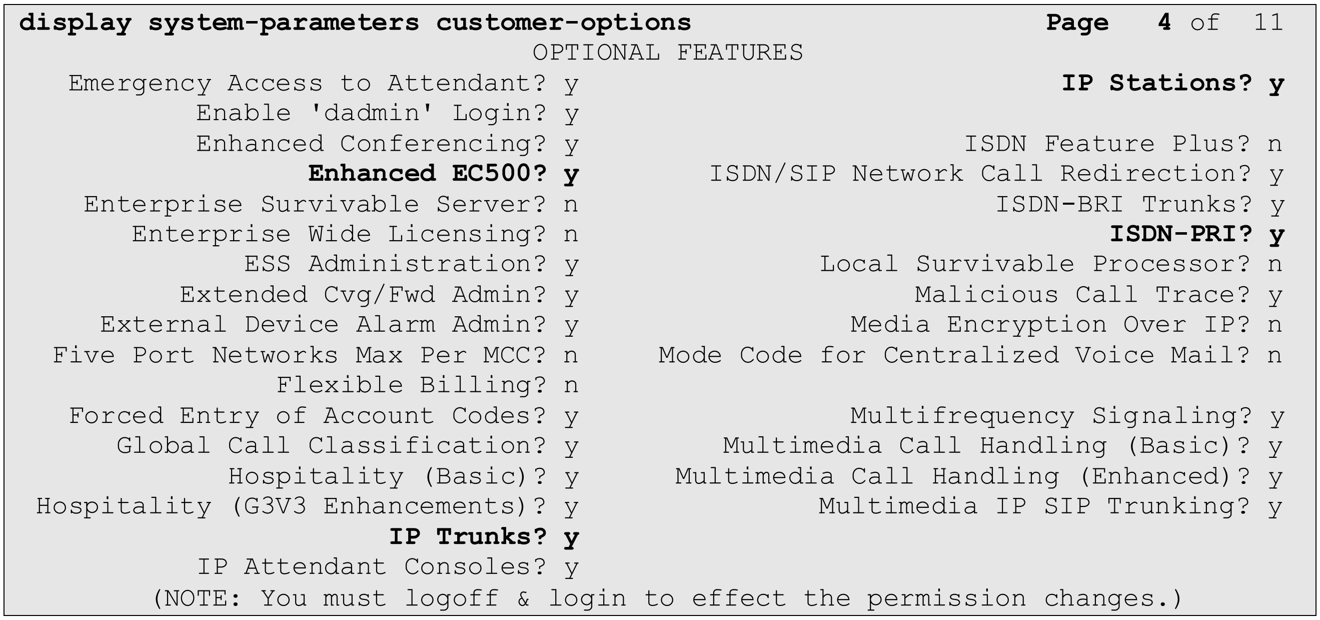
Step 2 - On **Page 3** of the **System-Parameters Customer-options** form, verify that the **ARS** feature is enabled.



```
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
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                 ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

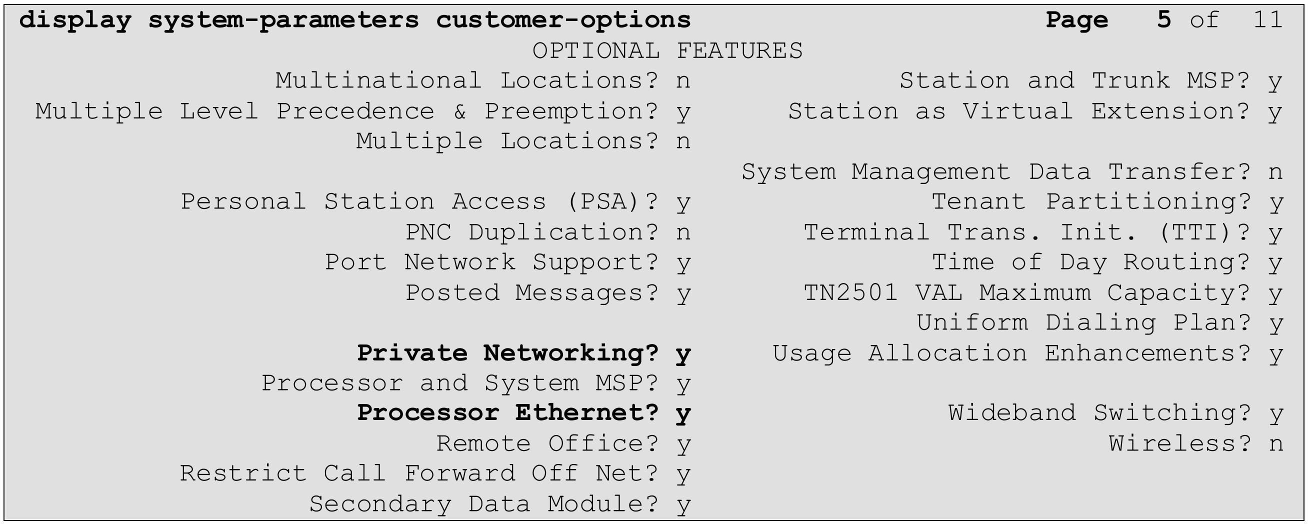
Step 3 - On **Page 4** of the **system-parameters customer-options** form:

a. Verify that the **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
```

6.2. Dial Plan

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

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

- 3-digit dial access codes (indicated with a **Call Type** of **dac**) beginning with the digit **1.** Trunk Access Codes (TACs) defined for trunk groups in this reference configuration conform to this format.
- 5-digit extensions with a **Call Type** of **ext** beginning with the digit **4**, (Local extensions for Communication Manager stations, agents, and Vector Directory Numbers (VDNs) in this reference configuration conform to this format). Also **3xxxx** to cover the Aura® Messaging pilot number (36000).
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g., access code **8** for outbound AAR dialing).
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g., access code **9** for outbound ARS dialing).
    - Note – ARS is typically used for outbound dialing, which the AT&T IP Toll Free service does not support. It is shown here for informational purposes.
- 3-digit facilities access codes beginning with * and # for Agent logon/logoff (e.g.,*66 or #76).

```
change dialplan analysis                                       Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 1
    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   1           3   dac
   3           5   ext
   4           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   fac
```

6.3. IP Node Names

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

Step 1 - Enter the **change node-names ip** command, and add a node name and IP address for the Session Manager signaling interface (e.g., **ASM61**)

Step 2 – Repeat **Step 1** to add node names for the Avaya SBCE (e.g., **SBCE**) and for Aura® Messaging (e.g., **AAM**).

Step 3 - A Processor Ethernet (procr) based Communication Manager platform is used in the reference configuration. Make note of the Processor Ethernet node name and IP Address (**procr** & **192.168.67.202**). These entries appear automatically based on the address defined during Communication Manager installation.

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name                IP Address
ASM61                 192.168.67.210
SBCE                  192.168.67.120
AAM                   192.168.67.147
```

```
default                 0.0.0.0
procr                   192.168.67.202
procr6                  ::
```

6.4. IP Interface for procr

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

- Verify that **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** fields are set to **y**.
- Assign a **Network Region** (e.g., **1**).
- Use default values for the remaining parameters.

```
display ip-interface procr                                      Page   1 of   2
                                   IP INTERFACES
                  Type: PROCR
                                                     Target socket load: 19660

      Enable Interface? y                             Allow H.323 Endpoints? y
                                                       Allow H.248 Gateways? y
        Network Region: 1                                Gatekeeper Priority: 5

                                  IPV4 PARAMETERS
             Node Name: procr                       IP Address: 192.168.67.202
           Subnet Mask: /24
```

6.5. IP Network Regions

Network Regions are used to group various Communication Manager resources such as codecs, UDP port ranges, and inter-region communication. In the reference configuration, two network regions are used, one for local calls and one for AT&T calls.

6.5.1. IP Network Region 1 – Local Region

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

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

- Enter a descriptive name (e.g., **LOCAL**).
- Enter **customerb.com** in the **Authoritative Domain** field.
- Enter **1** for the **Codec Set** parameter.
- **Intra 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 IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min**: - Set to **16384** (**AT&T requirement**).

- **UDP Port Max**: - Set to **32767** (**AT&T requirement**).

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

Step 2 - On **page 4** of the form:

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

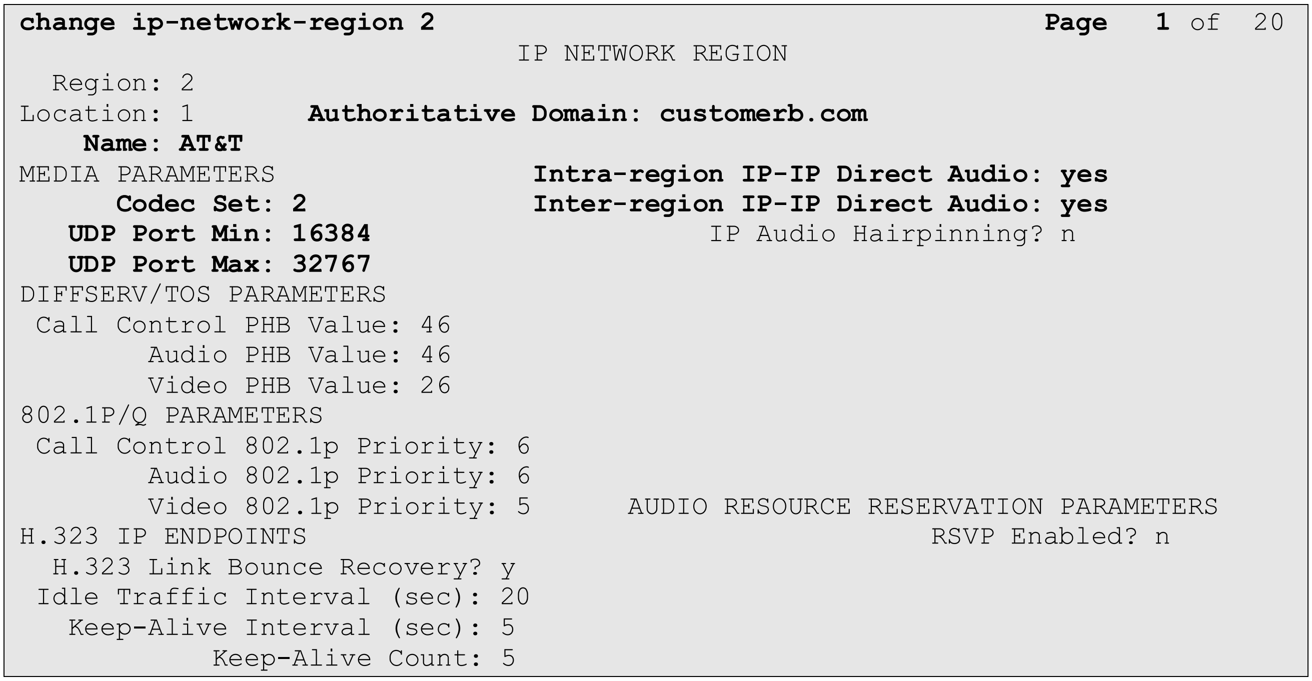
```
change ip-network-region 1                                      Page   4 of  20

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

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

In the reference configuration, AT&T SIP trunk calls are assigned to **ip-network-region 2**.

Step 1 - Repeat the steps in **Section 6.5.1** with the following changes:

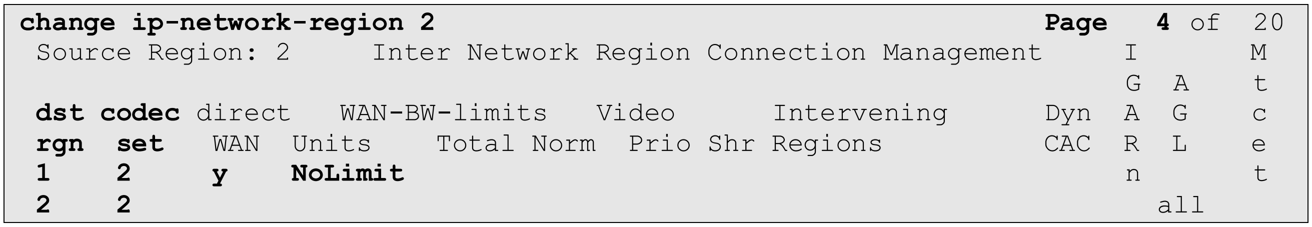
- **Page 1**
  - Enter a descriptive name (e.g., **AT&T**)
  - Enter **2** for the **Codec Set** parameter.



```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1         Authoritative Domain: 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 1** and **2**



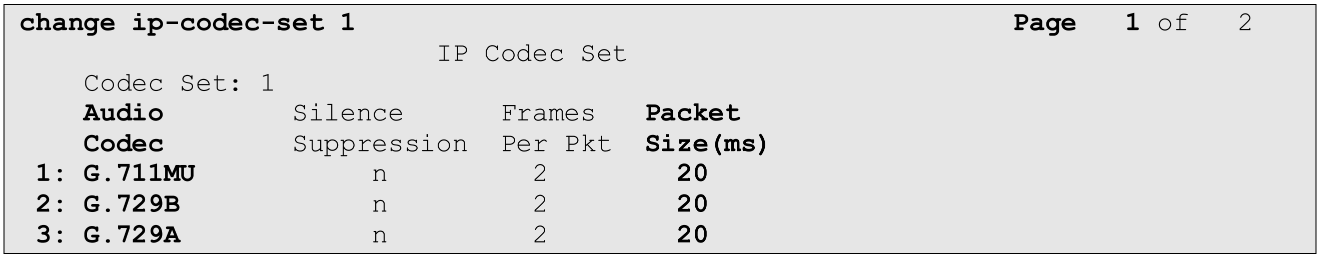
```
change ip-network-region 2                                      Page   4 of  20
 Source Region: 2     Inter Network Region Connection Management     I       M
                                                                     G  A    t
 dst codec direct   WAN-BW-limits   Video      Intervening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

6.6. IP Codec Parameters

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

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

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls. On **Page 1** of the **ip-codec-set** form, ensure that **G.711MU**, **G.729B**, and **G.729A** are included in the codec list. Note that the packet interval size will default to 20ms.



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

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

```
change ip-codec-set 1                                             Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? y
              Maximum Call Rate for Direct-IP Multimedia:   384:Kbits
     Maximum Call Rate for Priority Direct-IP Multimedia:   384:Kbits
                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         US                   3
    Clear-channel   n                    0
```

6.6.2. Codecs for IP Network Region 2

In the reference configuration IP Network Region **2** uses codec set **2** for calls from AT&T.

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g., **2**). This IP codec set will be used for inbound AT&T IP Toll Free calls. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown. For G729B and G729A set **3** for the **Frames Per Pkt**. This will automatically populate **30** for the Packet Size (ms). Let G711MU default to **20**.

Note – See **Section 2.2.1**, **Item 4** for an issue regarding SIP telephone packet sizes.

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

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

```
change ip-codec-set 2                                           Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? n
                    Mode                Redundancy
    FAX             t.38-standard        0
    Modem           off                  0
    TDD/TTY         off                  0
    Clear-channel   n                    0
```

6.7. SIP Trunks

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

- AT&T access – SIP Trunk 2
  - Note that this trunk will use TCP port 5080 as described in **Section 5.5.1**.
- Local for Avaya Aura® Messaging and Avaya SIP telephone access – SIP Trunk 1
  - Note that this trunk will use TCP port 5060 as described in **Section 5.5.2**.

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

Note – In the reference configuration, TCP (port 5060 or 5080) is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis, however, Avaya best practices call for TLS (port 5061) to be used as transport protocol in customer environments whenever possible.

6.7.1. SIP Trunk for Inbound 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. This trunk corresponds to the **ACM601_5080** Entity defined in **Section 5.4.2**.

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp**. Note – Although TCP is used as the transport protocol between the Avaya CPE components, the transport protocol used between the Avaya SBCE and the AT&T IP Toll Free service is UDP.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** Is set to **y** and that **Peer Server** is **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.3**
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g., **ASM61**).
- **Near-end Listen Port** and **Far-end Listen Port** – set to **5080** (see Transport Method note above).
- **Far-end Network Region** – Set the IP network region to **2**, as set in **Section 6.5.2**.
- **Far-end Domain** – Enter **customerb.com**. This is the domain provisioned for Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized 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 sends SIP OPTIONS messages to Session Manager to provide link status.

```
add signaling-group 2                                           Page   1 of   1
                                SIGNALING GROUP
 Group Number: 2              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
   Near-end Node Name: procr                      Far-end Node Name: ASM61
 Near-end Listen Port: 5080                     Far-end Listen Port: 5080
                                             Far-end Network Region: 2
                                   Far-end Secondary Node Name:
Far-end Domain: customerb.com
                                                  Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                       RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload                 Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                          IP Audio Hairpinning? n
         Enable Layer 3 Test? Y                          Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n                  Alternate Route Timer(sec): 6
```

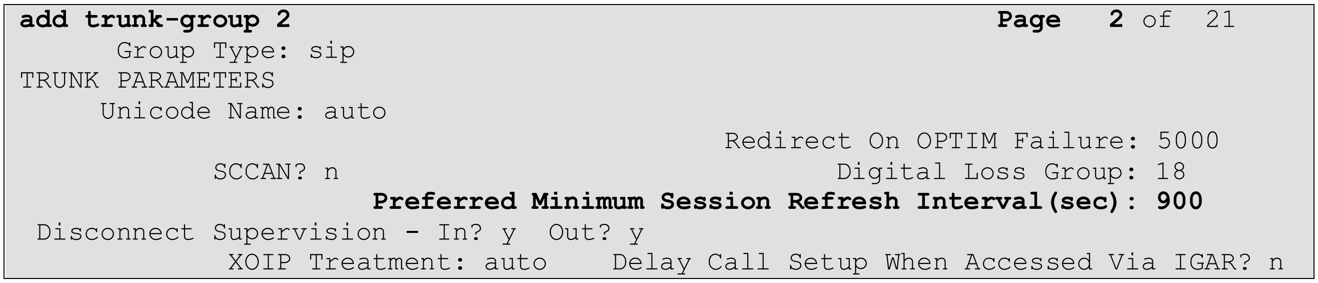
Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **2**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **ATT**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **102**).
- **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., **2**).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g., **20**).

```
add trunk-group 2                                               Page   1 of  21
                                TRUNK GROUP
Group Number: 2                   Group Type: sip         CDR Reports: y
  Group Name: ATT                        COR: 1        TN: 1        TAC: 102
   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: 2
                                              Number of Members: 20
```

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

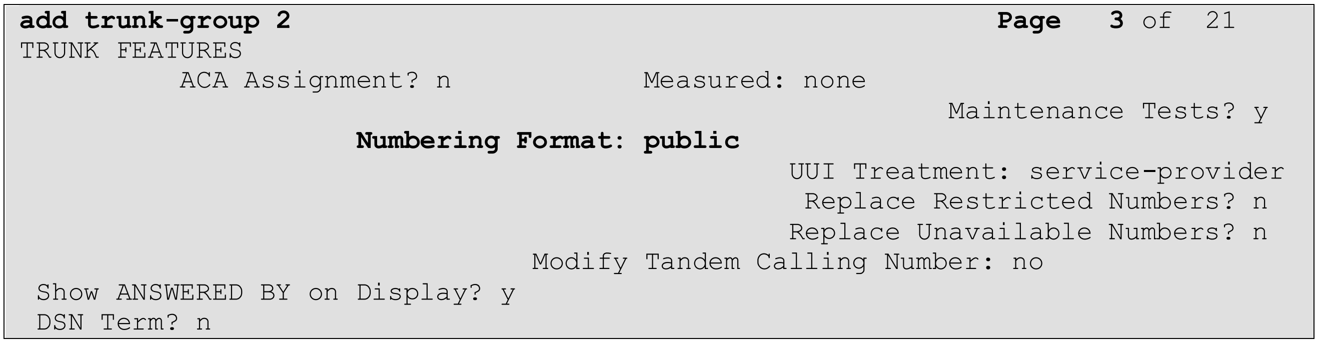
- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900.** This entry will actually cause a value of 1800 to be generated in the SIP header.



```
add trunk-group 2                                            Page   2 of  21
      Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                            Redirect On OPTIM Failure: 5000
            SCCAN? n                                   Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
 Disconnect Supervision - In? y  Out? y
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

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

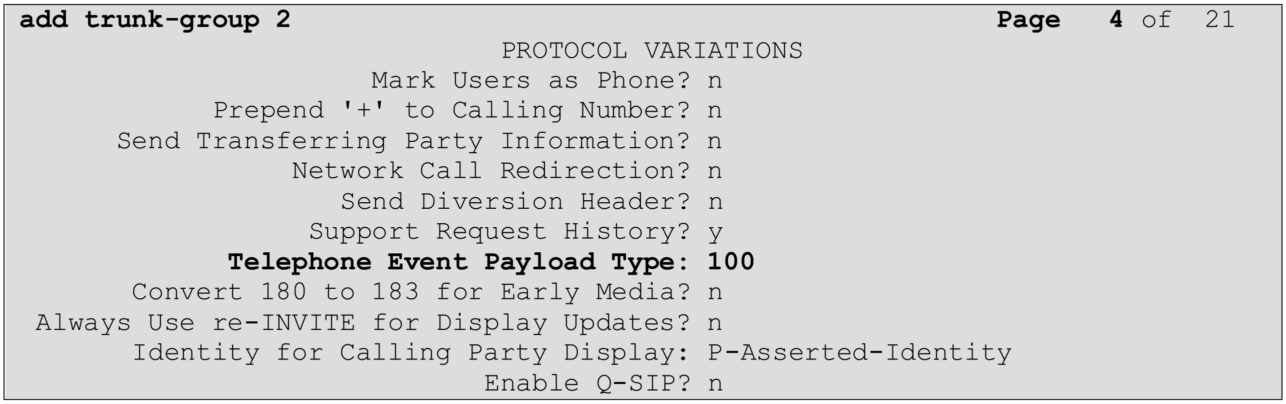
- Set N**umbering Format:** to **public**



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

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

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



```
add trunk-group 2                                            Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 100
       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

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

This section describes the steps for administering the local SIP trunk for Avaya Aura® Messaging and Avaya SIP station calls. This trunk corresponds to the **ACM601** Entity defined in **Section 5.4.3**.

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

- **Group Type** – Set to **sip**.
- **Transport Method** – Set to **tcp**. Note – Although TCP is used as the transport protocol between the Avaya CPE components, the transport protocol used between the Avaya SBCE and the AT&T IP Toll Free service is UDP.
- Verify that **IMS Enabled?** is set to **n**.
- Verify that **Peer Detection Enabled?** Is set to **y** and that **Peer Server** is **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 6.3**
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g., **ASM61**).
- **Near-end Listen Port** and **Far-end Listen Port** – set to **5060** (see Transport Method note above).
- **Far-end Network Region** – Set to the IP network region **1**, as defined in **Section 6.5.1**.
- **Far-end Domain** – Enter **customerb.com**. This is the domain used by Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized 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 sends SIP OPTIONS messages to Session Manager to provide link status.

```
add signaling-group 1                                       Page   1 of   1
                                SIGNALING GROUP
 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                            SIP Enabled LSP? n
     IP Video? n                                  Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
   Near-end Node Name: procr                 Far-end Node Name: ASM61
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
                                   Far-end Secondary Node Name:
Far-end Domain: customerb.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., **1**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **Local**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., **101**).
- **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., **1**).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g., **20**).

```
add trunk-group 1                                            Page   1 of  21
                                TRUNK GROUP
Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: Local                         COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? N
                                              Member Assignment Method: auto
                                              Signaling Group: 1
                                              Number of Members: 20
```

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

- 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 1                                            Page   2 of  21
      Group Type: sip
TRUNK PARAMETERS
     Unicode Name: auto
                                            Redirect On OPTIM Failure: 5000
            SCCAN? n                                Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 900
 Disconnect Supervision - In? y  Out? y
             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

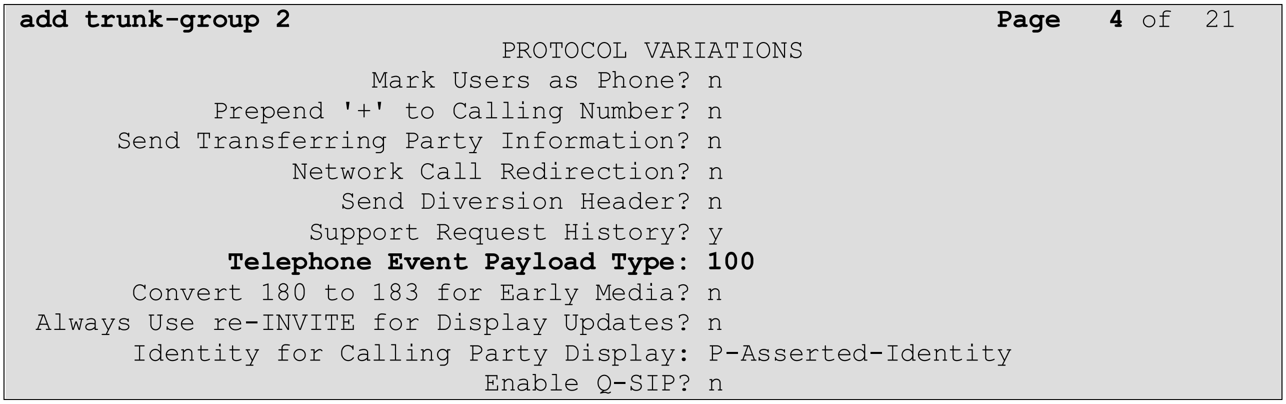
Step 4 - On **Page 3** of the **Trunk Group** form:

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

```
add trunk-group 1                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y
                     Numbering Format: private
                                                UUI Treatment: service-provider
                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
 DSN Term? n
```

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

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



```
add trunk-group 2                                          Page   4 of  21
                              PROTOCOL VARIATIONS
                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? n
                 Network Call Redirection? n
                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 100
       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

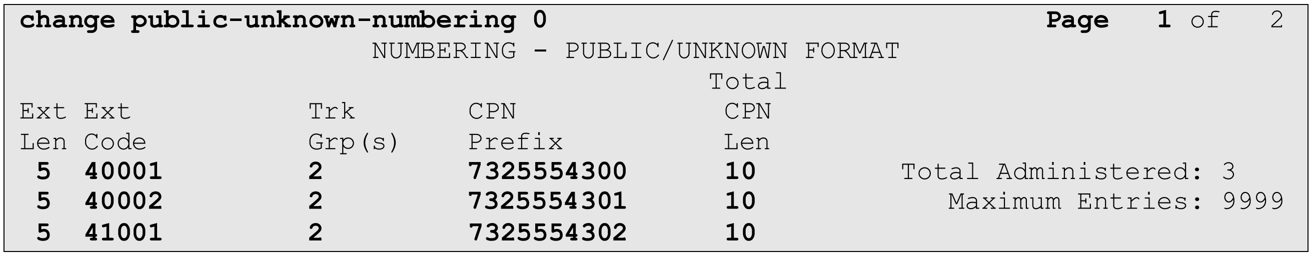
6.8. Public Unknown Numbering

In the **public-unknown-numbering** form, Communication Manager local extensions are converted to AT&T Toll Free DNIS numbers (previously identified by AT&T) for inclusion in any SIP headers directed to the AT&T Toll Free service via the public trunk defined in **Section 6.7.1**.

