Avaya Solution & Interoperability Test Lab

Applications Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Sipera™ Systems E