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

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension (e.g., **40001**).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g., **2**).
- **CPN Prefix** – Enter the corresponding AT&T IP Toll Free DNIS number (e.g., **7325554300**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g., **10**).

Step 2 – Repeat **Step 1** for all AT&T IP Toll Free DNIS numbers and their corresponding Communication Manager extensions.



```
change public-unknown-numbering 0                             Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                        Total
Ext Ext              Trk      CPN         CPN
Len Code             Grp(s)   Prefix      Len
 5  40001            2        7325554300  10        Total Administered: 3
 5  40002            2        7325554301  10           Maximum Entries: 9999
 5  41001            2        7325554302  10
```

6.9. Private Numbering

The private-numbering form is used to direct calls to Avaya Aura® Messaging (call coverage/retrieval) to the local trunk defined in **Section 6.7.2**. It is also used to define the local extensions used by the SIP telephones.

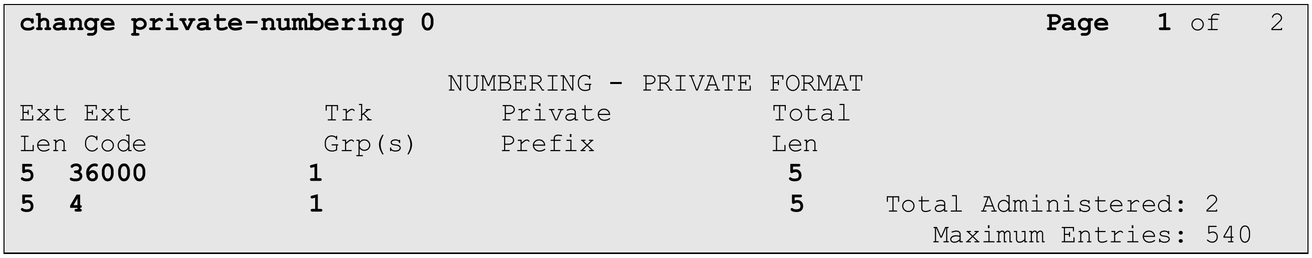
Step 1 - Using the **change private-numbering 0** command, enter the following for the messaging pilot number:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension assigned to the Avaya Aura® Messaging coverage hunt group defined in **Section 6.12** (e.g., **36000**).

- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).

Step 2 - Enter the following for the SIP phone local extensions:

- **Ext Len** – Enter the total number of digits in the local extension range (e.g., **5**).
- **Ext Code –** Enter the Communication Manager extension range used by the SIP telephones (e.g., **4**).
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g., **1**).
- **Total Len** – Enter the total number of digits after the digit conversion (e.g., **5**).



```
change private-numbering 0                                      Page   1 of   2

                           NUMBERING - PRIVATE FORMAT
Ext Ext           Trk        Private           Total
Len Code          Grp(s)     Prefix            Len
5   36000        1                              5
5   4            1                              5     Total Administered: 2
                                                         Maximum Entries: 540
```

6.10. Route Patterns

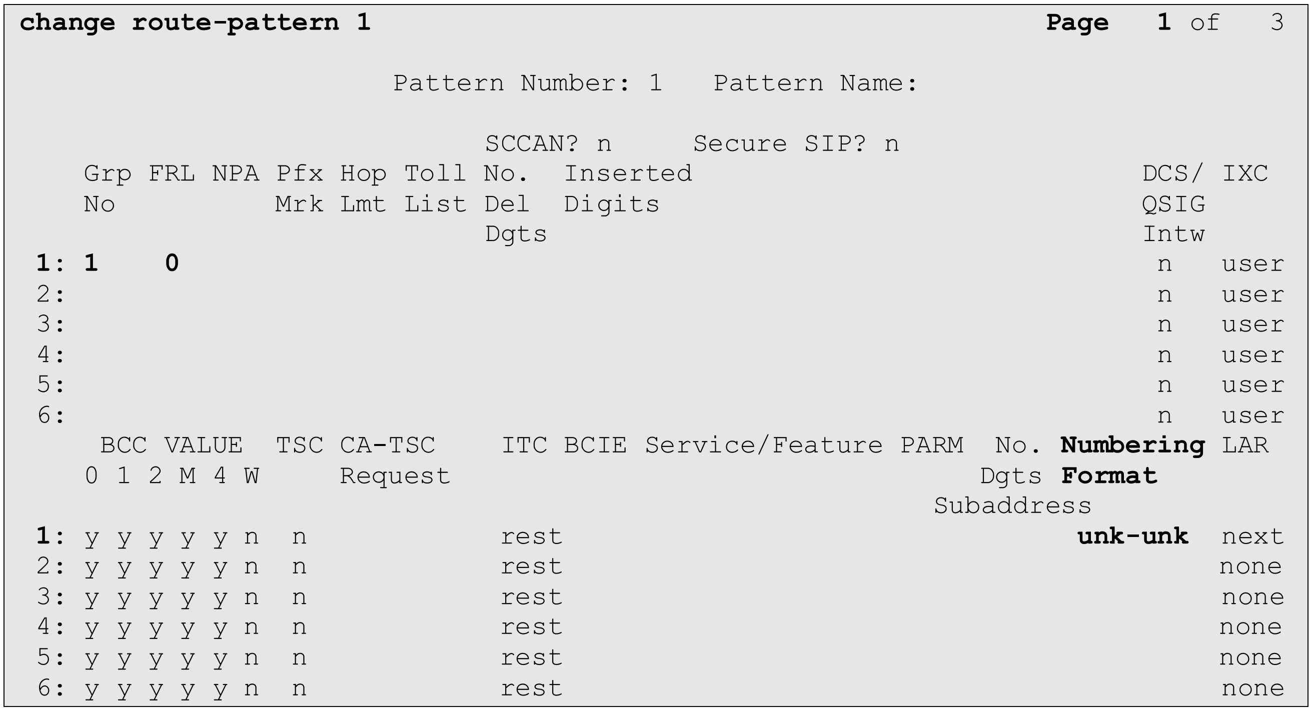
The AT&T IP Toll Free service does not support outbound dialing, so a route pattern is not required to direct calls to the public trunk. However a route pattern is used to direct calls to the local trunk.

6.10.1. Route Pattern for Calls to Aura® Messaging

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

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

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



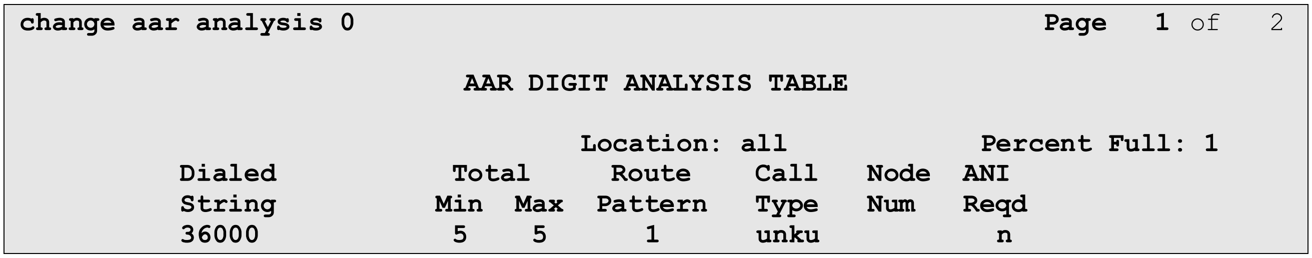
```
change route-pattern 1                                          Page   1 of   3

                       Pattern Number: 1   Pattern Name:

                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 1    0                                                             n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user
     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                unk-unk  next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

6.11. AAR Dialing

Automatic Alternate Routing (AAR) is used to direct coverage calls for Avaya Aura® Messaging (36000) to the route pattern defined in **Section 6.10**.

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 **1**
- **Call Type** enter **unku**



```
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      1       unku           n
```

6.12. Provisioning for Coverage to Aura® Messaging

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

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

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

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

```
add hunt-group 1                                                Page   1 of  60
                                  HUNT GROUP

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

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

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

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

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

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

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

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

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

```
add coverage path 1                                         Page   1 of   1
                                COVERAGE PATH
                   Coverage Path Number: 1
     Cvg Enabled for VDN Route-To Party? n        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:
```

6.12.3. Station Coverage Path to Avaya Aura® Messaging

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

Step 1 – Enter the command **change station xxxxx**, where **xxxxx** is a previously defined station or agent extension (e.g., Agent **47002**), and on **Page 1** of the form enter the following:

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

```
change 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:   :
     WARNING:  Agent must log in again before changes take effect
```

6.13. 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 [5], [6] and [7] 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
```

7. Avaya Aura® Messaging

In this reference configuration, Avaya Aura® Messaging is used to verify DTMF, Message Waiting Indicator (MWI), as well as basic call coverage functionality. The administration for Avaya Aura® Messaging is beyond the scope of these Application Notes. Consult [8] and [9] for further details.

8. Configure Avaya Session Border Controller for Enterprise

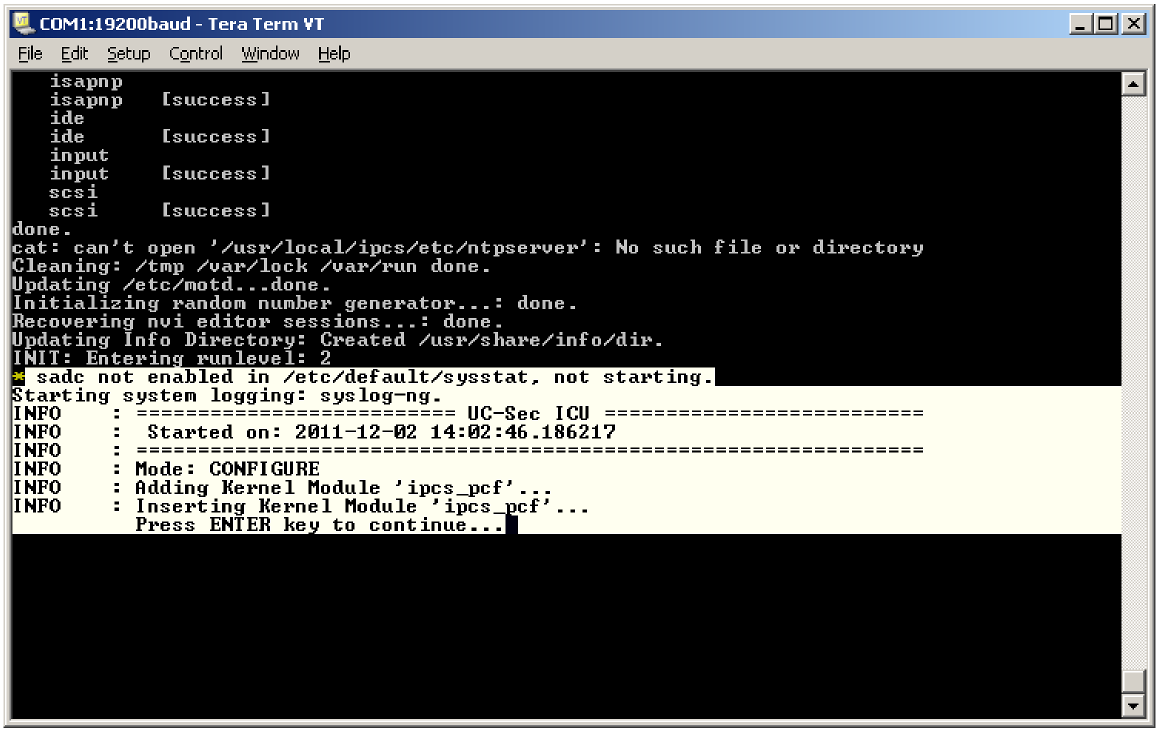
8.1. Initial Provisioning

The following sections describe the provisioning of the Avaya SBCE.

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

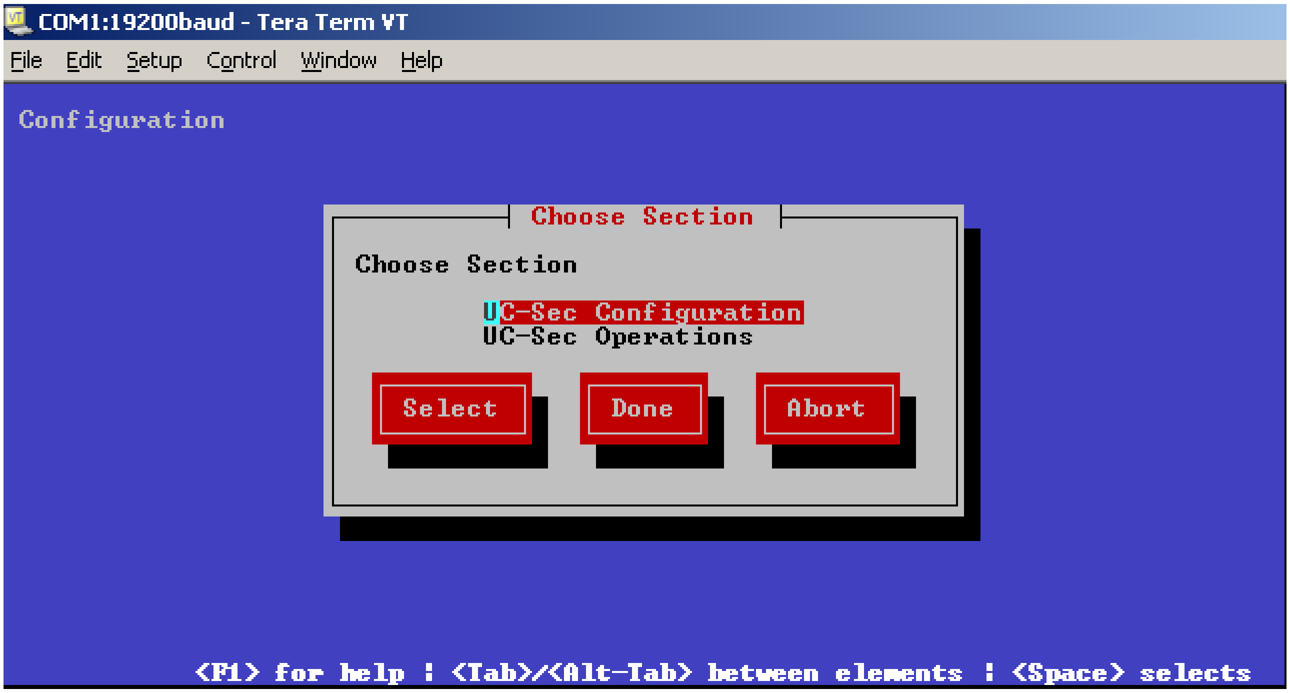
The Avaya SBCE was configured via a serial console port connection and via an IP connection once the basic system provisioning was completed. The platform was configured as a single **EMS + UC-SEC** configuration. The following are the steps required for provisioning the basic configuration:

1. Connect to the console port on the back of the server.
2. Start the serial connection application (i.e. Hyperterminal, Putty, etc.)
3. Power on the equipment.
4. The system will recognize that there is no configuration and will prompt the user to enter Config mode by asking the user to hit **Enter** twice.


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help

```
   isapnp
   isapnp    [success]
   ide
   ide       [success]
   input
   input     [success]
   scsi
   scsi      [success]
done.
cat: can't open '/usr/local/ipcs/etc/ntpserver': No such file or directory
Cleaning: /tmp /var/lock /var/run done.
Updating /etc/motd...done.
Initializing random number generator...: done.
Recovering nvi editor sessions...: done.
Updating Info Directory: Created /usr/share/info/dir.
INIT: Entering runlevel: 2
* sadc not enabled in /etc/default/sysstat, not starting.
Starting system logging: syslog-ng.
INFO     : ========================== UC-Sec ICU ==========================
INFO     :  Started on: 2011-12-02 14:02:46.186217
INFO     : ================================================================
INFO     : Mode: CONFIGURE
INFO     : Adding Kernel Module 'ipcs_pcf'...
INFO     : Inserting Kernel Module 'ipcs_pcf'...
           Press ENTER key to continue...
```

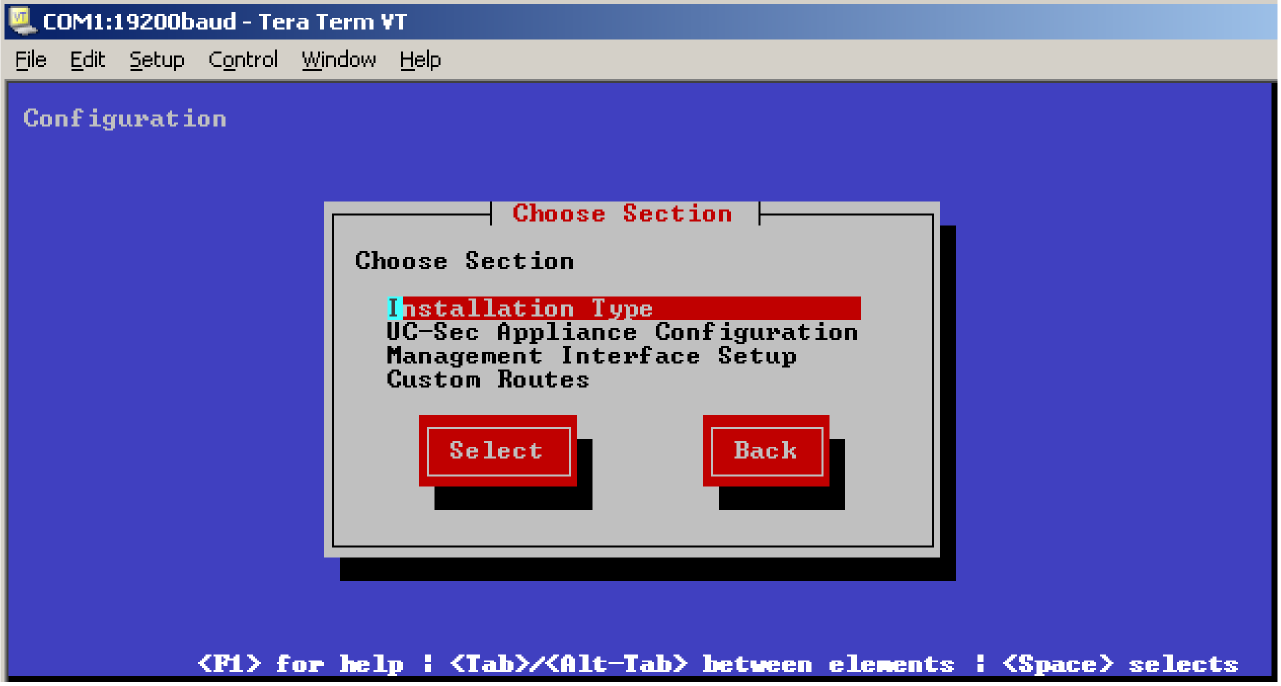
4. A menu will appear. Select **UC Sec Configuration**



COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help

```
Configuration

                 Choose Section

   Choose Section

           UC-Sec Configuration
           UC-Sec Operations

     Select        Done        Abort

  <F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

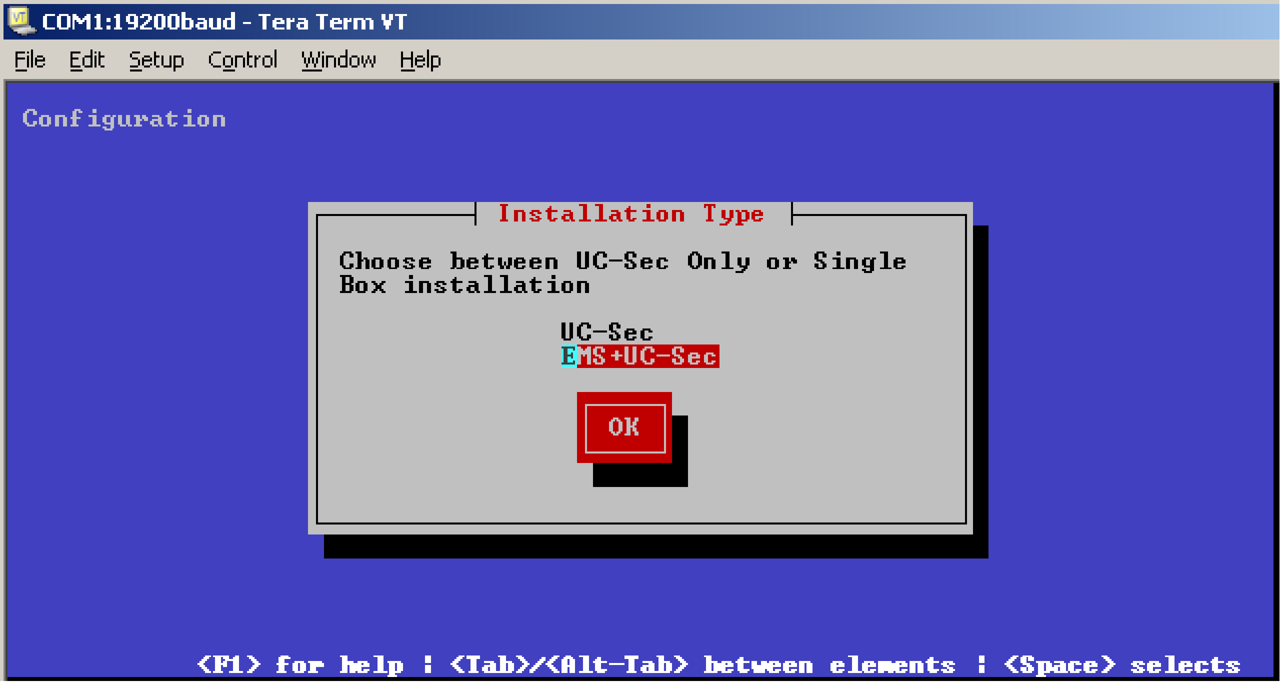
7. Select **Installation Type**



COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help

```
Configuration

                 Choose Section

   Choose Section

     Installation Type
     UC-Sec Appliance Configuration
     Management Interface Setup
     Custom Routes

       Select            Back

  <F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

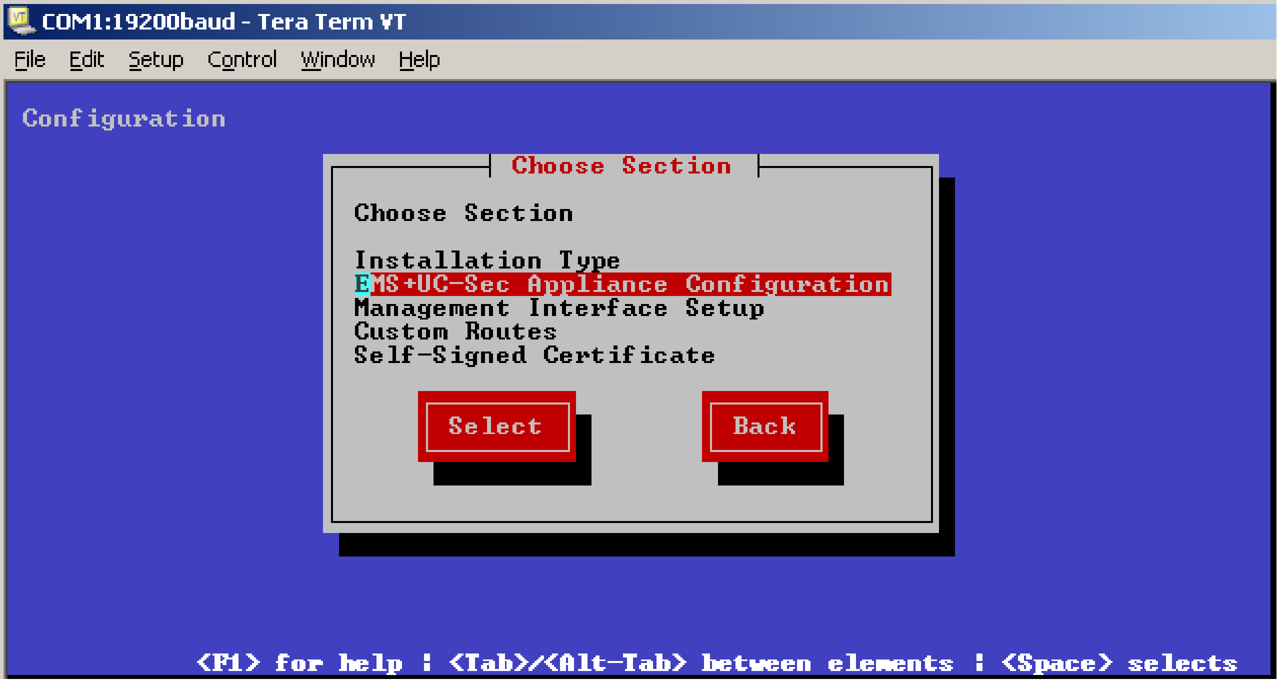
8. Select **EMS + UC-SEC**



COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help

```
Configuration

Installation Type

Choose between UC-Sec Only or Single
Box installation

UC-Sec
EMS+UC-Sec

OK

<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

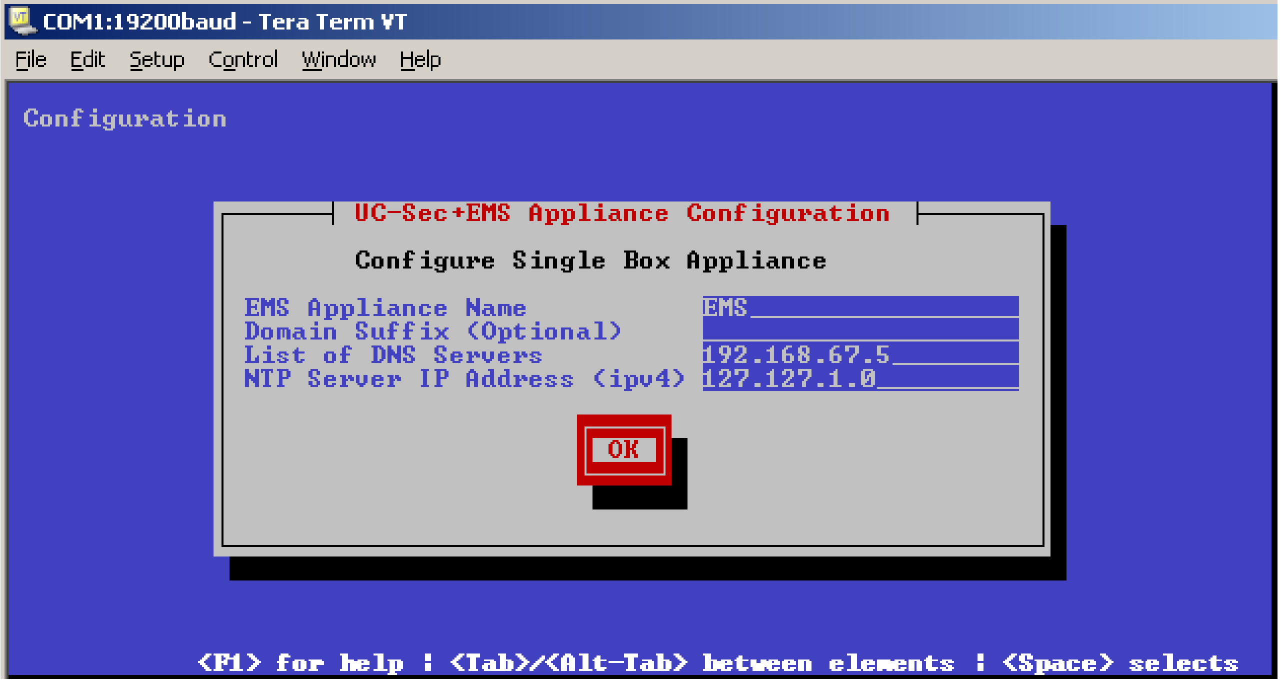
9. Select **EMS + UC-SEC Appliance Configuration**



COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help

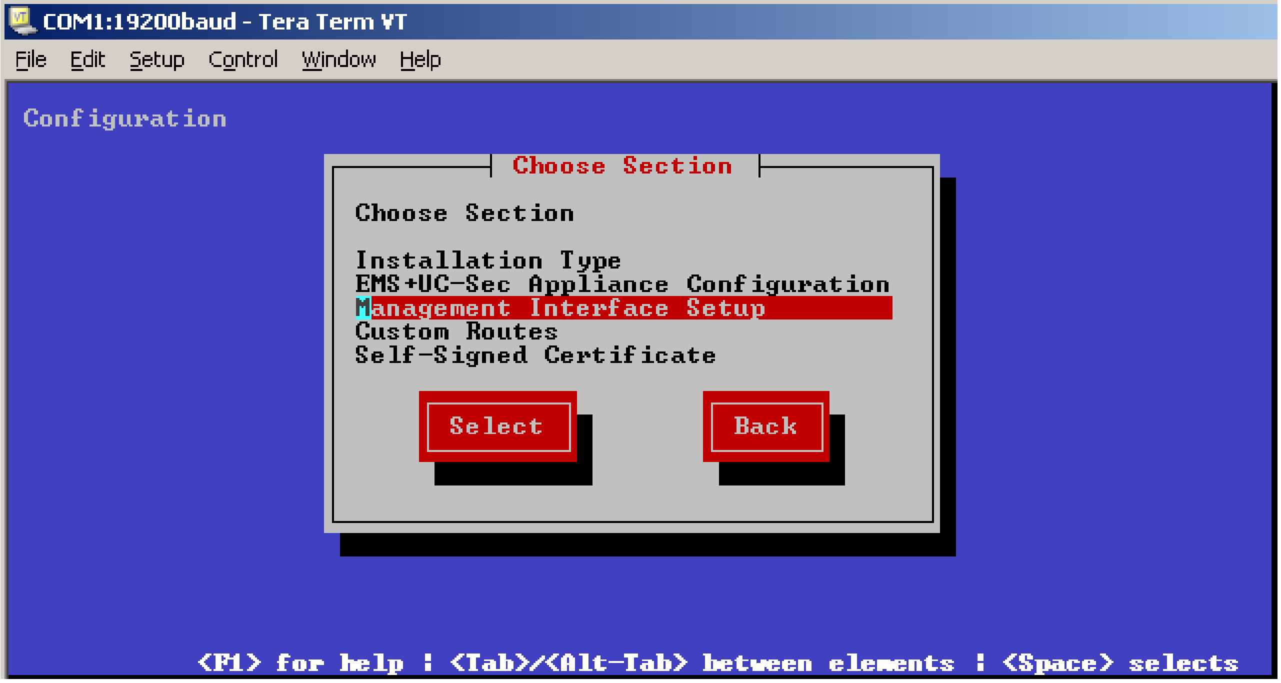
```
Configuration

Choose Section

Choose Section

Installation Type
EMS+UC-Sec Appliance Configuration
Management Interface Setup
Custom Routes
Self-Signed Certificate

Select          Back

<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

10. Enter or leave Name as default (e.g., **EMS**). Enter IP address of DNS Servers if applicable. If no NTP leave default value. Press OK


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
OK

```
Configuration

            UC-Sec+EMS Appliance Configuration

              Configure Single Box Appliance

  EMS Appliance Name              EMS
  Domain Suffix (Optional)
  List of DNS Servers             192.168.67.5
  NTP Server IP Address (ipv4)    127.127.1.0

<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

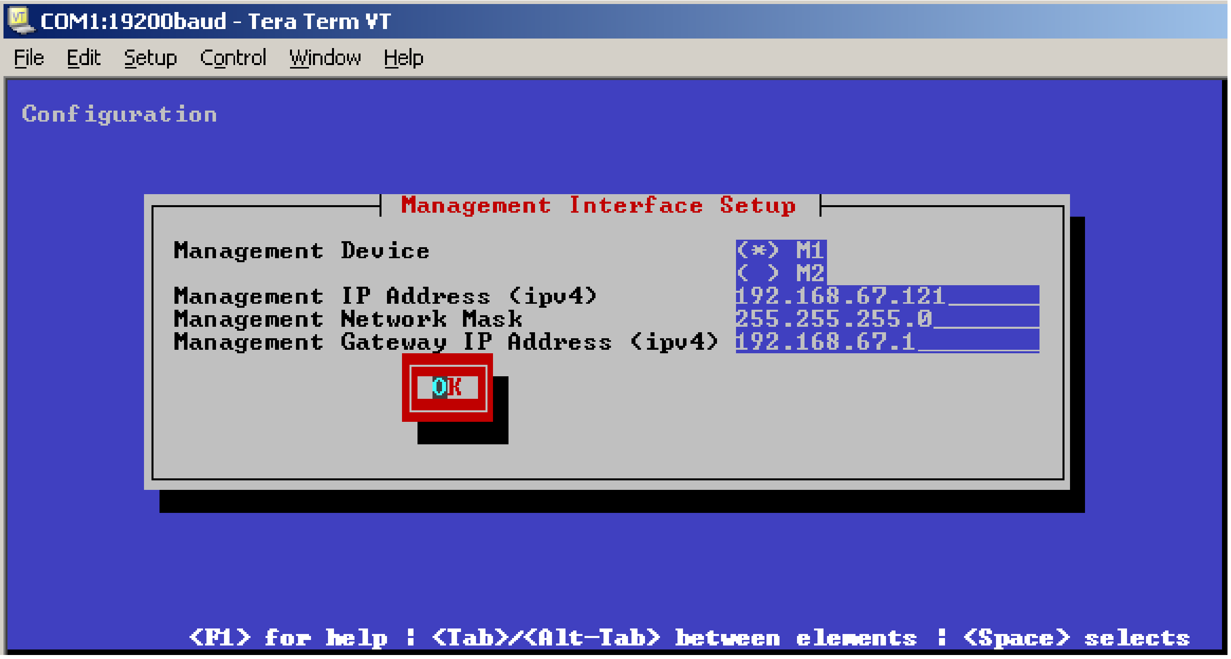
11. Select **Management Interface Setup**.


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Select
Back

```
Configuration

            Choose Section

  Choose Section

  Installation Type
  EMS+UC-Sec Appliance Configuration
  Management Interface Setup
  Custom Routes
  Self-Signed Certificate

<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

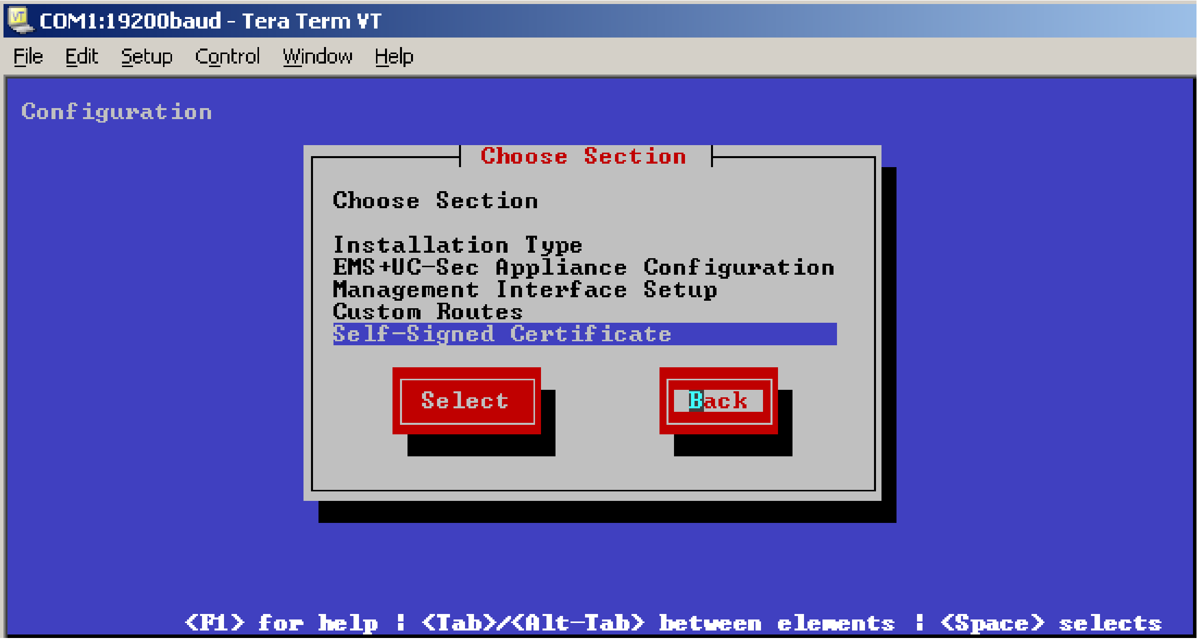
12. Select the **M1** interface. Enter the IP address you want for management (e.g. **192.168.67.121**). Enter mask and gateway. Select OK

IMPORTANT! – The Management interface must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Management Interface Setup
OK
<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects

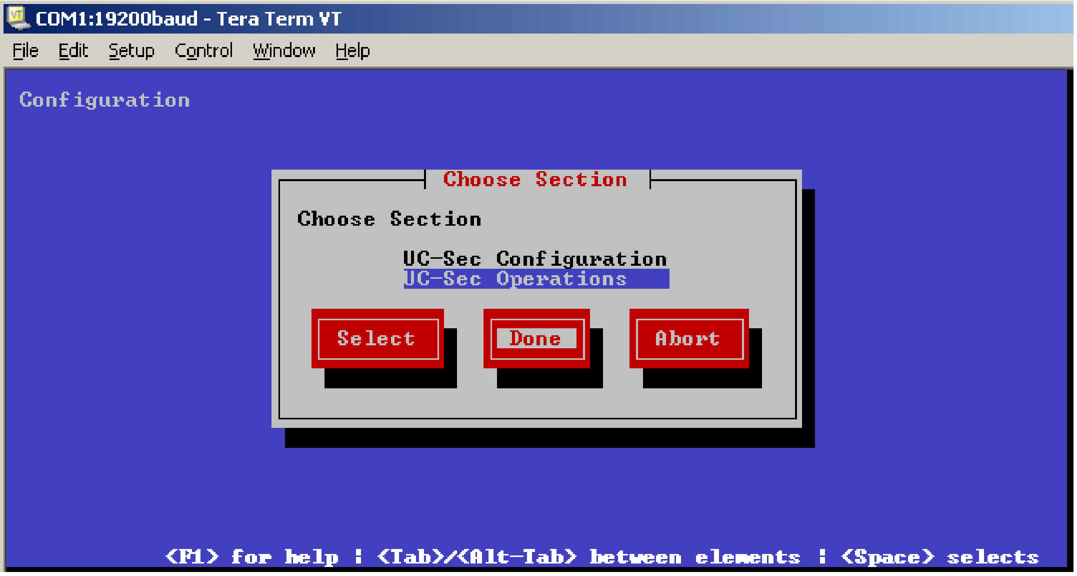
```
Management Device                      (*) M1
                                       ( ) M2
Management IP Address (ipv4)           192.168.67.121
Management Network Mask                255.255.255.0
Management Gateway IP Address (ipv4)   192.168.67.1
```

13. You will be returned to the prior menu. Select **Back**.


COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Configuration
Choose Section
Select
Back
<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects

```
Choose Section

Installation Type
EMS+UC-Sec Appliance Configuration
Management Interface Setup
Custom Routes
Self-Signed Certificate
```

14. Select **Done**. The SBC will reboot.



```
Configuration

Choose Section

Choose Section

UC-Sec Configuration
UC-Sec Operations

<F1> for help | <Tab>/<Alt-Tab> between elements | <Space> selects
```

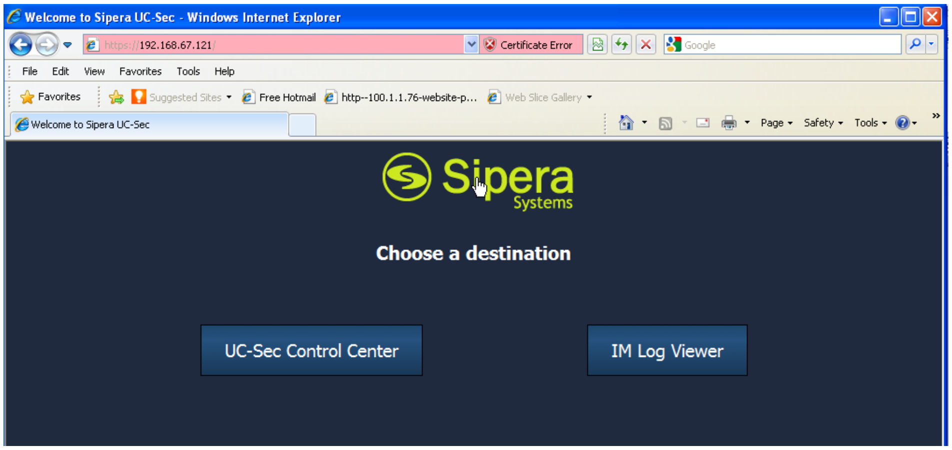
COM1:19200baud - Tera Term VT
File Edit Setup Control Window Help
Select
Done
Abort

15. After the SBC reboots you will be prompted to press Enter as before. The SBC will then prompt for the date and time.
16. The SBC will prompt you for the password for “root” and then user “ipcs”. Enter appropriate passwords for each.
17. The initial installation is complete and any further configuration will be done in the web interface.

8.2. Advanced Configuration

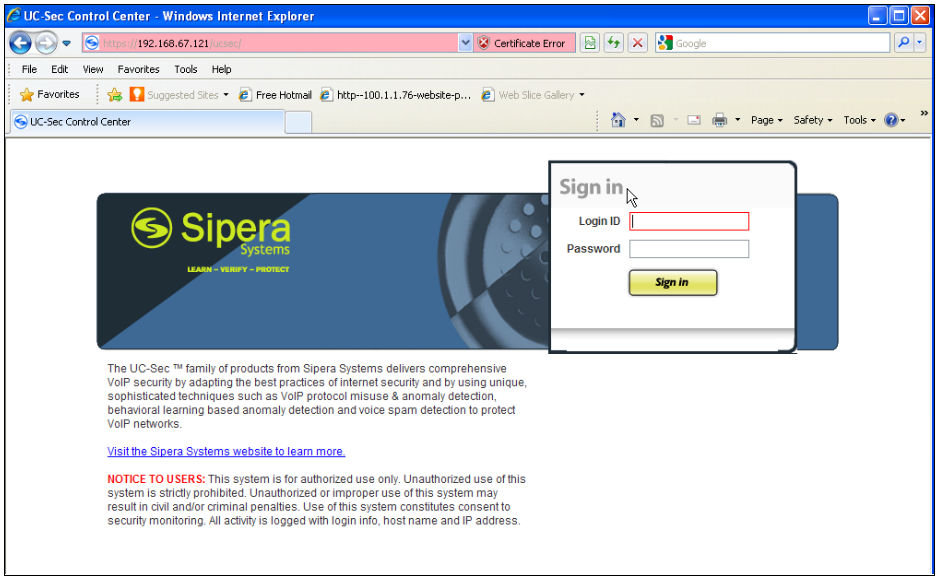
The follow provisioning is performed via the Avaya SBCE GUI interface.

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



Choose a destination

3. Enter the login ID and password



The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

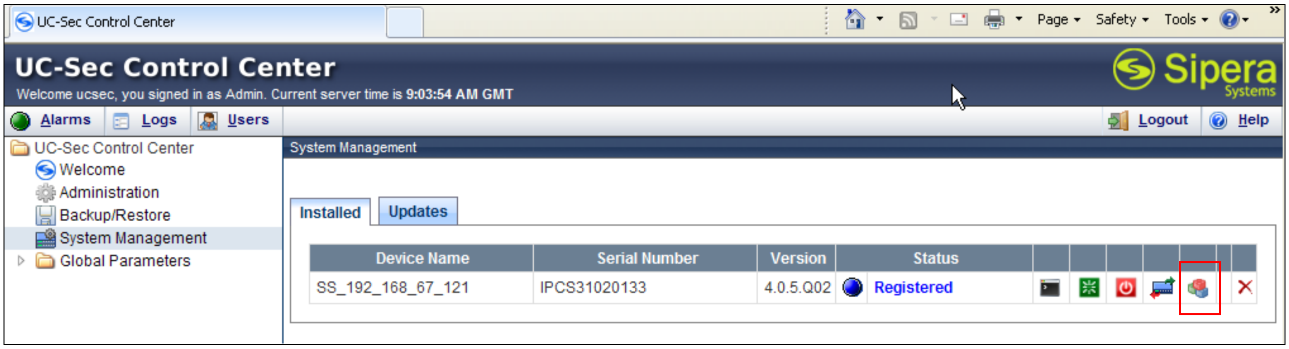
Visit the Sipera Systems website to learn more.

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

8.3. System Management

When accessing the Avaya SBCE system for the first time through the web interface, the user needs to configure some basic parameters.

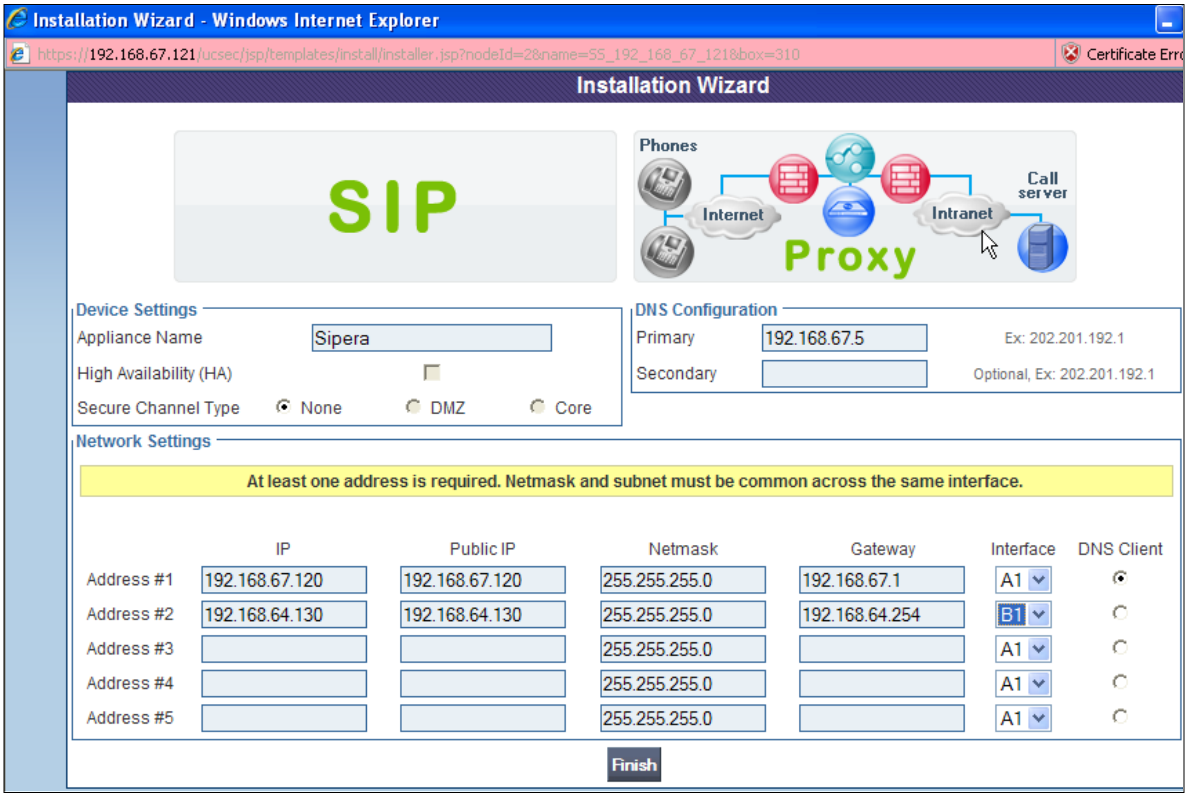
1. Click on **System Management**, the user will see the screen below:



Welcome ucsec, you signed in as Admin. Current server time is 9:03:54 AM GMT

Device Name	Serial Number	Version	Status
SS_192_168_67_121	IPCS31020133	4.0.5.Q02	● Registered

2. The initial status of the SBCE is **Registered**, as shown in the above diagram. User should then click on the **install** button (highlighted in red). Click on the **System Management**, the screen below will open:


Installation Wizard - Windows Internet Explorer
https://192.168.67.121/ucsec/jsp/templates/install/installer.jsp?nodeId=2&name=55_192_168_67_121&box=310
Certificate Err
SIP
Phones
Internet
Intranet
Call server
Proxy

Installation Wizard

Device Settings

Appliance Name	Sipera
High Availability (HA)	□
Secure Channel Type	● None ○ DMZ ○ Core

DNS Configuration

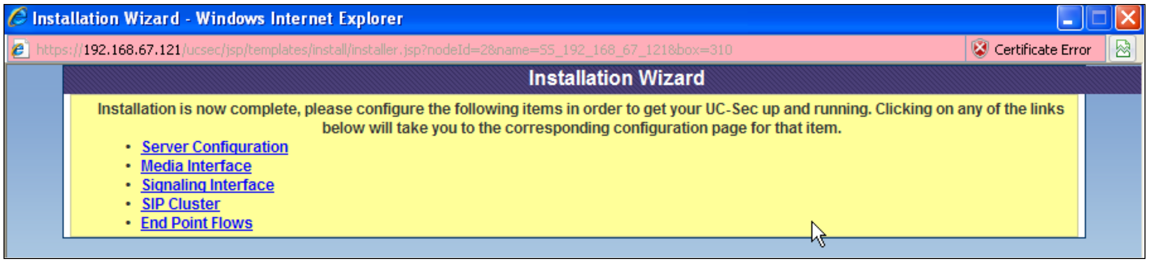
Primary	192.168.67.5	Ex: 202.201.192.1
Secondary		Optional, Ex: 202.201.192.1

Network Settings

At least one address is required. Netmask and subnet must be common across the same interface.

	IP	Public IP	Netmask	Gateway	Interface	DNS Client
Address #1	192.168.67.120	192.168.67.120	255.255.255.0	192.168.67.1	A1	●
Address #2	192.168.64.130	192.168.64.130	255.255.255.0	192.168.64.254	B1	○
Address #3			255.255.255.0		A1	○
Address #4			255.255.255.0		A1	○
Address #5			255.255.255.0		A1	○

3. Enter the following information:
   - **Device Settings → Appliance Name** – Enter a descriptive name (e.g. **Sipera**).
   - **DNS Configuration → Primary** – Enter the IP address of a DNS Server if applicable.
   - **Network Settings → Address #1** – Note this will be the trusted "inside" interface:
     - Enter the appropriate IP address for **IP** and **Public IP** (the same address in each field).
     - Enter the appropriate **Netmask** and **Gateway**
     - Select interface **A1** (this interface is labeled **A1** on the back of the chassis).
   - Repeat the previous steps for **Address #2**, (this will be the untrusted "outside" interface), using the appropriate IP addressing, Netmask, and Gateway. Select interface **B1**.
4. Click **Finish**, and the following screen will appear giving an outline of the remaining tasks. This window may be closed.


Installation Wizard - Windows Internet Explorer
https://192.168.67.121/ucsec/jsp/templates/install/installer.jsp?nodeId=2&name=55_192_168_67_121&box=310
Certificate Error

Installation Wizard

Installation is now complete, please configure the following items in order to get your UC-Sec up and running. Clicking on any of the links below will take you to the corresponding configuration page for that item.

- Server Configuration
- Media Interface
- Signaling Interface
- SIP Cluster
- End Point Flows

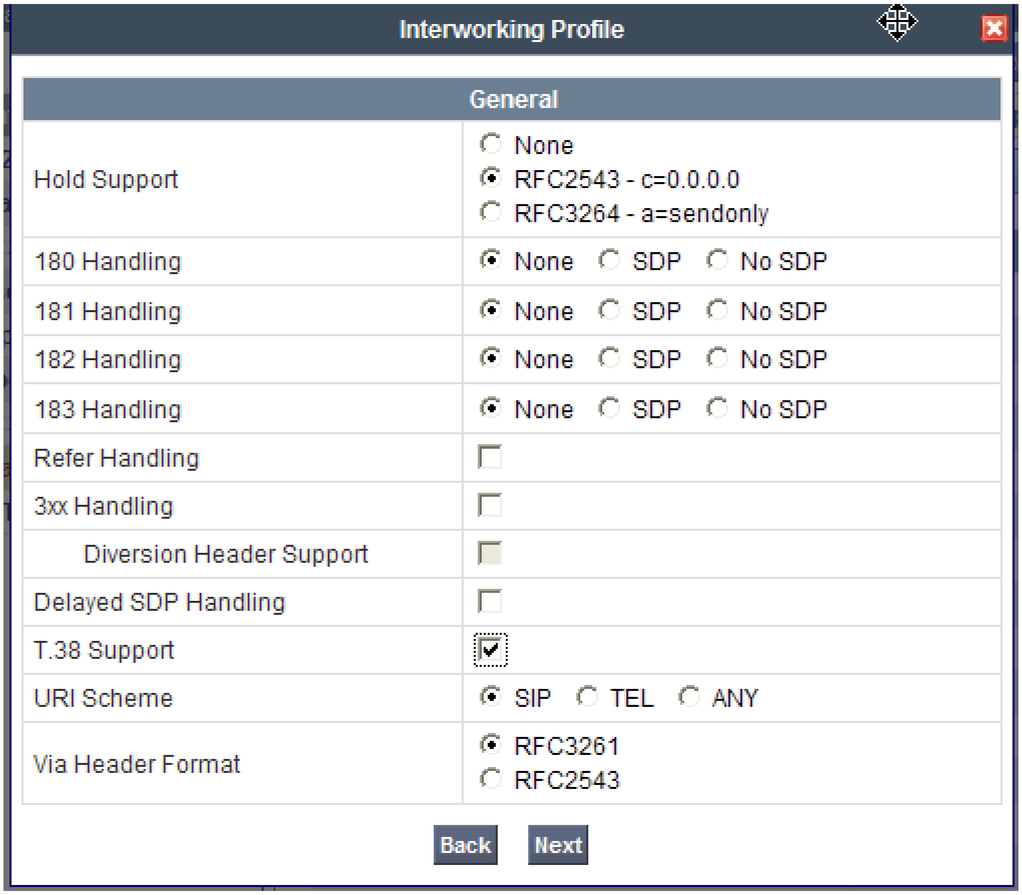
8.4. Global Profiles

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

8.4.1. Server Interworking – Avaya Side

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

1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Server Interworking**
3. Select **Add Profile**
4. Select the **General** Tab:
    a. Enter profile name**: Avaya**
    b. Check **Hold Support: →RFC2543**
    c. Check **T38 Support →Yes**
    d. All other options on the General Tab can be left at default.
    e. Select **Next**

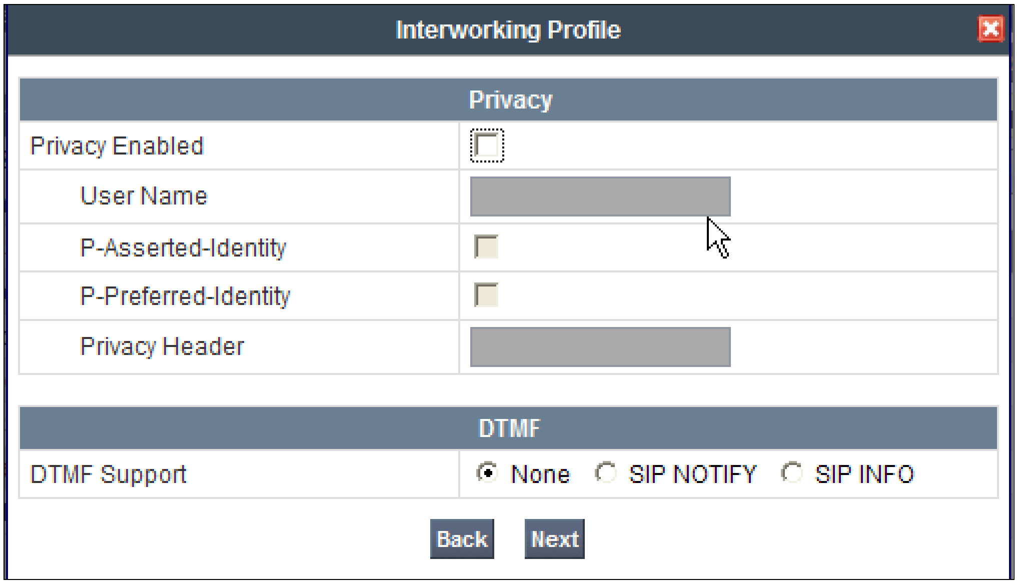


Interworking Profile

General

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

5. On the Privacy window
    a. Select **Next** to accept default values.

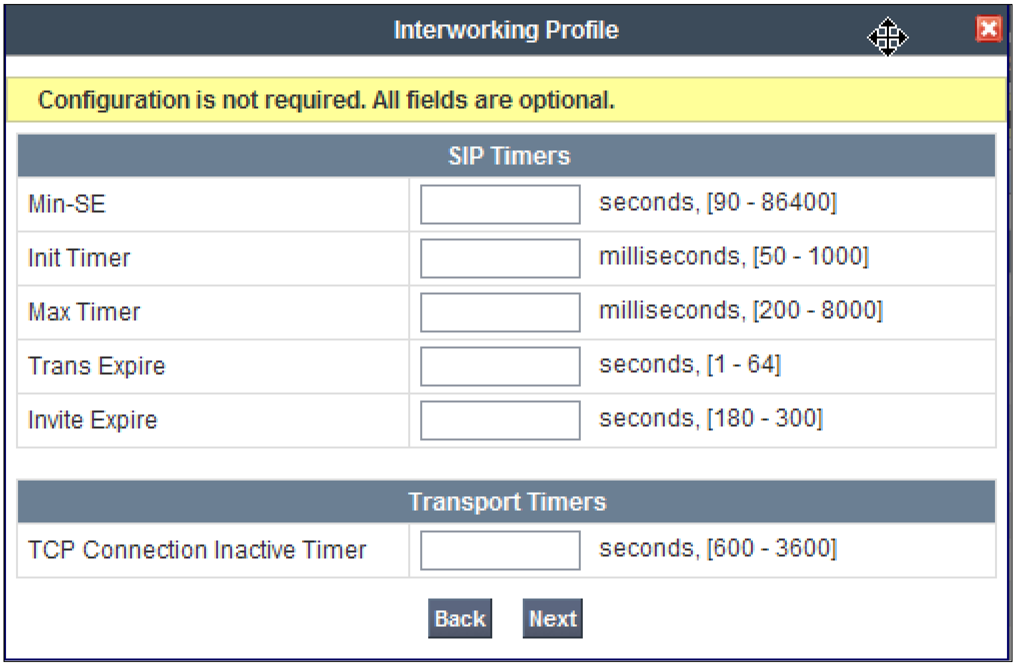


Interworking Profile

Privacy	
Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF	
DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO

6. On the **SIP Timers** window
   a. Select **Next** to accept default values.



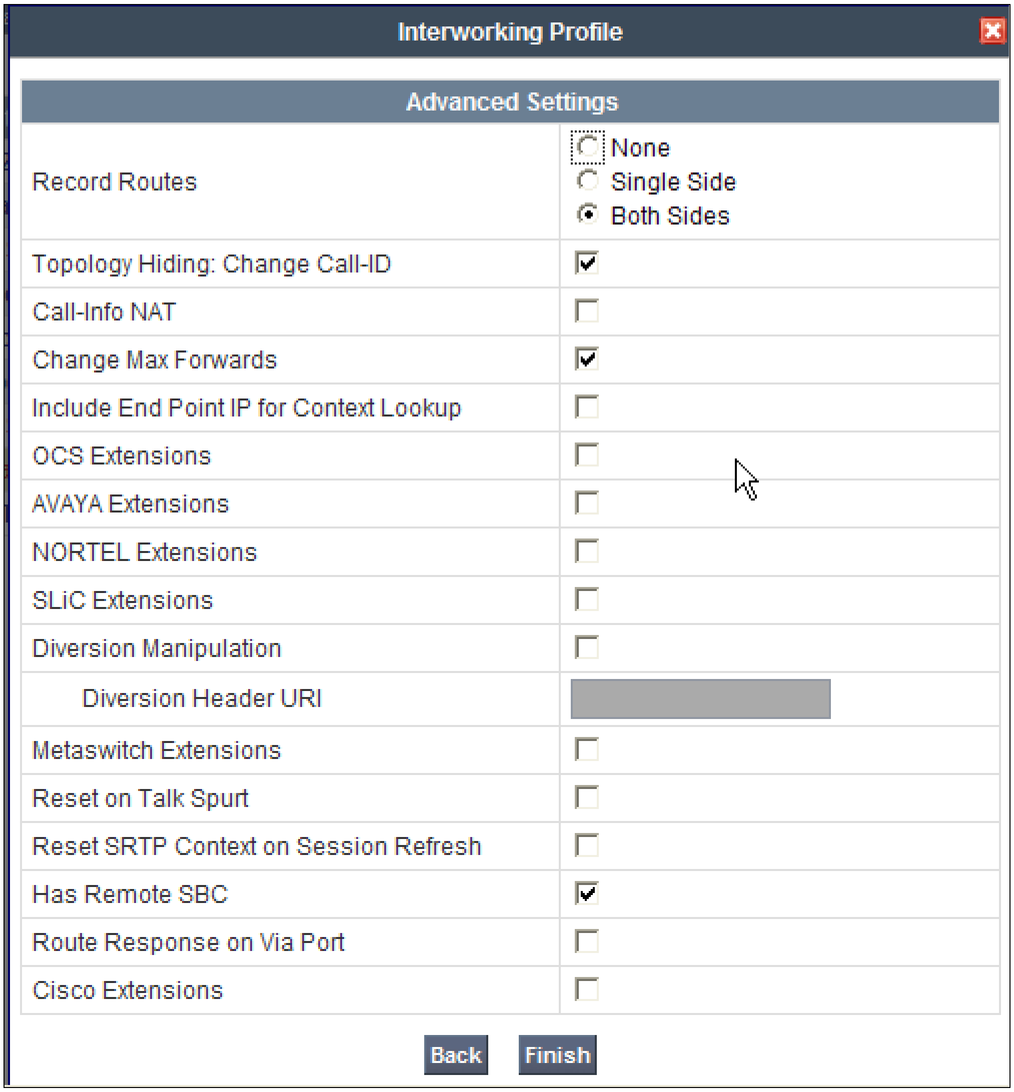
Interworking Profile

Configuration is not required. All fields are optional.

SIP Timers		
Min-SE		seconds, [90 - 86400]
Init Timer		milliseconds, [50 - 1000]
Max Timer		milliseconds, [200 - 8000]
Trans Expire		seconds, [1 - 64]
Invite Expire		seconds, [180 - 300]

Transport Timers		
TCP Connection Inactive Timer		seconds, [600 - 3600]

7. On the **Advanced Settings** window
   a. Select **Next** to accept default values.
   b. Click **Finish.**



Advanced Settings

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

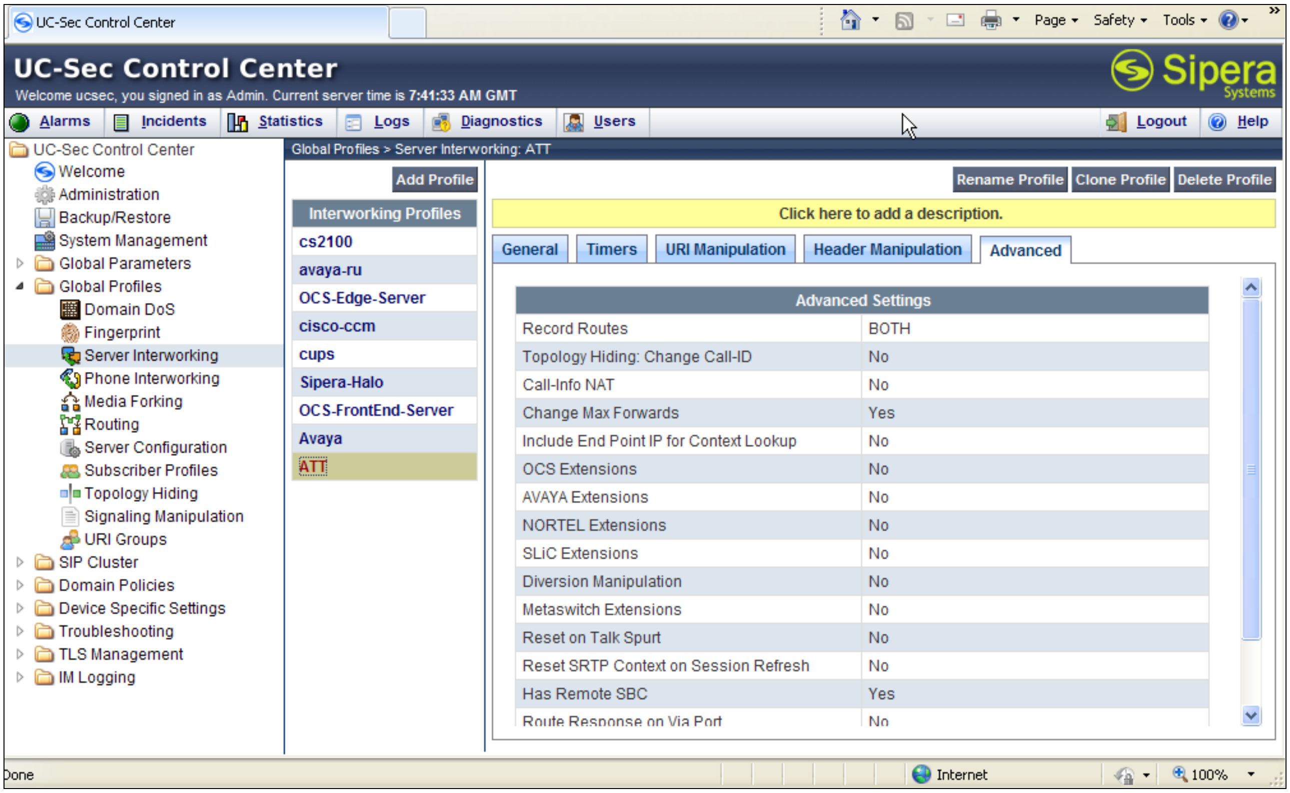
8.4.2. Server Interworking – AT&T Side

Repeat the steps shown in **Section 8.4.1** to add an Interworking Profile for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Server Interworking**
3. Select **Add Profile**
4. On the **General** Tab:
    a. Enter a profile name**:** (e.g., **ATT**)
    b. Check **T38 Support** □ **Yes**
    c. All other options on the General Tab can be left at default
    d. Select **Next**

5. At the **Privacy** tab

    a. Select **Next** to accept default values.
6. At the **Interworking Profile** tab
    a. Select **Next** to accept default values.
7. On the **Advanced** Tab
    a. Select **Next** to accept default values.
8. Click **Finish**

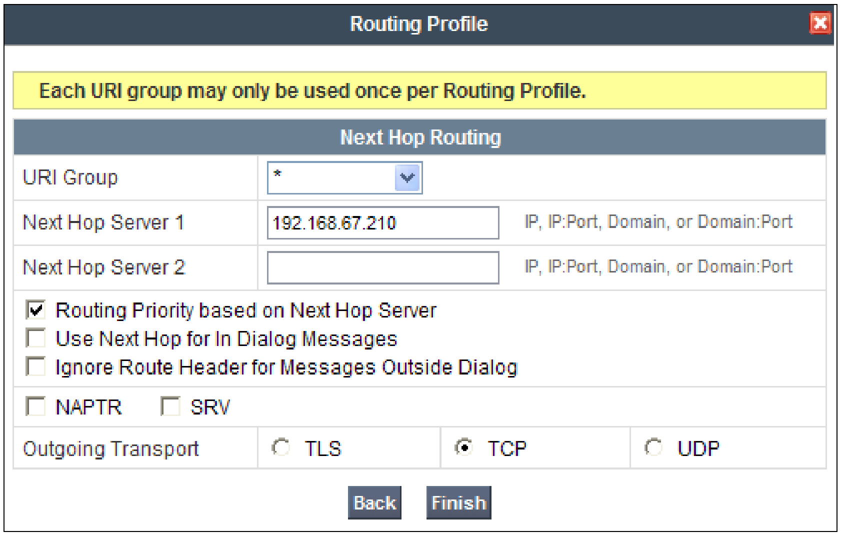


Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No

8.4.3. Routing – Avaya Side

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

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Routing** tab
3. Select **Add Profile**
4. Enter Profile Name: (e.g., **To_Avaya)**
5. Click **Next**
    a. **Next Hop Server 1: 192.168.67.210** (Session Manager IP address)
    b. Select **Routing Priority Based on Next Hop Server**
    c. **Outgoing Transport**: **TCP**
6. Click **Finish**



Routing Profile

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

Next Hop Routing

URI Group	*	
Next Hop Server 1	192.168.67.210	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

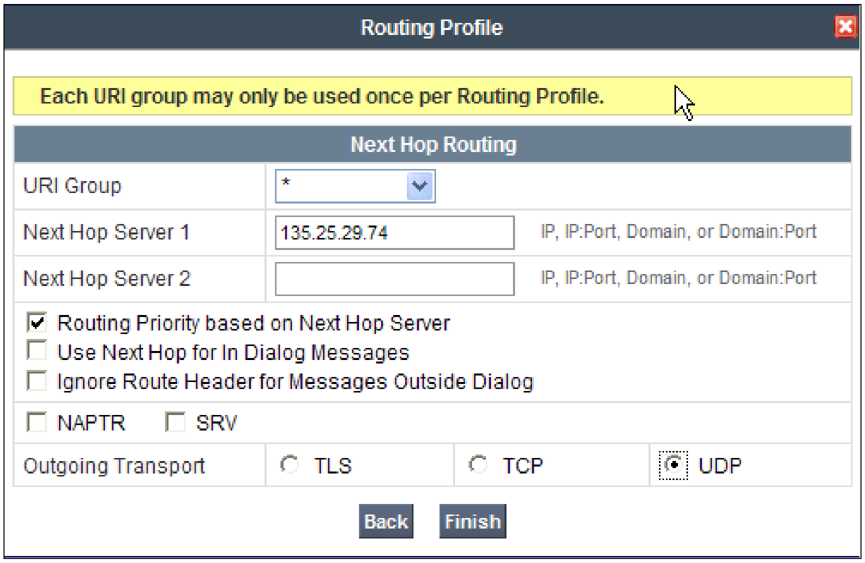
☐ NAPTR ☐ SRV

Outgoing Transport ○ TLS ● TCP ○ UDP

8.4.4. Routing – AT&T Side

Repeat the steps in **Section 8.4.3** to add a Routing Profile for the AT&T connection.

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



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

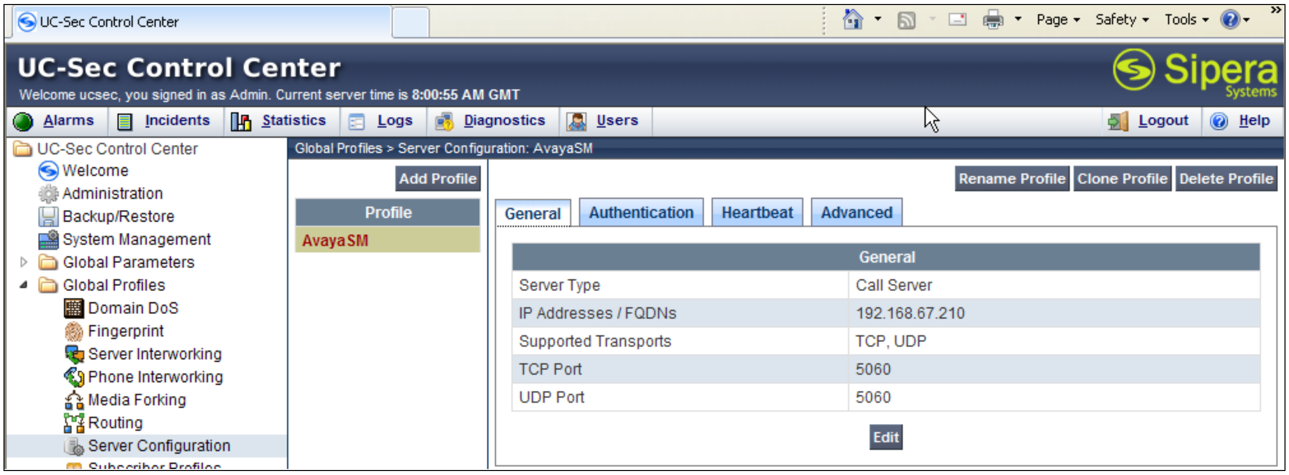
Outgoing Transport ○ TLS ○ TCP ● UDP

8.4.5. Server Configuration – To Avaya Aura® Session Manager

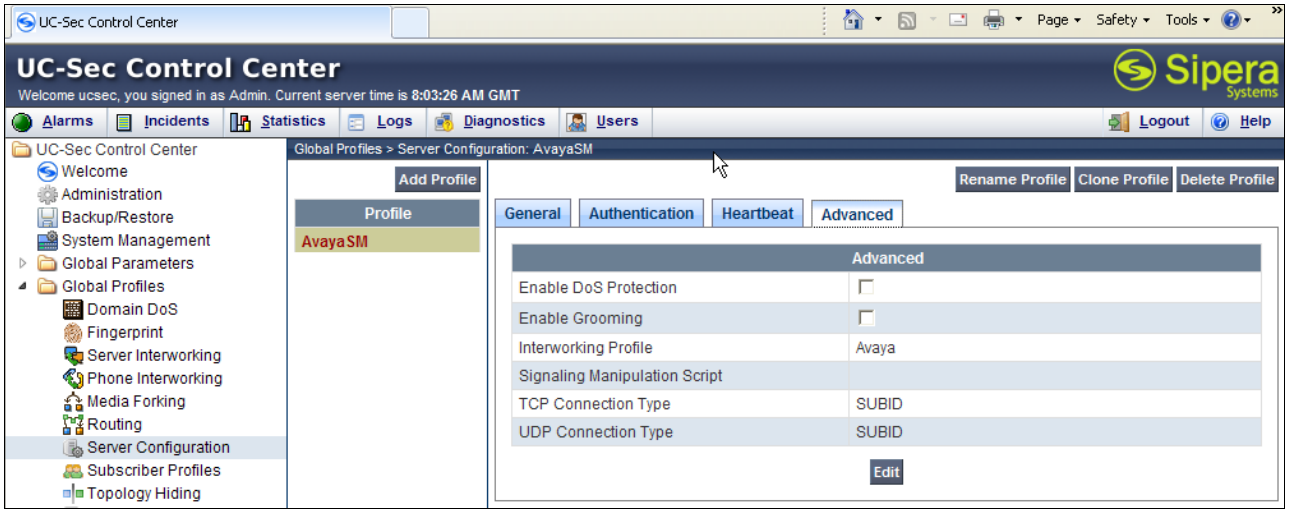
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters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

1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Server Configuration**
3. Select **Add Profile** and the **Profile Name** window will open (not shown).Enter a Profile Name (e.g., **Avaya SM**) and select **Next**.
4. The **Add Server Configuration Profile - General** window will Open (not shown).
   a. Select Server Type**: Call Server**
   b. **IP Address: 192.168.67.210** (Session Manager IP Address)
   c. **Supported Transports**: Check **UDP** and **TCP**
   d. **TCP Port: 5060**
   e. **UDP Port: 5060**
   f. Select **Next**.
5. The **Add Server Configuration Profile - Authentication** window will open (not shown).
   a. Select **Next** to accept default values.
6. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
   a. Select **Next** to accept default values.
7. The **Add Server Configuration Profile - Advanced** window will open (not shown).
   a. Select **Avaya** for Interworking Profile
   b. Select **Finish**

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



General	
Server Type	Call Server
IP Addresses / FQDNs	192.168.67.210
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060



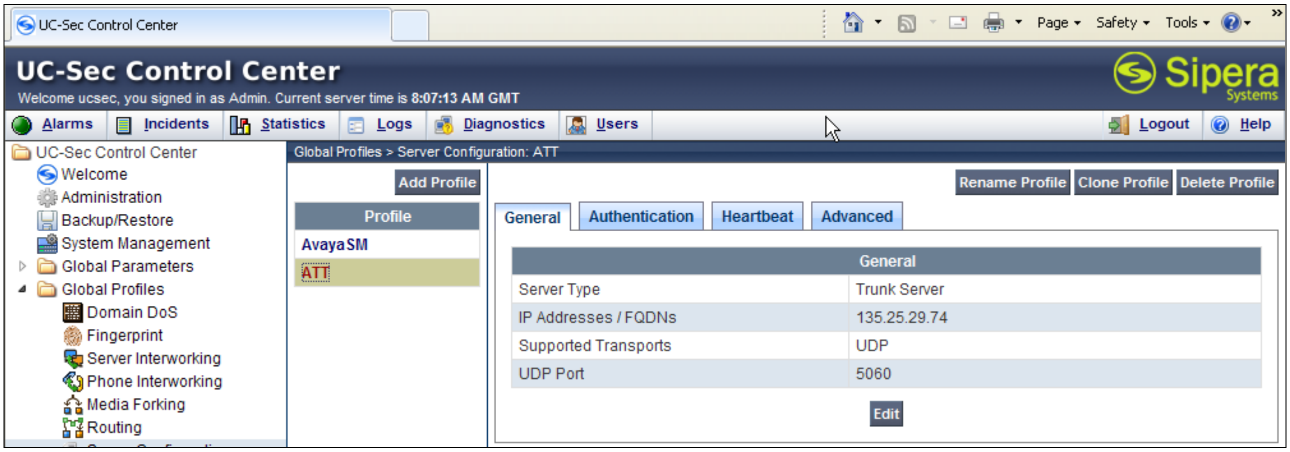
Advanced	
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Avaya
Signaling Manipulation Script	
TCP Connection Type	SUBID
UDP Connection Type	SUBID

8.4.6. Server Configuration – To AT&T

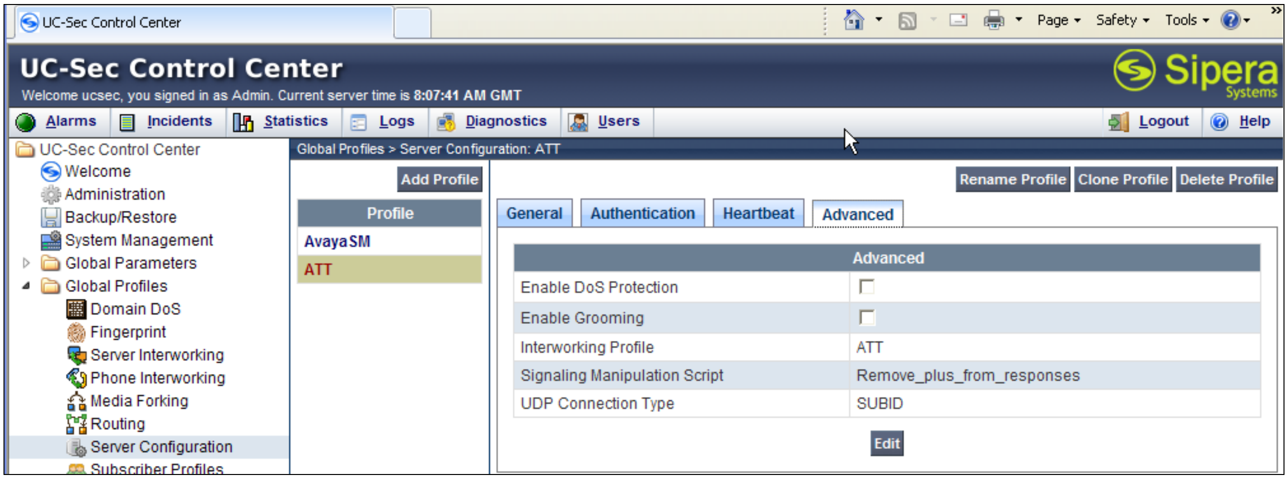
Repeat the steps in **Section 8.4.5** to create a Server Configuration for the connection to AT&T.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Server Configuration**
3. Select **Add Profile** and the **Profile Name** window will open (not shown).Enter a Profile Name (e.g., **ATT**) and select **Next**.
4. The **Add Server Configuration Profile - General** window will Open (not shown).
   a. Select Server Type**: Trunk Server**
   b. **IP Address: 135.25.29.74** (AT&T Border Element IP Address)
   c. **Supported Transports**: Check **UDP**
   d. **UDP Port: 5060**
   e. Select **Next**.
5. The **Add Server Configuration Profile - Authentication** window will open (not shown).
   a. Select **Next** to accept default values.
6. The **Add Server Configuration Profile - Heartbeat** window will open (not shown).
   a. Select **Next** to accept default values.
7. The **Add Server Configuration Profile - Advanced** window will open (not shown).
   a. Select **Avaya** for Interworking Profile
   b. In the Signaling Manipulation Script field select the script defined in Section **8.4.9** (e.g., **Remove_Plus_from_Responses**).
   c. Select **Finish.**

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



General	
Server Type	Trunk Server
IP Addresses / FQDNs	135.25.29.74
Supported Transports	UDP
UDP Port	5060



Advanced	
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	ATT
Signaling Manipulation Script	Remove_plus_from_responses
UDP Connection Type	SUBID

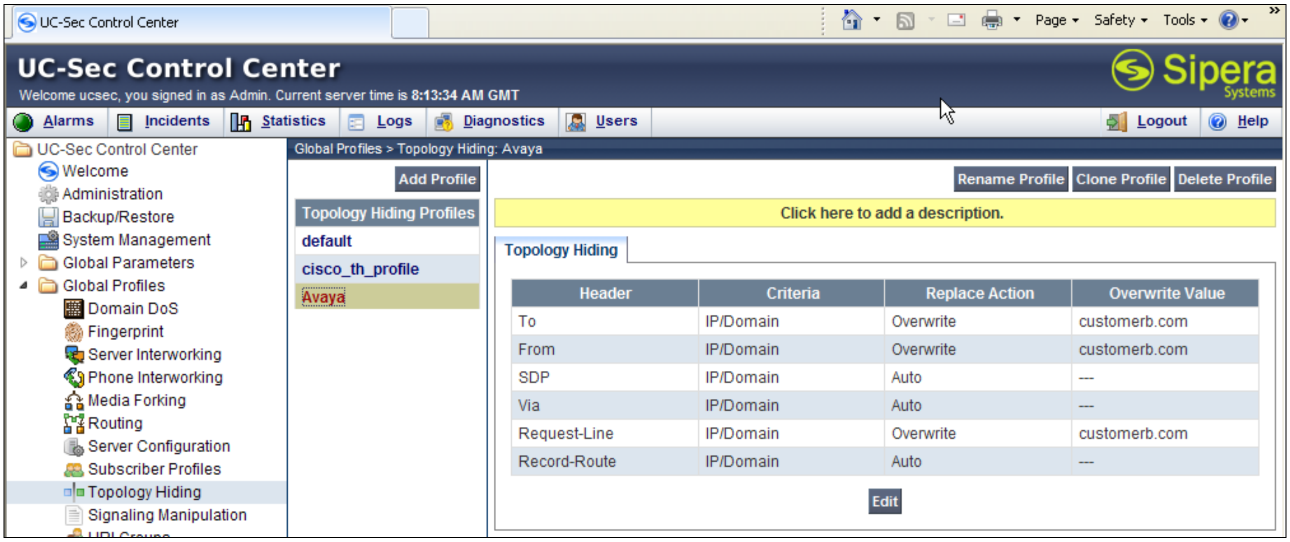
8.4.7. Topology Hiding – Avaya Side

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

1. Select **Global Profiles** from the menu on the left-hand side
2. Select **Topology Hiding**
3. Click **default** profile and select **Clone Profile**
4. Enter Profile Name: (e.g., **Avaya**)
5. For the Header **To,**
   a. In the **Criteria** column select **IP/Domain**
   b. In the **Replace Action** column select**: Overwrite**
   c. In the **Overwrite Value** column**: customerb.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**: customerb.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**: customerb.com**

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

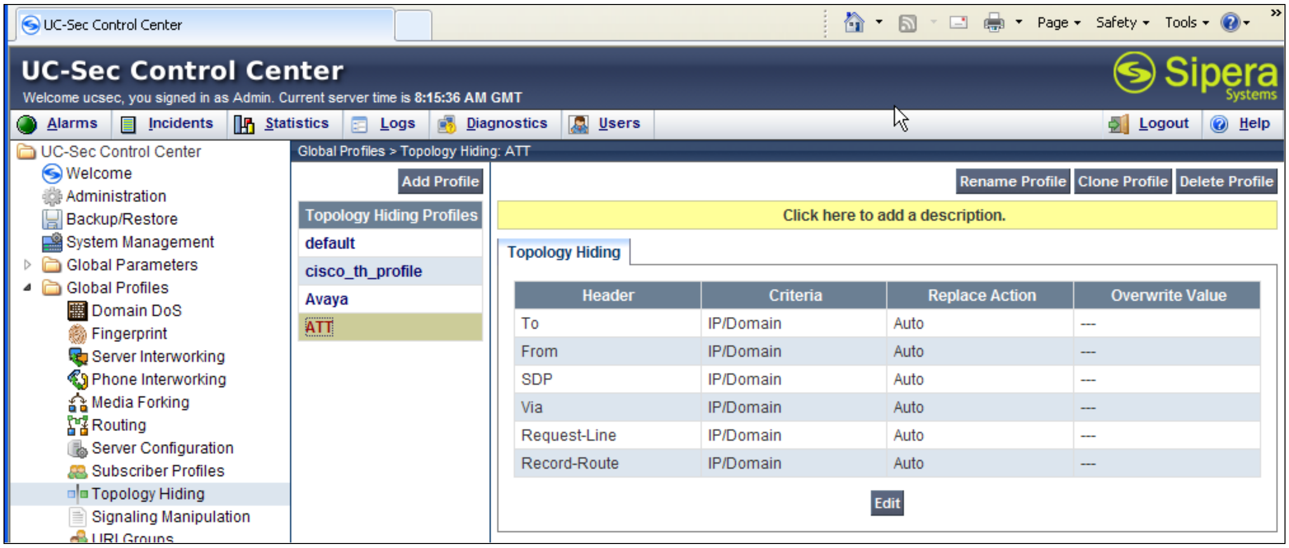


Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	customerb.com
From	IP/Domain	Overwrite	customerb.com
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	customerb.com
Record-Route	IP/Domain	Auto	---

8.4.8. Topology Hiding – AT&T Side

Repeat the steps in **Section 8.4.7** 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**)
5. Leave all Replace Action to **"Auto"**
6. Click **Finish**

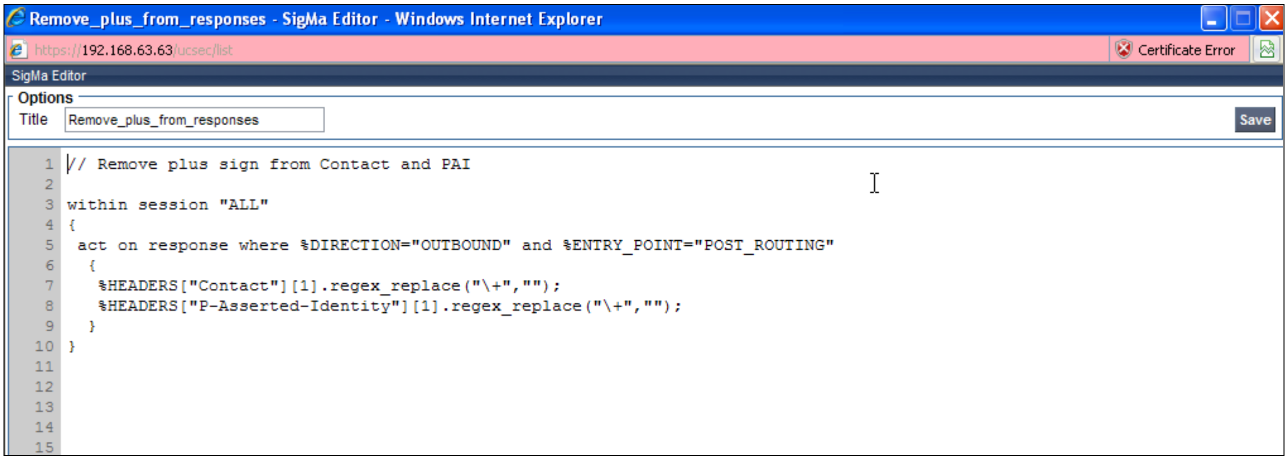


Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

8.4.9. Signaling Manipulation

Avaya Communication Manager will insert a plus sign (+) into calling number strings. These leading plus signs may cause issues to the AT&T IP Toll Free service. The Avaya SBCE may be used to remove the plus signs before they are passed to AT&T, by defining a SIP header manipulation script. Refer to [10] and [11] for information on the Avaya SBCE scripting language.

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

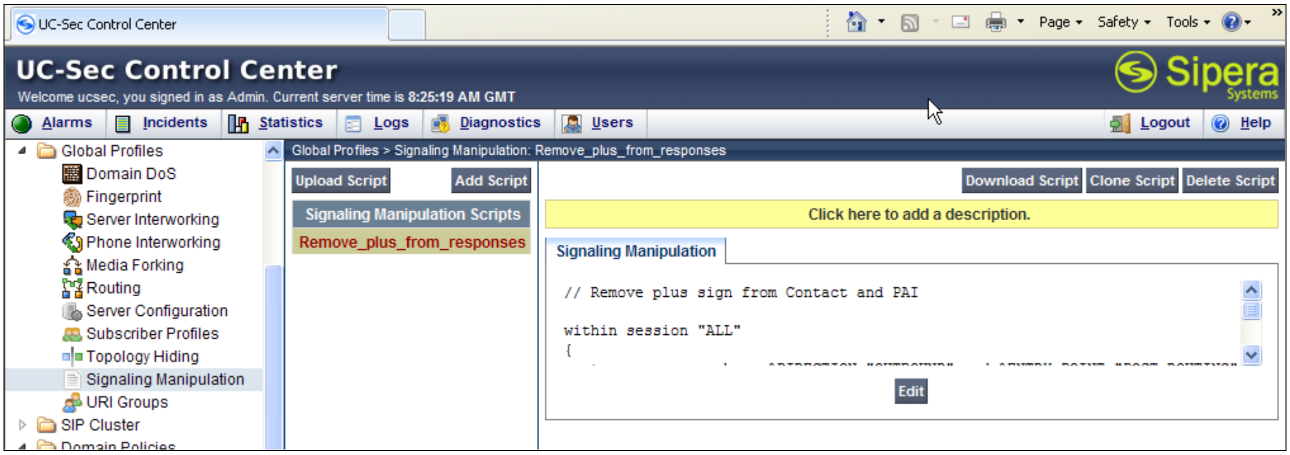

Remove_plus_from_responses - SigMa Editor - Windows Internet Explorer
https://192.168.63.63/ucsec/list
Certificate Error
SigMa Editor
Options
Save

Title: Remove_plus_from_responses

```
// Remove plus sign from Contact and PAI

within session "ALL"
{
 act on response where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
   %HEADERS["Contact"][1].regex_replace("\+","");
   %HEADERS["P-Asserted-Identity"][1].regex_replace("\+","");
  }
}
```

6. Click on **Save**. The script editor will test for any errors, and the editor window will close.
7. If changes are required, click on the **Edit** button.

Note -This script is specified in the **Server Configuration** defined in **Section 8.4.6**, **Step 7**.



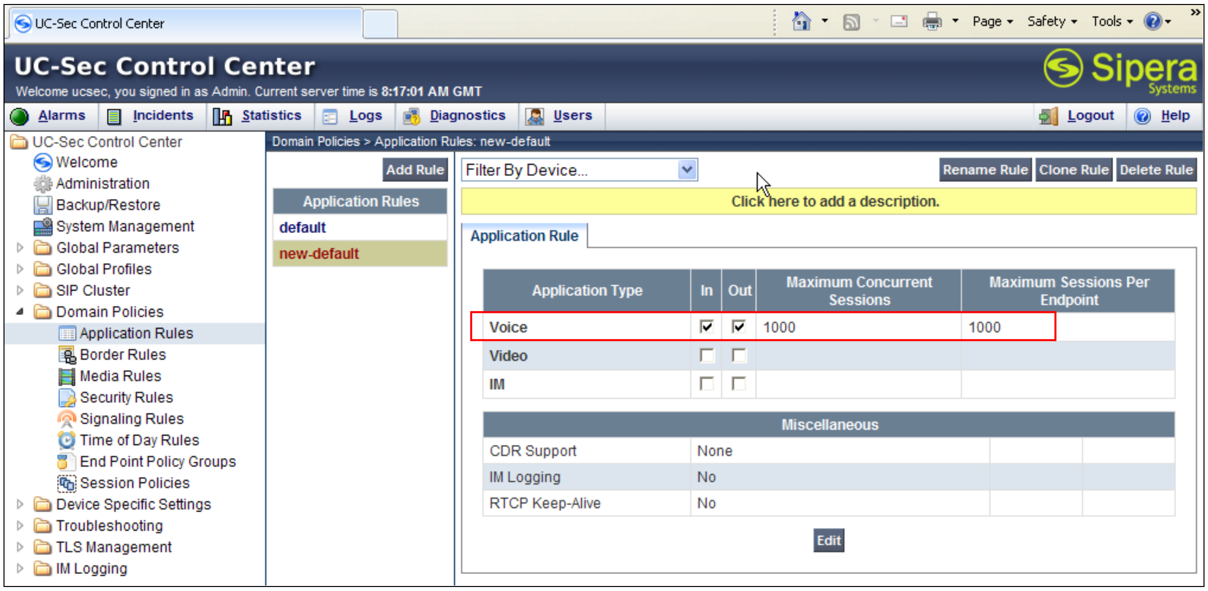
```
// Remove plus sign from Contact and PAI

within session "ALL"
{
```

8.5. 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. There are default policies available to use, or you can create a custom domain policy.

8.5.1. Application Rules

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Application Rules**
3. Select the **default** Rule
4. Select **Clone Rule** button
    a. Name**: new-default**
    b. Click **Finish**
5. Highlight the rule just created: **new-default**
    a. Click the **Edit** button
    b. In the **Voice** row:
        i. Change the **Maximum Concurrent Sessions** to **1000**
        ii. Change the **Maximum Sessions per Endpoint** to **1000**



Domain Policies > Application Rules: new-default

Click here to add a description.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	☑	☑	1000	1000
Video	□	□		
IM	□	□		

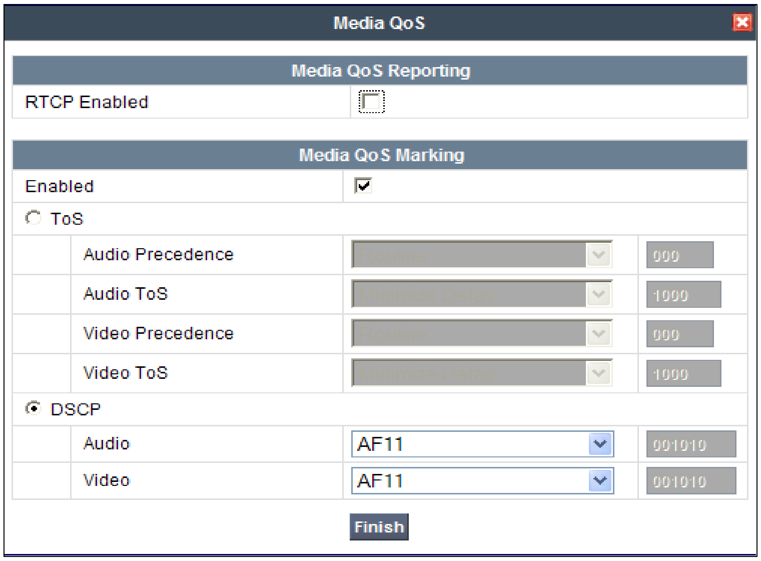
Miscellaneous	
CDR Support	None
IM Logging	No
RTCP Keep-Alive	No

8.5.2. Media Rules

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

1. Select **Domain Policies** from the menu on the left-hand side menu (not shown).
2. Select the **Media Rules** (not shown).
3. The Media Rules window will open (not shown). From the Media Rules menu, select the **default-low-med** rule

4. Select **Clone Rule** button
    a. Name**: default-low-med-QOS**
    b. Click **Finish**
5. Highlight the rule just created from the Media Rules menu: **default-low-med-QOS**
    a. Select the **Media QOS** tab (not shown).
    b. Click the **Edit** button and the **Media QOS** window will open.
    c. Check the **Media QOS Marking - Enabled**
    d. Select the **DSCP** box
    e. **Audio:** Select **AF11** from the drop-down
    f. **Video**: Select **AF11** from the drop-down
6. Click **Finish**

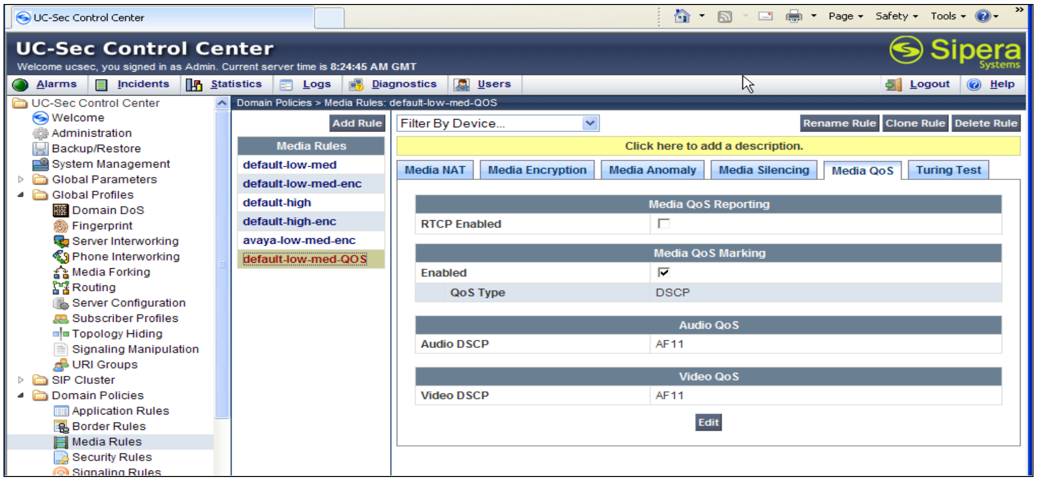


Media QoS

Media QoS Reporting		
RTCP Enabled	□	

Media QoS Marking		
Enabled	☑	
○ ToS		
Audio Precedence		000
Audio ToS		1000
Video Precedence		000
Video ToS		1000
● DSCP		
Audio	AF11	001010
Video	AF11	001010

The screen shot below shows the completed **Media Rules** window.



Welcome ucsec, you signed in as Admin. Current server time is 8:24:45 AM GMT

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

Media Rules
- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- default-low-med-QOS

Media QoS Reporting	
RTCP Enabled	□

Media QoS Marking	
Enabled	☑
QoS Type	DSCP

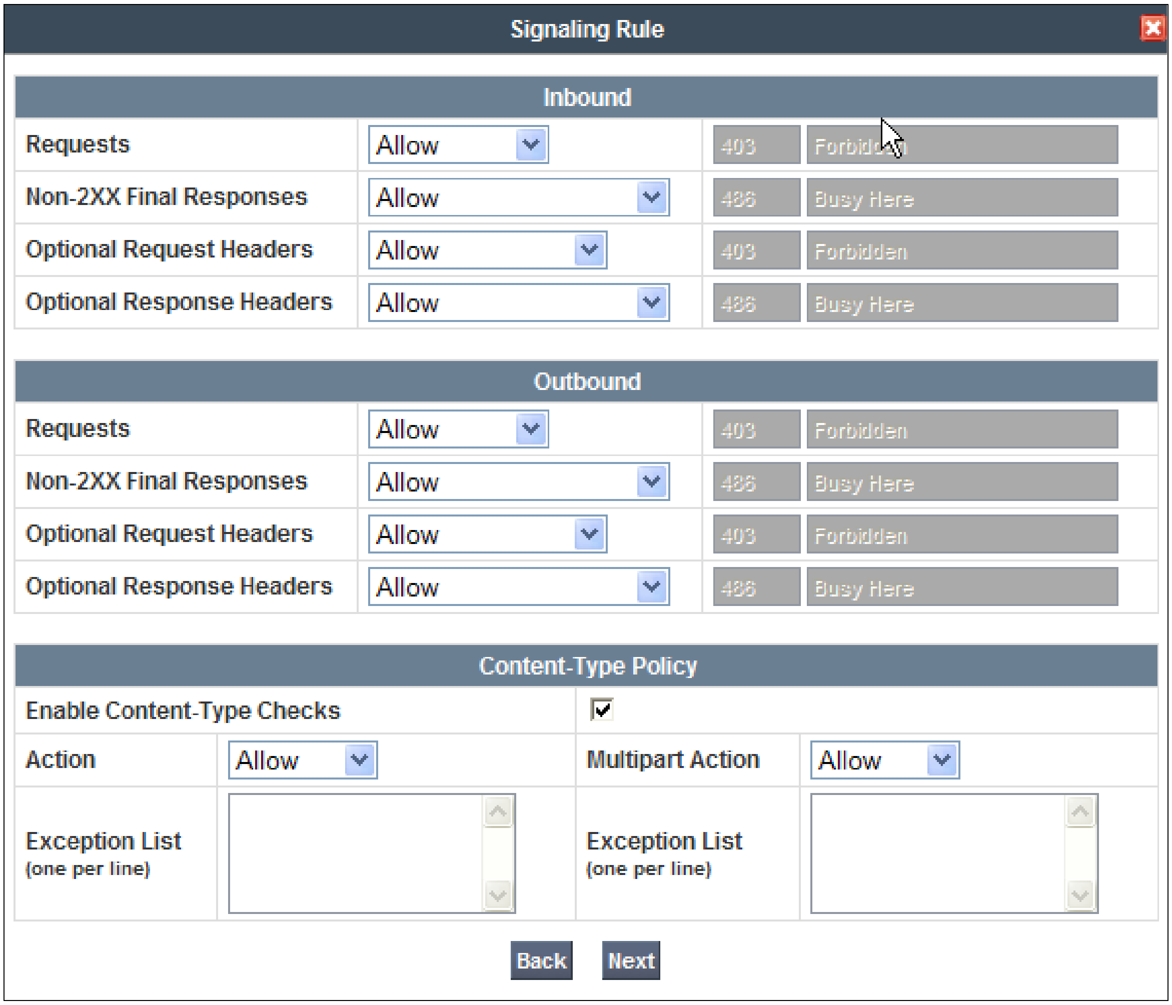
Audio QoS	
Audio DSCP	AF11

Video QoS	
Video DSCP	AF11

8.5.3. Signaling Rules

This signaling rule is being created to strip the P-location header information from the SIP messages before sending it on to the service provider (the P-Location header may contain network information from the "inside" network).

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Signaling Rules**
3. Select **Add Rule**
    a) Name**: HideP-Loc**
    b) Click **Next**
4. On the **Signaling Rule** page
    a) Click **Next** to accept default values.



Signaling Rule

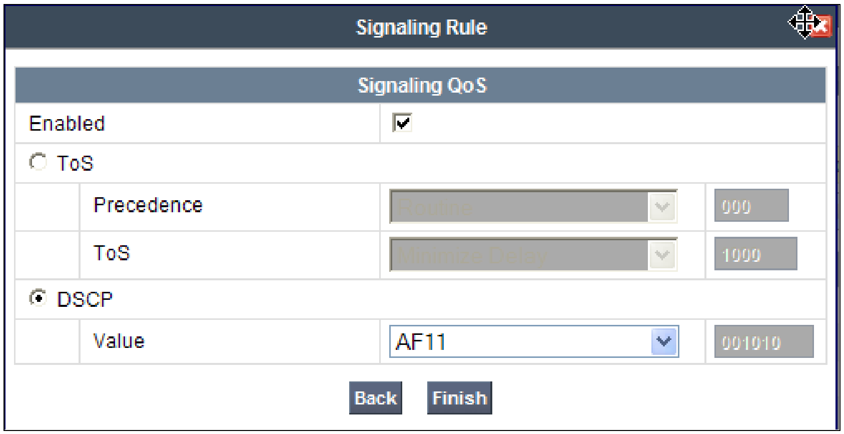
Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Content-Type Policy			
Enable Content-Type Checks	☑		
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	

5. On the **Signaling QOS** page
    a. Select **DSCP**

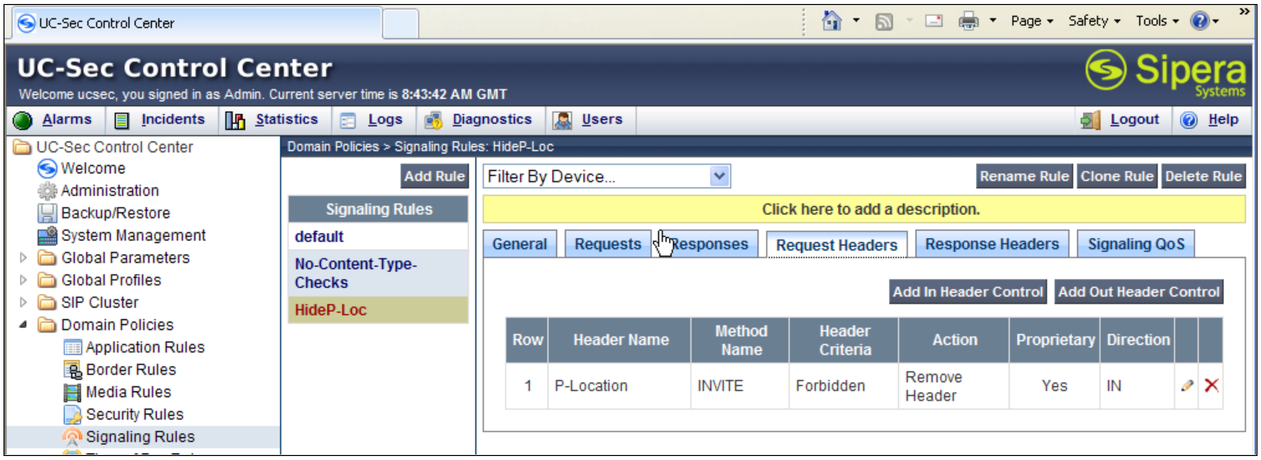
b. Select **AF11** from the drop-down box
c. Select **Finish**



Signaling Rule

Signaling QoS		
Enabled	☑	
○ ToS		
Precedence	Routine	000
ToS	Minimize Delay	1000
● DSCP		
Value	AF11	001010

6. Select the **Request Headers** Tab
   a) Select **Add in Header Control**
   b) Check the **Proprietary Request Header** box
   c) **Header Name: P-Location**
   d) **Method Name: INVITE**
   e) **Header Criteria: Forbidden**
   f) **Action: Remove Header**
   g) Click **Finish** (not shown)



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 8:43:42 AM GMT

Domain Policies > Signaling Rules: HideP-Loc

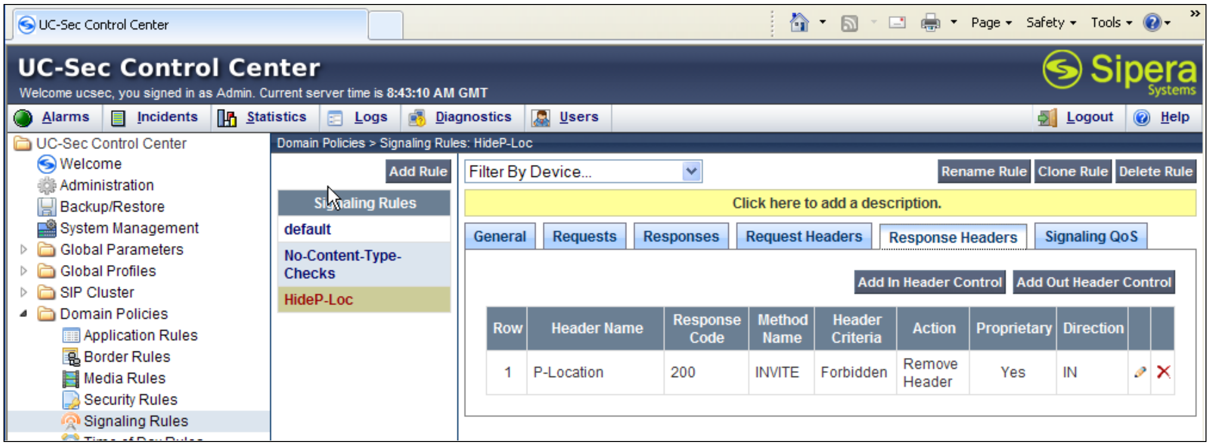
Click here to add a description.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	P-Location	INVITE	Forbidden	Remove Header	Yes	IN

7. Select the **Response Headers** Tab
   a) Select **Add in Header Control**
   b) Check the **Proprietary Request Header** box
   c) **Header Name: P-Location**
   d) **Response Code: 200**
   e) **Method Name: INVITE**
   f) **Header Criteria: Forbidden**

    g) **Action: Remove Header**

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



Welcome ucsec, you signed in as Admin. Current server time is 8:43:10 AM GMT

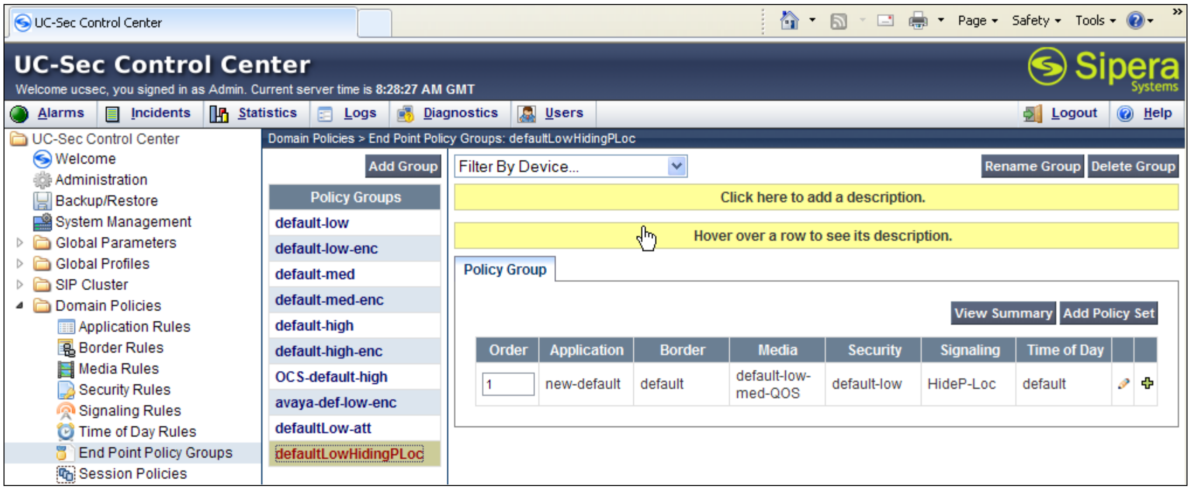
Domain Policies > Signaling Rules: HideP-Loc

Click here to add a description.

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	P-Location	200	INVITE	Forbidden	Remove Header	Yes	IN	✎	✕

8.5.4. 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: defaultLowHidingPLoc**
    b) **Application Rule: new-default**
    c) **Border Rule: default**
    d) **Media Rule: default-low-med-QOS**
    e) **Security Rule: default-low**
    f) **Signaling Rule: HideP-Loc**
    g) **Time of Day: default**
4. Select **Finish** (not shown)



Welcome ucsec, you signed in as Admin. Current server time is 8:28:27 AM GMT

Domain Policies > End Point Policy Groups: defaultLowHidingPLoc

Click here to add a description.

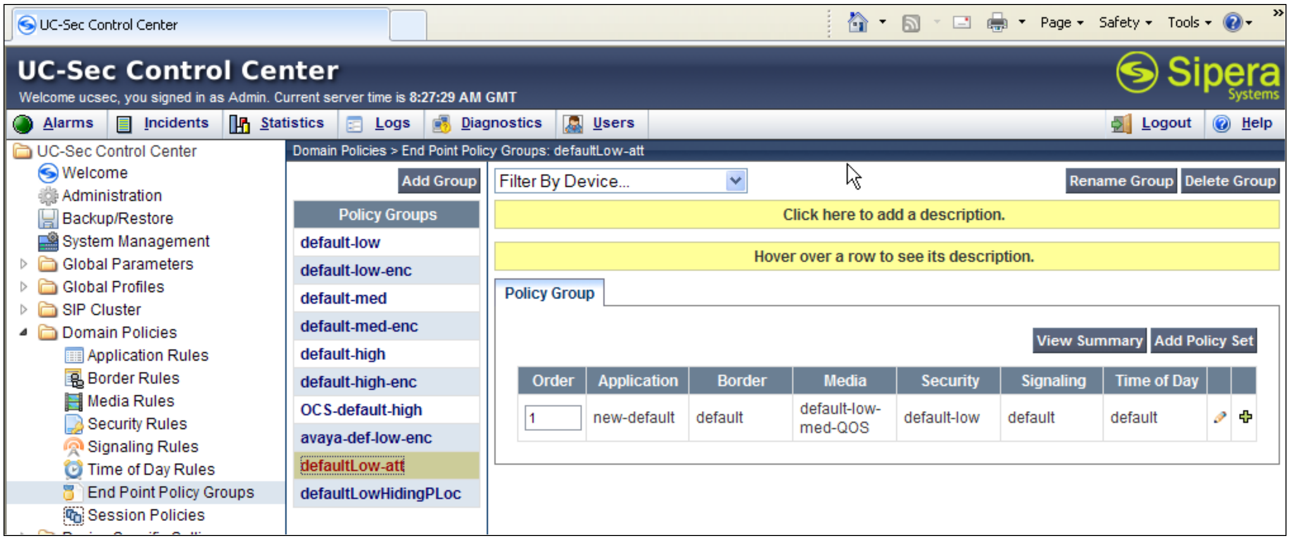
Hover over a row to see its description.

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	new-default	default	default-low-med-QOS	default-low	HideP-Loc	default	✎	✚

8.5.5. Endpoint Policy Groups – AT&T

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

2. Select **End Point Policy Groups**
3. Select **Add Group**
   a) **Name: defaultLow-att**
   b) **Application Rule: new-default**
   c) **Border Rule: default**
   d) **Media Rule: default-low-med-QOS**
   e) **Security Rule: default-low**
   f) **Signaling Rule: default**
   g) **Time of Day: default**
4. **Select Finish** (not shown)



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 8:27:29 AM GMT

Domain Policies > End Point Policy Groups: defaultLow-att

Click here to add a description.

Hover over a row to see its description.

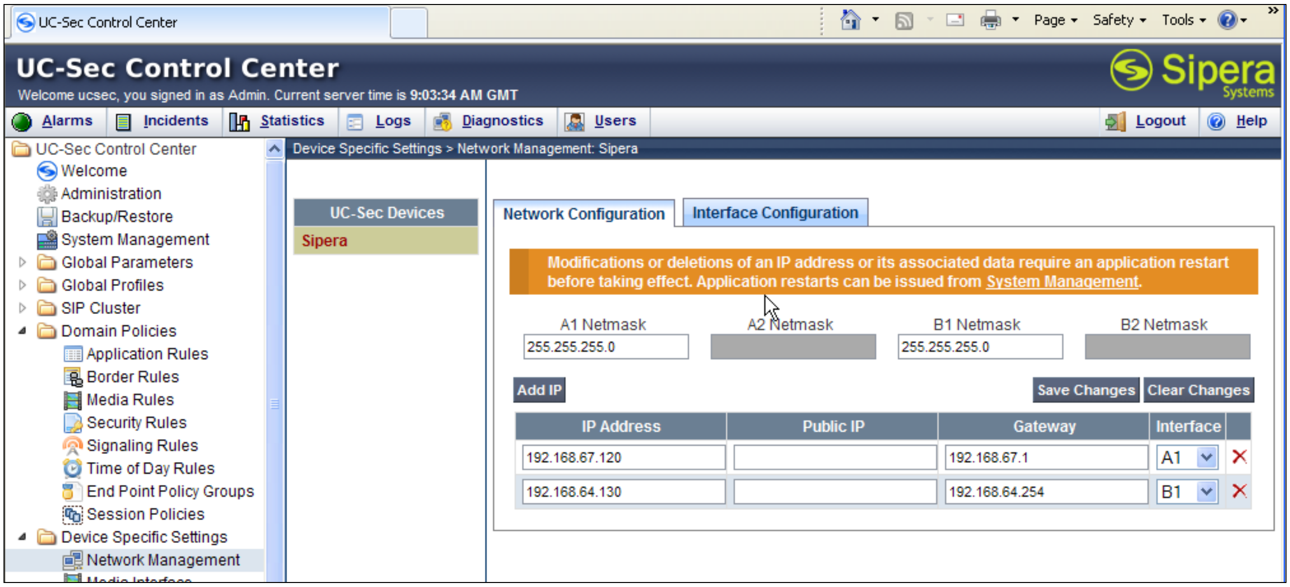
Order	Application	Border	Media	Security	Signaling	Time of Day
1	new-default	default	default-low-med-QOS	default-low	default	default

8.6. Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view system information, and manage various device-specific network parameters. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows, and Network Management.

8.6.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**
   a) The network interfaces were provisioned in **Section 8.3**. However if these values need to be modified, do so via this tab.

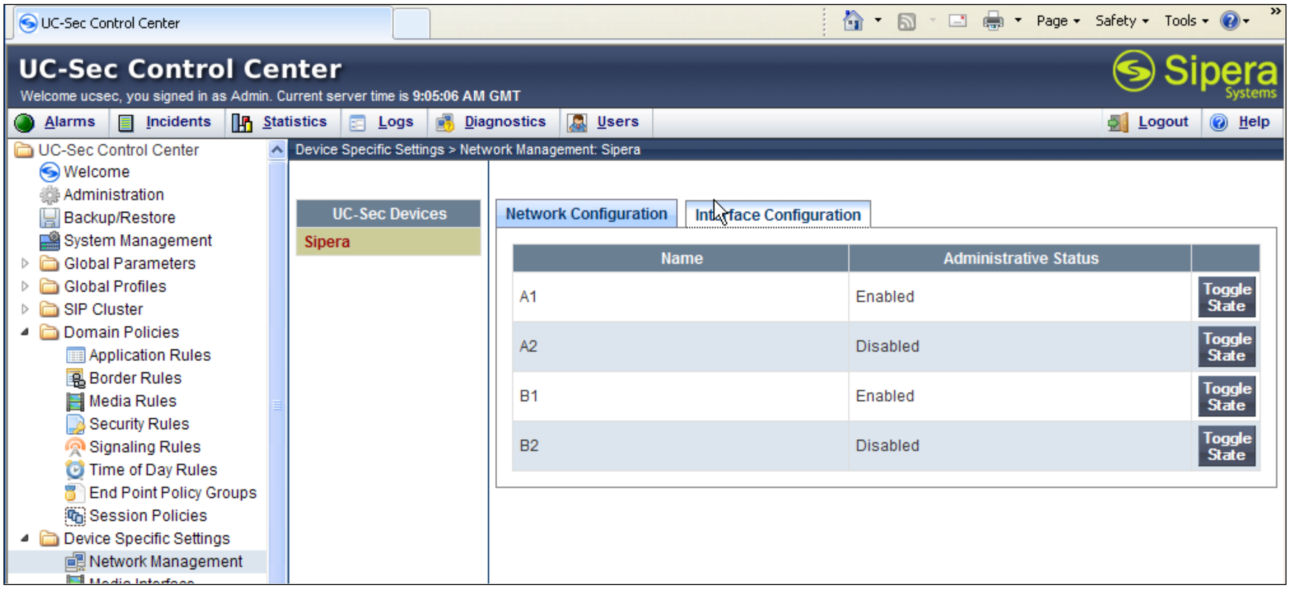


Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.0	

IP Address	Public IP	Gateway	Interface
192.168.67.120		192.168.67.1	A1
192.168.64.130		192.168.64.254	B1

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.



Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

8.6.2. Media Interfaces

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

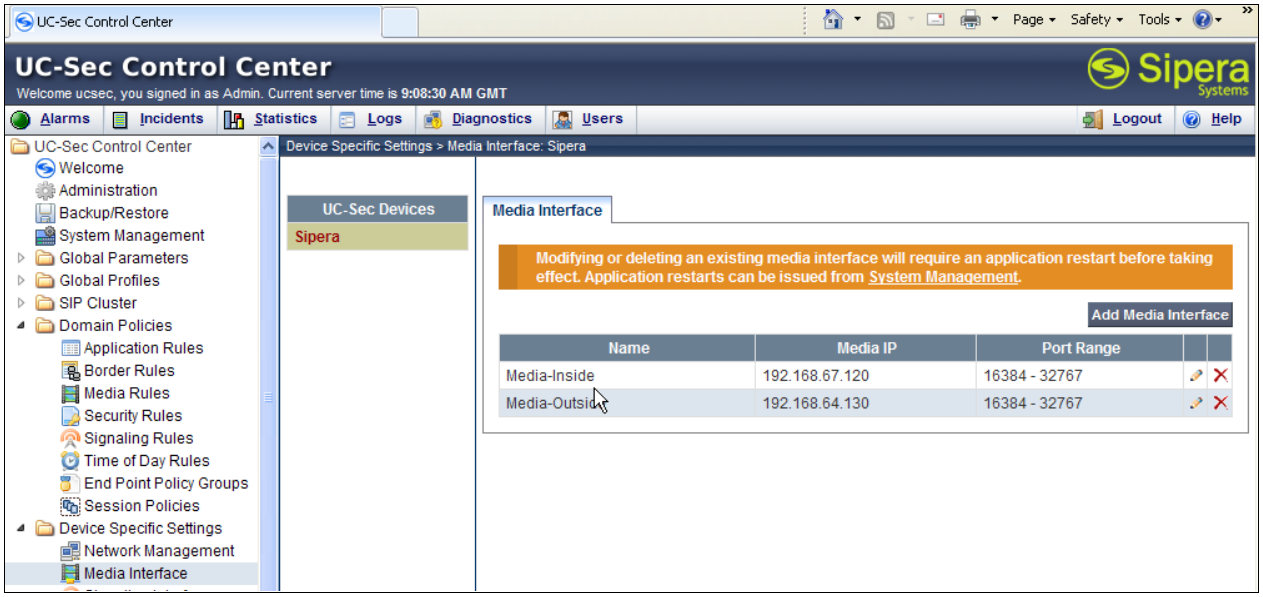
1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Media Interface**
3. Select **Add Media Interface**

a) **Name: Media-Inside**
b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Session Manager)
c) **Port Range: 16384 - 32767**

4. Click **Finish** (not shown)
5. Select **Add Media Interface**

a) **Name: Media-Outside**
b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
c) **Port Range: 16384 - 32767**

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



Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range
Media-Inside	192.168.67.120	16384 - 32767
Media-Outside	192.168.64.130	16384 - 32767

8.6.3. Signaling Interface

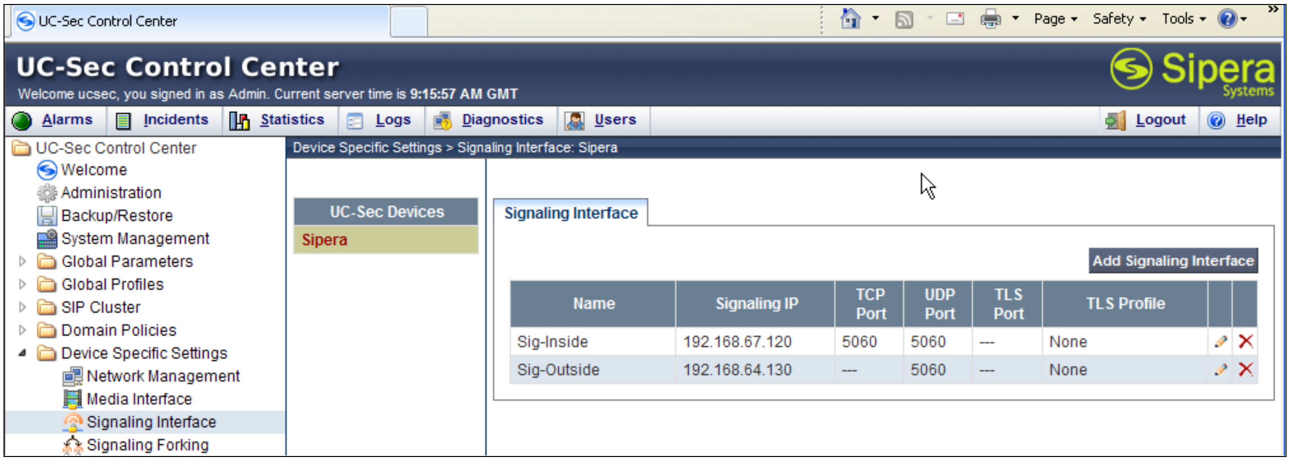
1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Signaling Interface**
3. Select **Add Signaling Interface**

a) **Name: Sig-Inside**
b) **Media IP: 192.168.67.120** (Avaya SBCE internal address toward Session Manager)
c) **TCP Port: 5060**
d) **UDP Port: 5060**

4. Click **Finish**
5. Select **Add Media Interface**

a) **Name: Sig-Outside**
b) **Media IP: 192.168.64.130** (Avaya SBCE external address toward AT&T)
c) **UDP Port: 5060**

6. Click **Finish**



Welcome ucsec, you signed in as Admin. Current server time is 9:15:57 AM GMT

Device Specific Settings > Signaling Interface: Sipera

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
Sig-Inside	192.168.67.120	5060	5060	---	None
Sig-Outside	192.168.64.130	---	5060	---	None

8.6.4. Endpoint Flows – To Session Manager

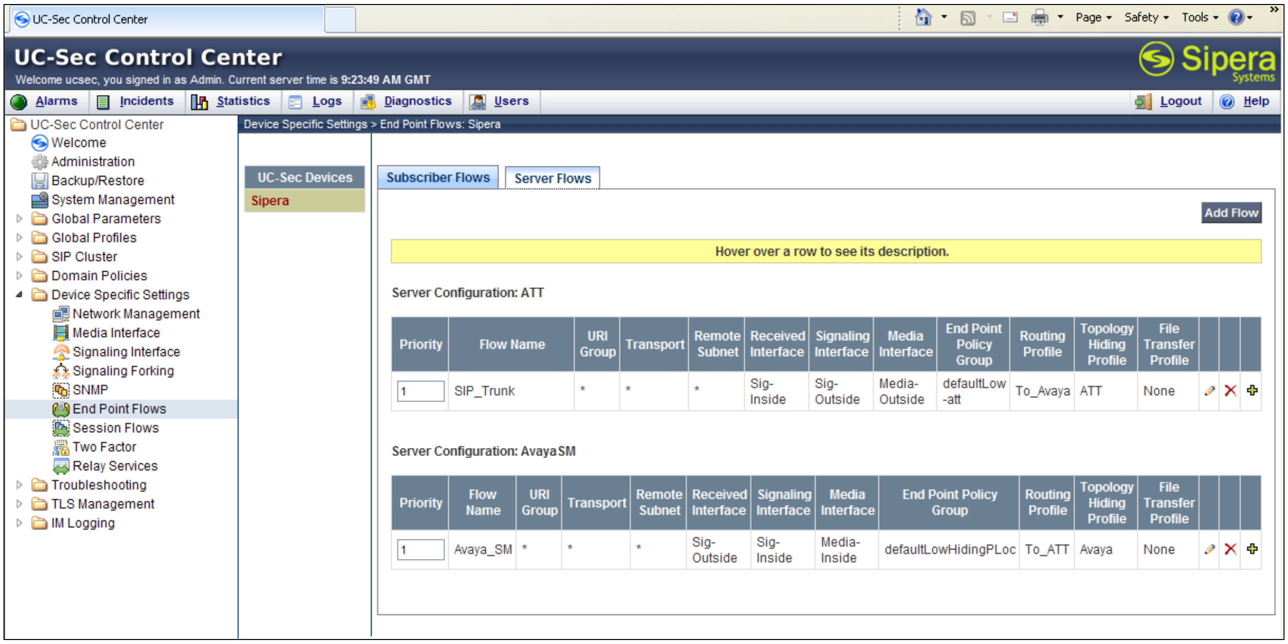
1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** tab
4. Select **Add Flow**
    a) **Name: Avaya_SM**
    b) **Server Configuration**: **Avaya_SM**
    c) **URI Group: ***
    d) **Transport: ***
    e) **Remote Subnet: ***
    f) **Received Interface**: **Sig-Outside**
    g) **Signaling Interface: Sig-Inside**
    h) **Media Interface**: **Media-Inside**
    i) **End Point Policy Group: defaultLowHidingPLoc**
    j) **Routing Profile: To_ATT**
    k) **Topology Hiding Profile: Avaya**
    l) **File Transfer Profile: None**
5. Click **Finish** (not shown)

8.6.5. Endpoint Flows – To AT&T

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** tab
4. Select **Add Flow**
    a) **Name: SIP Trunk**
    b) **Server Configuration: SIP Trunk**
    c) **URI Group: ***
    d) **Transport: ***
    e) **Remote Subnet: ***
    f) **Received Interface: Sig-Inside**
    g) **Signaling Interface: Sig-Outside**

h) **Media Interface: Media-Outside**
i) **End Point Policy Group**: **defaultLow-att**
j) **Routing Profile: To_Avaya**
k) **Topology Hiding Profile: ATT**
l) **File Transfer Profile: None**

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



Server Configuration: ATT

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	SIP_Trunk	*	*	*	Sig-Inside	Sig-Outside	Media-Outside	defaultLow-att	To_Avaya	ATT	None	✎	✕	✚

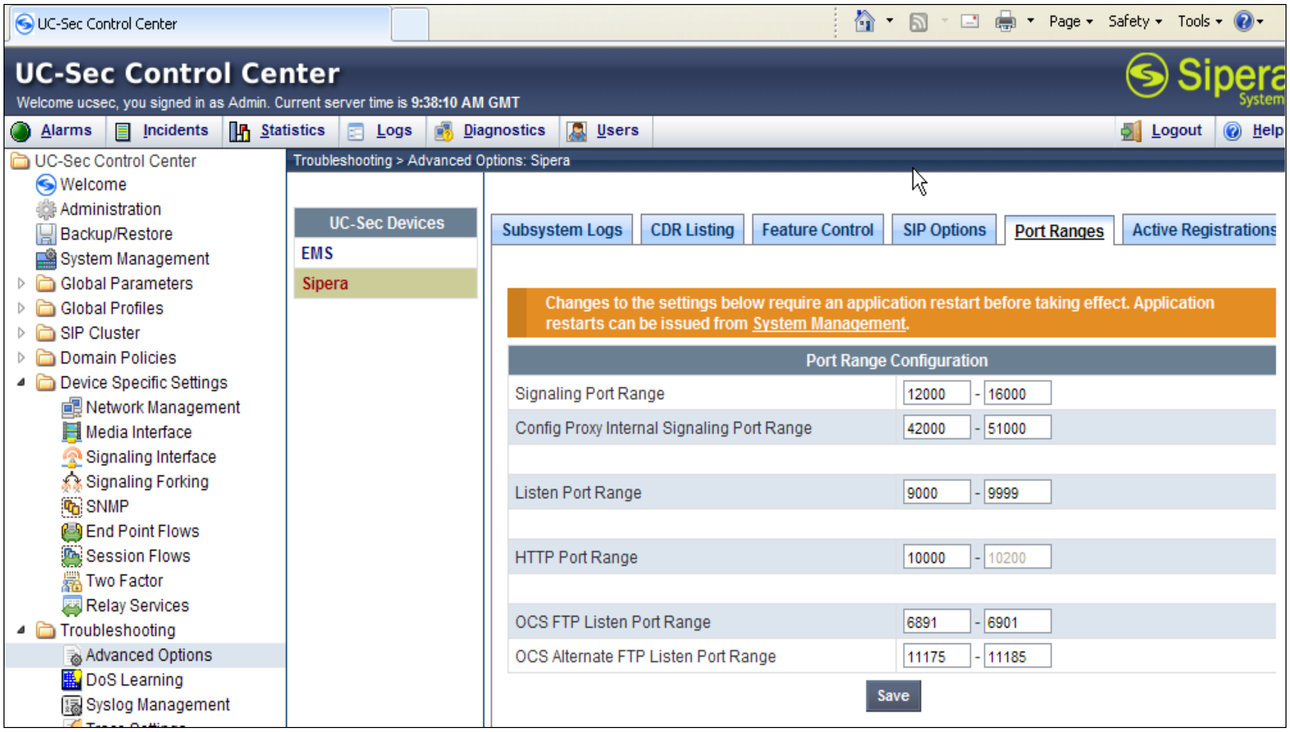
Server Configuration: AvayaSM

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Avaya_SM	*	*	*	Sig-Outside	Sig-Inside	Media-Inside	defaultLowHidingPLoc	To_ATT	Avaya	None	✎	✕	✚

8.7. Troubleshooting Port Ranges

The default port range in this section needs to be changed to exclude the AT&T RTP port range of 16384 – 32767 (**Section 8.6.2**).

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**



Welcome ucsec, you signed in as Admin. Current server time is 9:38:10 AM GMT

Troubleshooting > Advanced Options: Sipera

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

9. Verification Steps

The following steps may be used to verify the configuration:

9.1. General

1. Place an inbound call, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Place an inbound call to an agent or telephone, but do not answer the call. Verify that the call covers to Avaya Aura® Messaging voicemail. Retrieve the message from Avaya Aura® Messaging.

9.2. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See [5], [6] and [7] for more information.

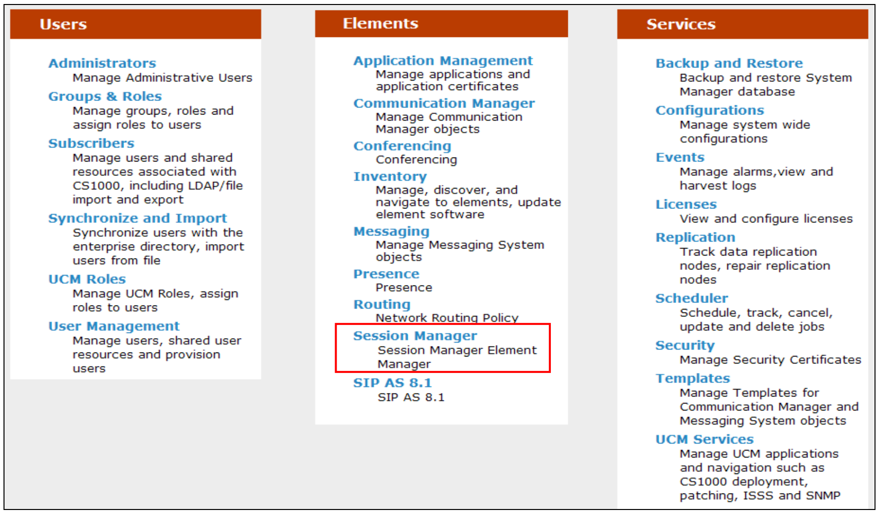
- From the Communication Manager console connection enter the command ***list trace tac xxx***, where ***xxx*** is a trunk access code defined for the SIP trunk to AT&T (e.g., 101). Note that Session Manager has previously converted the AT&T IP Toll Free number included in the Request URI to the Communication Manager extension 40002, before sending the INVITE to Communication Manager.

```
list trace tac 101                                    Page   1

                            LIST TRACE

time            data

10:50:35 TRACE STARTED 07/19/2010 CM Release String cold-00.0.345.0-18246
10:50:49 SIP<INVITE sip:40002@customerb.com:5060;transport=tcp S
10:50:49 SIP<IP/2.0
10:50:49     active trunk-group 1 member 1  cid 0x270
10:50:49 SIP>SIP/2.0 183 Session Progress
10:50:49     dial 40002
10:50:49     ring station    40002 cid 0x270
10:50:49     G711MU ss:off ps:20
           rgn:1 [192.168.67.80]:17382
           rgn:1 [192.168.67.203]:16390
10:50:49     G729B ss:off ps:20
           rgn:2 [192.168.67.130]:16480
           rgn:1 [192.168.67.203]:16386
10:50:49     xoip OPTIONS: fax:T38 modem:off tty:US  uid:0x50001
           xoip ip: [192.168.67.203]:16386
10:50:50 SIP>SIP/2.0 200 OK
10:50:50     active station    40002 cid 0x270
10:50:50 SIP<ACK sip:7325554384@192.168.67.202;transport=tcp SIP
10:50:50 SIP</2.0
10:50:50 SIP>INVITE sip:7325552438@192.168.67.130:5060;transport
10:50:50 SIP>=tcp SIP/2.0
10:50:50 SIP<SIP/2.0 100 Trying
10:50:51 SIP<SIP/2.0 200 OK
10:50:51 SIP>ACK sip:7325552438@192.168.67.130:5060;transport=tc
10:50:51 SIP>p SIP/2.0
10:50:51     G729AB ss:off ps:20
           rgn:2 [192.168.67.130]:16480
           rgn:1 [192.168.67.80]:17382
10:50:51     G729B ss:off ps:20
           rgn:1 [192.168.67.80]:17382
           rgn:2 [192.168.67.130]:16480
10:50:54 SIP>BYE sip:7325552438@192.168.67.130:5060;transport=tc
10:50:54 SIP>p SIP/2.0
10:50:54     idle station    40002 cid 0x270
```

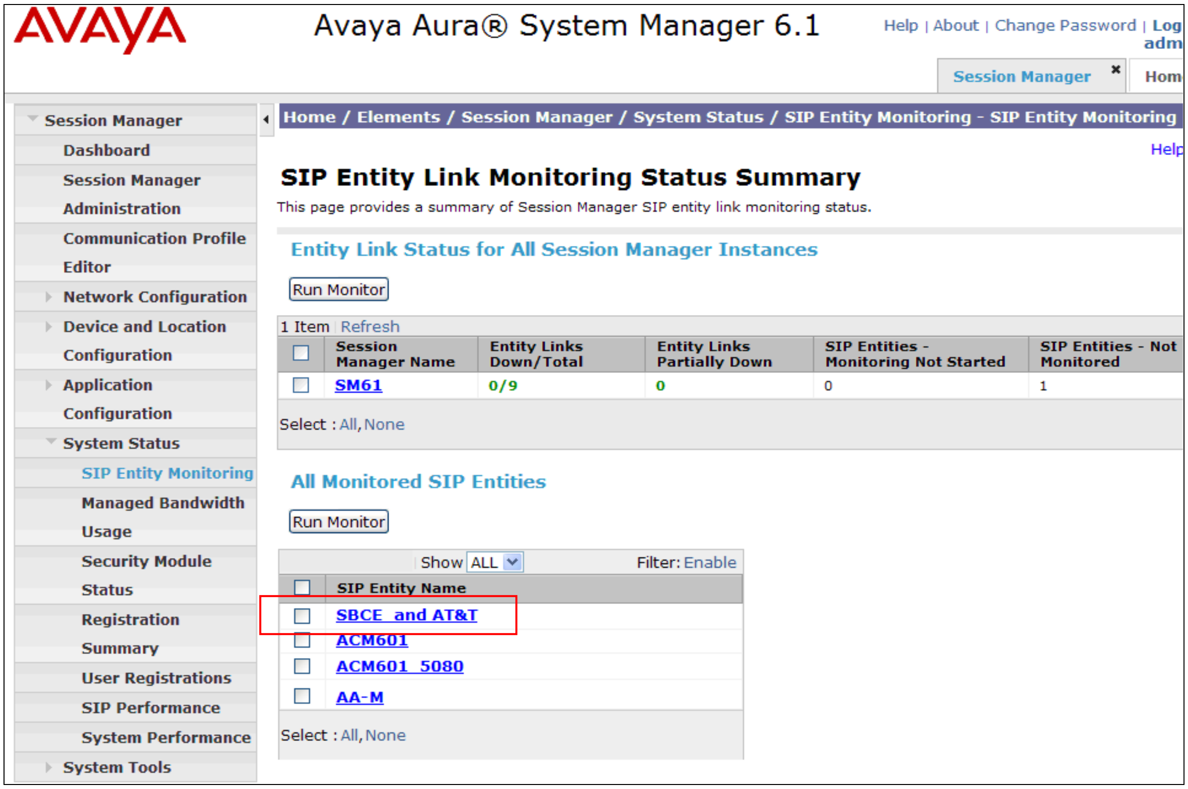
- Similar Communication Manager commands are, ***list trace station***, ***list trace vdn***, and ***list trace vector***. Other useful commands are ***status trunk*** and ***status station***.

9.3. Avaya Aura® Session Manager

Step 1 - Access the System Manager GUI, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Session Manager**.


Users
Administrators
Manage Administrative Users
Groups & Roles
Manage groups, roles and assign roles to users
Subscribers
Manage users and shared resources associated with CS1000, including LDAP/file import and export
Synchronize and Import
Synchronize users with the enterprise directory, import users from file
UCM Roles
Manage UCM Roles, assign roles to users
User Management
Manage users, shared user resources and provision users
Elements
Application Management
Manage applications and application certificates
Communication Manager
Manage Communication Manager objects
Conferencing
Conferencing
Inventory
Manage, discover, and navigate to elements, update element software
Messaging
Manage Messaging System objects
Presence
Presence
Routing
Network Routing Policy
Session Manager
Session Manager Element Manager
SIP AS 8.1
SIP AS 8.1
Services
Backup and Restore
Backup and restore System Manager database
Configurations
Manage system wide configurations
Events
Manage alarms,view and harvest logs
Licenses
View and configure licenses
Replication
Track data replication nodes, repair replication nodes
Scheduler
Schedule, track, cancel, update and delete jobs
Security
Manage Security Certificates
Templates
Manage Templates for Communication Manager and Messaging System objects
UCM Services
Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Step 2 - Expand **System Status** → **SIP Entity Monitoring**.



SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

1 Item | Refresh

□	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
□	SM61	0/9	0	0	1

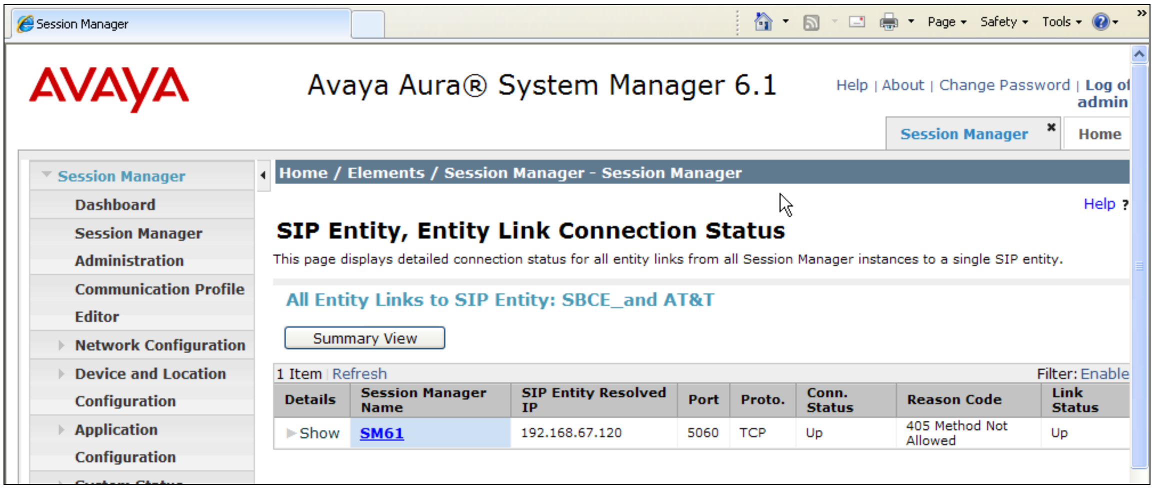
Select : All, None

All Monitored SIP Entities

□	SIP Entity Name
□	SBCE_and AT&T
□	ACM601
□	ACM601_5080
□	AA-M

Select : All, None

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



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: SBCE_and AT&T

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	SM61	192.168.67.120	5060	TCP	Up	405 Method Not Allowed	Up

9.3.1. Call Routing Test

The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. The following example shows an inbound call to Communication Manager from the AT&T IP Toll Free service. Note that the Request URI called number was 0000001050 and Session Manager converts this to Communication Manager extension 44003 before routing the call to Communication Manager

Step 1 – **Called Party URI** field = the information passed in the Request URI sent by the Avaya SBCE (e.g., **0000001050@customerb.com**)

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

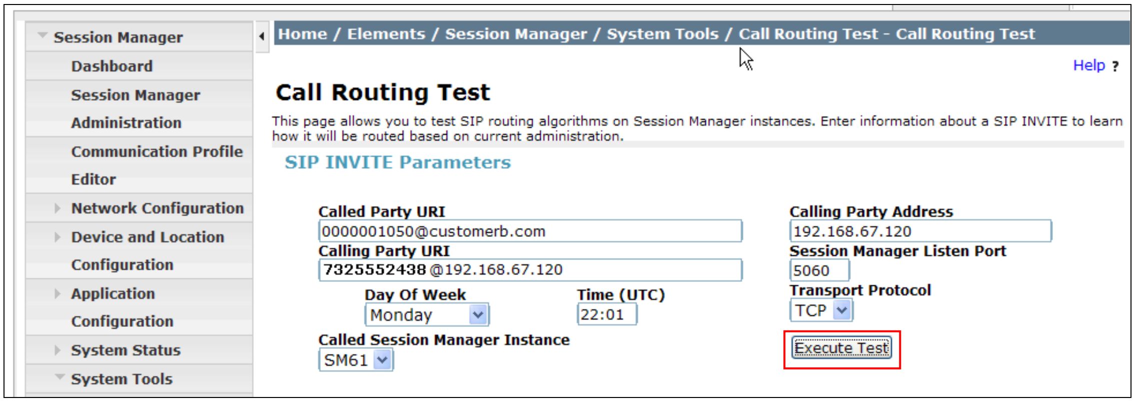
Step 3 – **Calling Party URI** field = The contents of the From header (e.g **7325552438@192.168.67.120**).

Step 4 – **Session Manager Listening Port** = **5060** and **Transport protocol** = **TCP** (see the note in **Section 5.5** regarding the use of TCP).

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

Step 6 – Verify that the **Called Session Manager** instance is correct (if multiple ones are defined).

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


Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Home / Elements / Session Manager / System Tools / Call Routing Test - Call Routing Test
Help ?

Call Routing Test

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

SIP INVITE Parameters

Called Party URI: 0000001050@customerb.com

Calling Party URI: 7325552438@192.168.67.120

Day Of Week: Monday

Time (UTC): 22:01

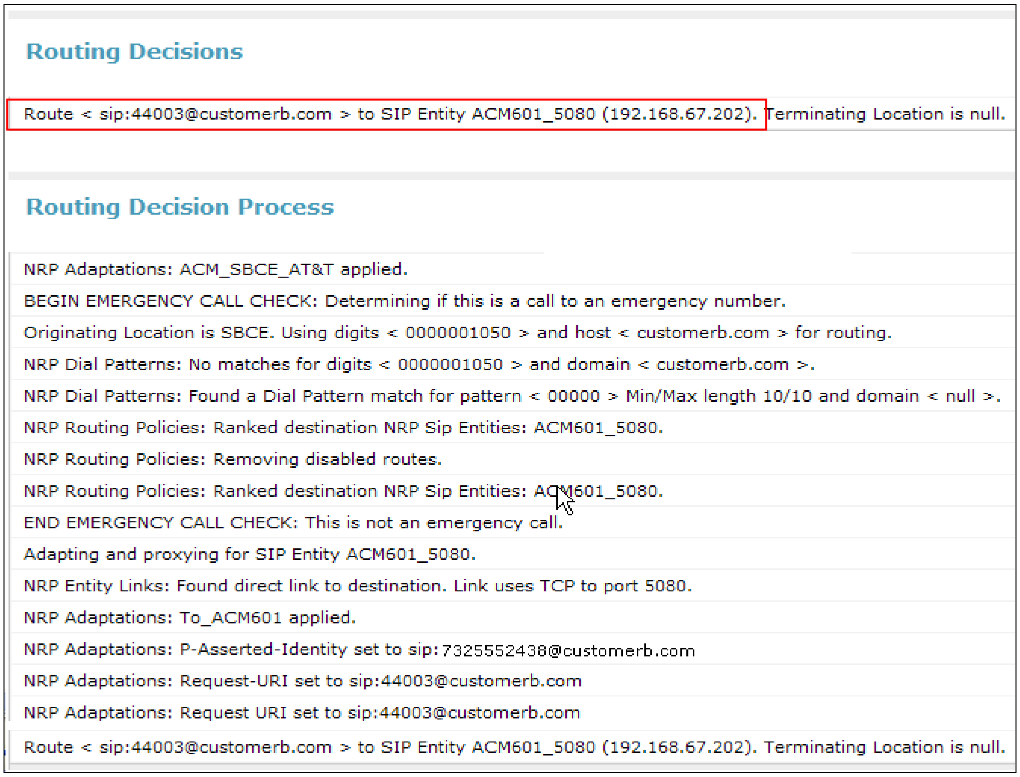
Called Session Manager Instance: SM61

Calling Party Address: 192.168.67.120

Session Manager Listen Port: 5060

Transport Protocol: TCP

The results of the test are shown below. The ultimate routing decision is displayed under the heading **Routing Decisions.** The example shows that a PSTN call to AT&T IP Toll Free service, delivering 0000001050 in the Request URI, is sent to Communication Manager extension **44003**. Further down, the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated).Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 5**.



Routing Decisions

```
Route < sip:44003@customerb.com > to SIP Entity ACM601_5080 (192.168.67.202). Terminating Location is null.
```

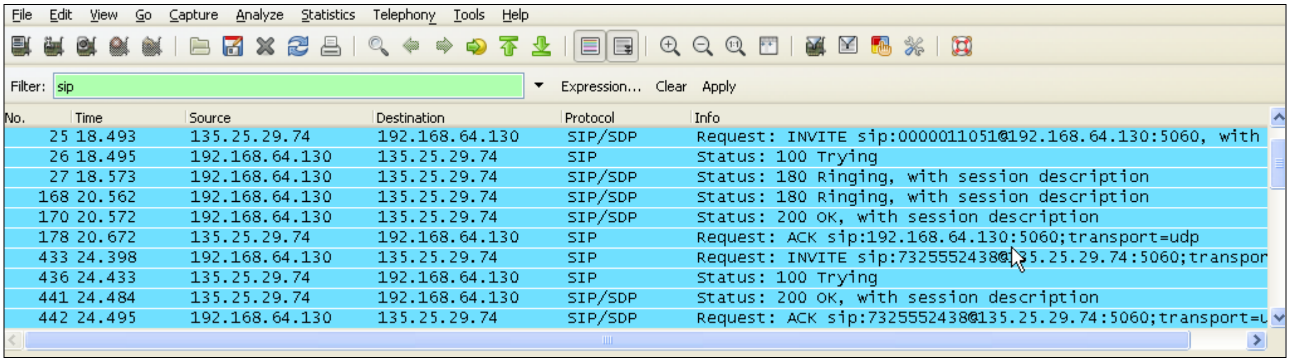
Routing Decision Process

```
NRP Adaptations: ACM_SBCE_AT&T applied.
BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.
Originating Location is SBCE. Using digits < 0000001050 > and host < customerb.com > for routing.
NRP Dial Patterns: No matches for digits < 0000001050 > and domain < customerb.com >.
NRP Dial Patterns: Found a Dial Pattern match for pattern < 00000 > Min/Max length 10/10 and domain < null >.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACM601_5080.
NRP Routing Policies: Removing disabled routes.
NRP Routing Policies: Ranked destination NRP Sip Entities: ACM601_5080.
END EMERGENCY CALL CHECK: This is not an emergency call.
Adapting and proxying for SIP Entity ACM601_5080.
NRP Entity Links: Found direct link to destination. Link uses TCP to port 5080.
NRP Adaptations: To_ACM601 applied.
NRP Adaptations: P-Asserted-Identity set to sip:7325552438@customerb.com
NRP Adaptations: Request-URI set to sip:44003@customerb.com
NRP Adaptations: Request URI set to sip:44003@customerb.com
Route < sip:44003@customerb.com > to SIP Entity ACM601_5080 (192.168.67.202). Terminating Location is null.
```

9.4. 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.

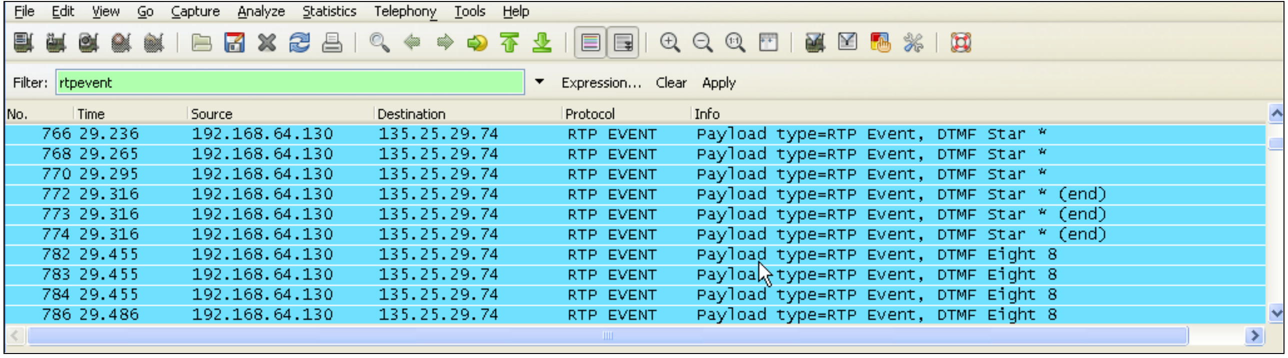
The following are examples of calls filtering on the SIP protocol.


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

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;transpor
 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
```

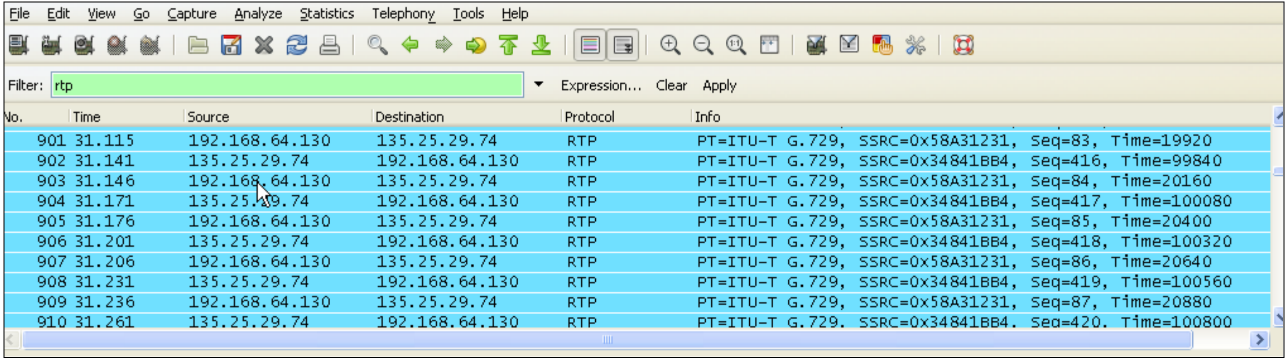
The following is an example of a call filtering on DTMF.


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

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.


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

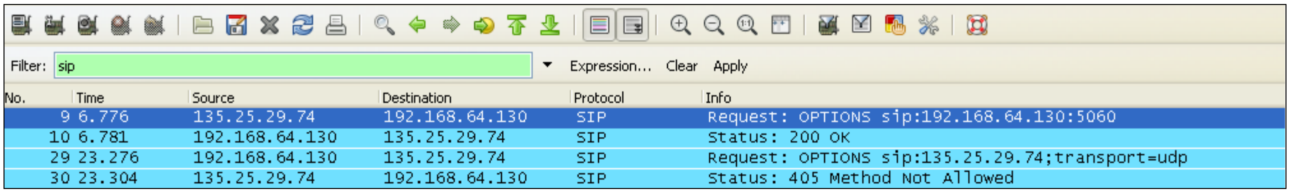
Filter: rtp

```
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
```

9.5. Avaya Session Border Controller for Enterprise Verification

9.5.1. Verify Sipera SBCE Connectivity to AT&T IP Flexible Reach

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



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

9.5.2. Internal Tracing

The Avaya SBCE can take internal traces of specified interfaces.

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

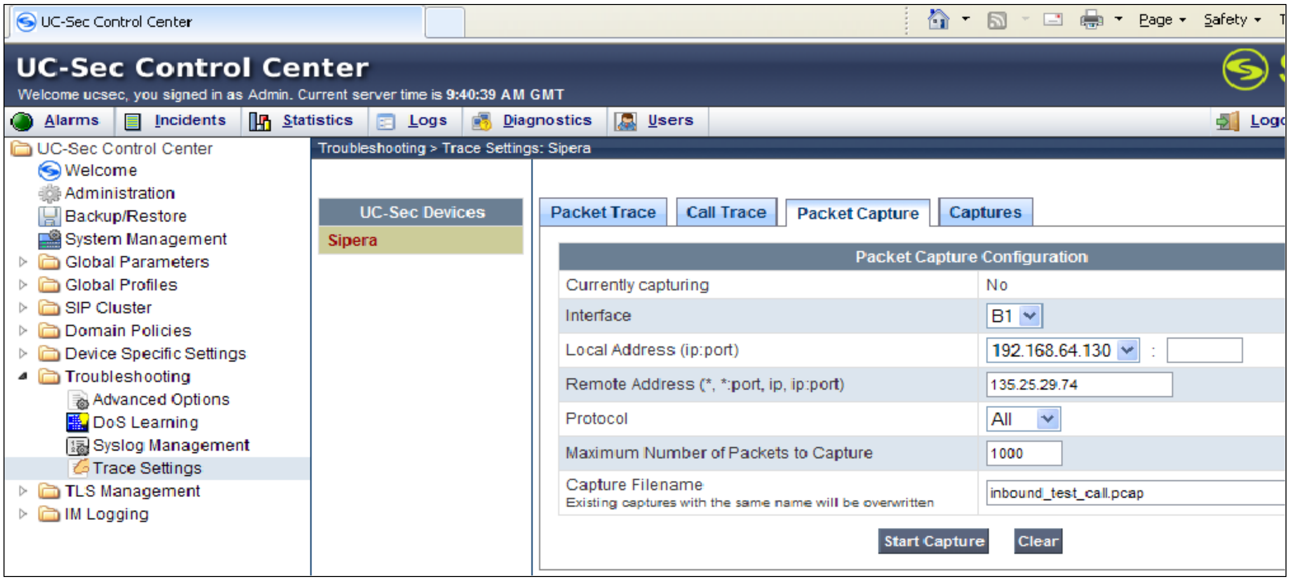
Step 2 - Select the **Packet Capture** tab and select the following:

a. Select the desired **Interface** from the drop down menu (e.g., B1, the interface to AT&T)

b. Specify the **Maximum Number of Packets to Capture** (e.g., **1000**)

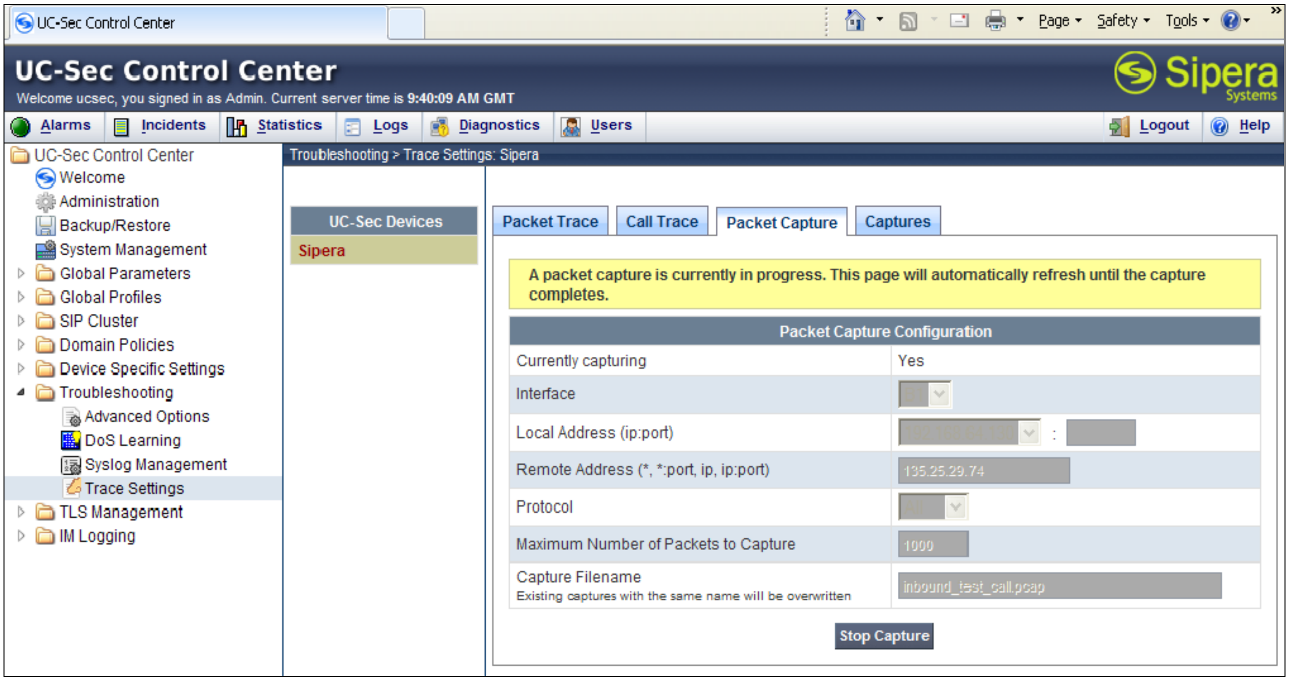
c. Specify a **Capture Filename**.

d. Click **Start Capture** to begin the trace.



Packet Capture Configuration	
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
Capture Filename Existing captures with the same name will be overwritten	inbound_test_call.pcap

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



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 9:40:09 AM GMT

Troubleshooting > Trace Settings: Sipera

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

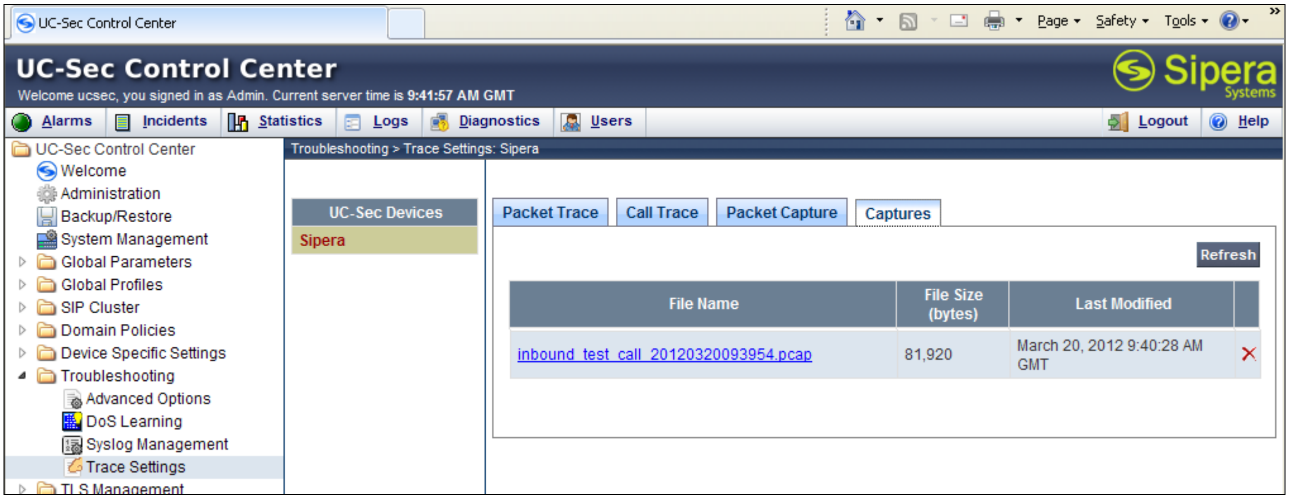
Packet Capture Configuration	
Currently capturing	Yes
Interface	
Local Address (ip:port)	:
Remote Address (*, *:port, ip, ip:port)	135.25.29.74
Protocol	
Maximum Number of Packets to Capture	1000
Capture Filename Existing captures with the same name will be overwritten	inbound_test_call.pcap

Step 3 – Run the test.

Step 4 - Select **Stop Capture** tab.

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

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



UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 9:41:57 AM GMT

Troubleshooting > Trace Settings: Sipera

File Name	File Size (bytes)	Last Modified	
inbound_test_call_20120320093954.pcap	81,920	March 20, 2012 9:40:28 AM GMT	✕

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Avaya Session Border Controller for Enterprise (Avaya SBCE) can be configured to interoperate successfully with the AT&T IP Toll Free service. 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.

Note: These Application Notes do NOT cover the AT&T IP Transfer Connect service option of the AT&T IP Toll Free service.

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

11. References

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

Avaya Aura® Session Manager/System Manager

[1] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Issue 4, May 2011

[2] *Installing and Configuring Avaya Aura® Session Manager*, Doc ID 03-603473 Issue 2.2, April 2011

[3] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Issue 4.1, March 2011

[4] **Administering Avaya Aura® System Manager**, Document Number 03-603324, June 2010

Avaya Aura® Communication Manager

[5] *Administering Avaya Aura® Communication Manager*, Release 6.003-300509, Issue 6.0, June 2010

[6] *Administering Avaya Aura® Call Center Features*, Release 6.0, June 2010

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

Avaya Aura® Messaging

[8] *Administering Avaya Aura® Messaging 6.1*, CID: 151610, December 2011

[9] *Implementing Avaya Aura® Messaging 6.1*, CID: 150976, October 2011

Avaya Session Border Controller for Enterprise

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

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

[11] *E-SBC Administration Guide, Release 4.0.5,* Part Number: 010-5424-405v1.00, Release Date: November 2011

AT&T IP Toll Free Service Descriptions:

[12] 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/

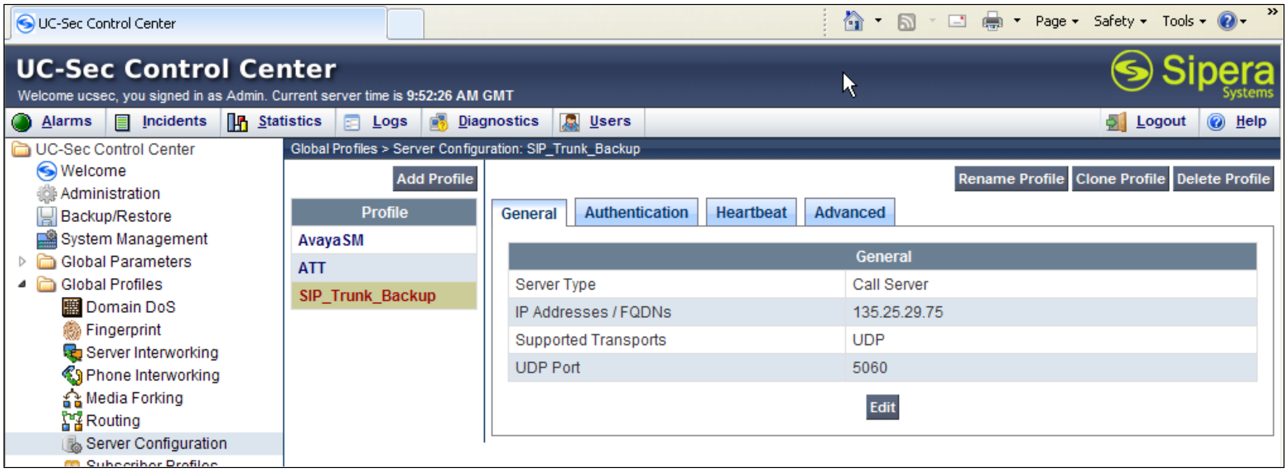
12. Addendum 1 – Avaya Session Border Controller for Enterprise Redundancy to Multiple AT&T Border Elements

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 trunk connection to 135.25.29.74 is defined in **Section 8.4.6**).

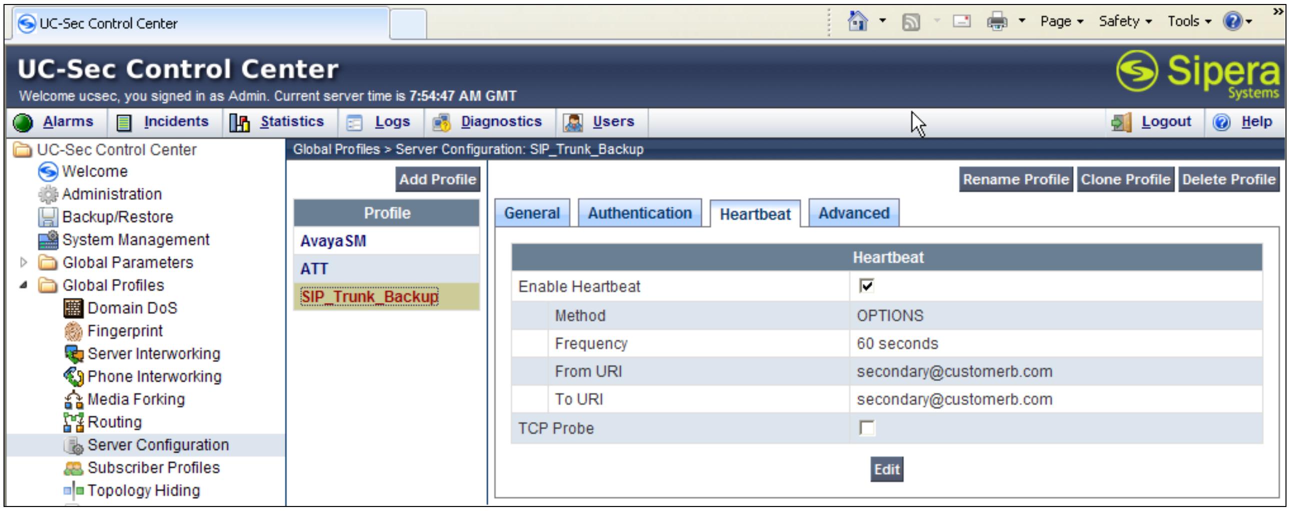
12.1.1. Step 1: Configure the Secondary Location in Server Configuration

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**
   a) **Name: SIP_Trunk_backup**
4. On the **Add Server Configuration Profile – General** tab:
   a) Select **Server Type: 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)



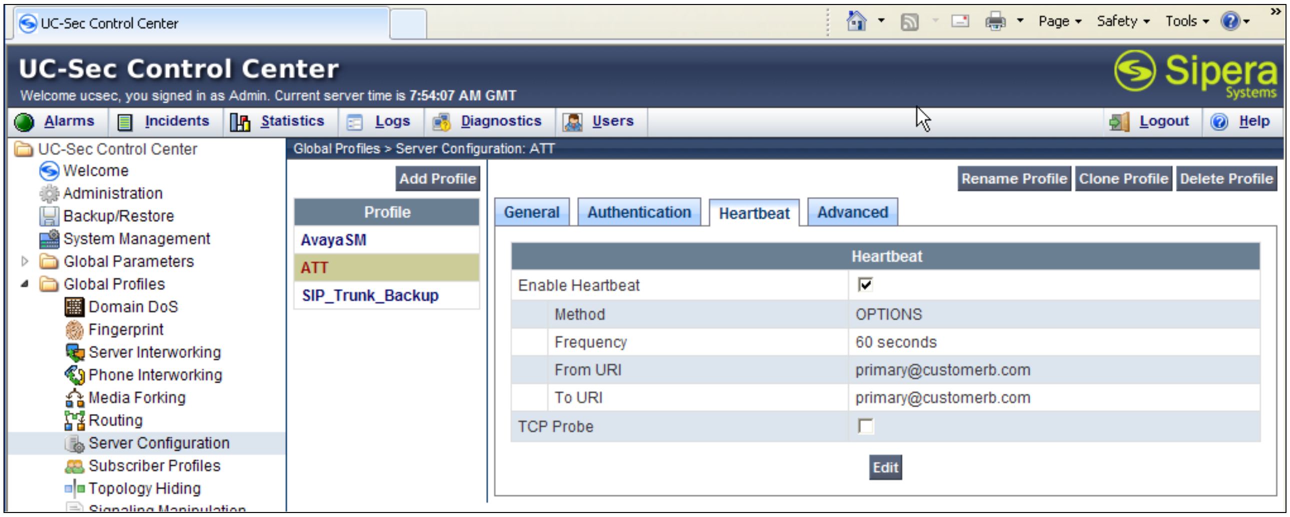
General	
Server Type	Call Server
IP Addresses / FQDNs	135.25.29.75
Supported Transports	UDP
UDP Port	5060

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@customerb.com**
   e) **To URI: secondary@customerb.com**
   f) Select **Next** (not shown)



Heartbeat	
Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	secondary@customerb.com
To URI	secondary@customerb.com
TCP Probe	☐

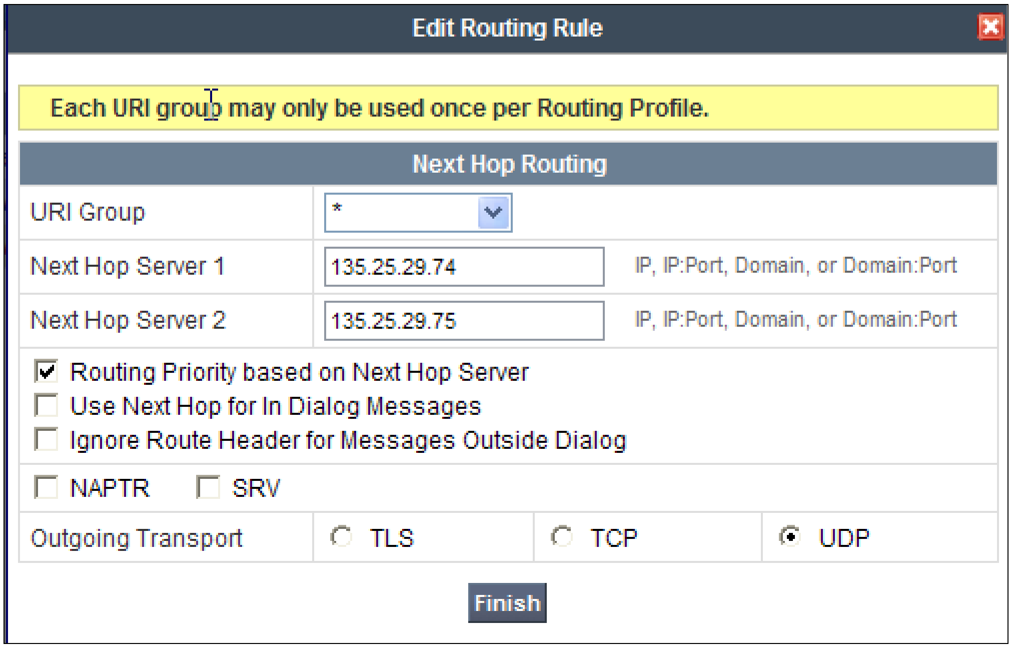
7. On the **Advanced** Tab
   a) Click **Finish** (not shown)
8. Select the Primary Trunk created in **Section 8.4.6** (e.g., **ATT**)
9. Select the **Heartbeat Tab**
10. Select **Edit**
11. Repeat **Steps 6 – 7**, but with information for the Primary Trunk as shown below.



Heartbeat	
Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	primary@customerb.com
To URI	primary@customerb.com
TCP Probe	☐

12.1.2. Step 2:– Add Secondary IP Address to Routing

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Routing**
3. Select the profile**: To_ATT**
4. Click the pencil icon at the end of the line to edit (not shown)
   a) Enter the IP Address of the secondary location in the **Next Hop Server 2** (e.g., **135.25.29.75**)
5. Click **Finish**



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

Next Hop Routing

URI Group	*	
Next Hop Server 1	135.25.29.74	IP, IP:Port, Domain, or Domain:Port
Next Hop Server 2	135.25.29.75	IP, IP:Port, Domain, or Domain:Port

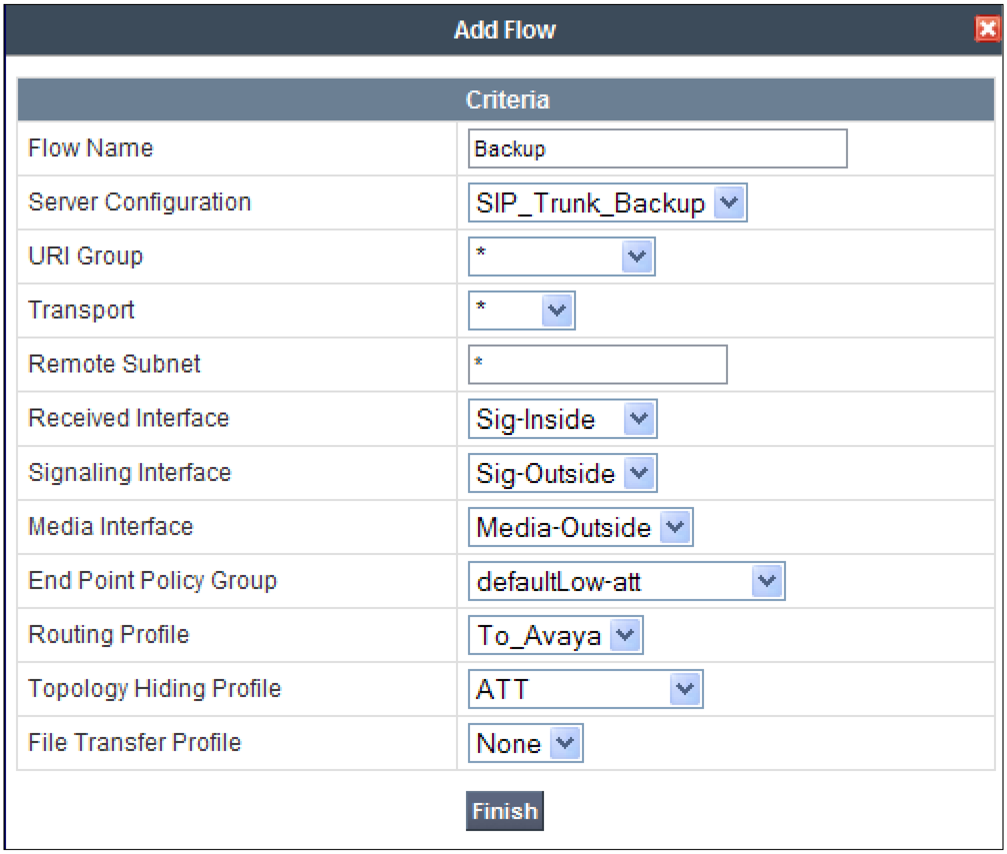
☑ Routing Priority based on Next Hop Server
□ Use Next Hop for In Dialog Messages
□ Ignore Route Header for Messages Outside Dialog

□ NAPTR □ SRV

Outgoing Transport ○ TLS ○ TCP ● UDP

12.1.3. Step 3:– Configure End Point Flows – SIP_Trunk_backup

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Endpoint Flows**
3. Select the **Server Flows** Tab
4. Select **Add Flow**
   a) **Name: Backup**
   b) **Server Configuration: SIP_Trunk_Backup**
   c) **URI Group: ***
   d) **Transport: ***
   e) **Remote Subnet: ***
   f) **Received Interface: Sig-Inside**
   g) **Signaling Interface: Sig-Outside**
   h) **Media Interface: Media-Outside**
   i) **End Point Policy Group**: **defaultLow-att**
   j) **Routing Profile: To_Avaya**
   k) **Topology Hiding Profile: ATT**
   l) **File Transfer Profile: None**
5. Click **Finish**



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
File Transfer Profile	None

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect program at devconnect@avaya.com.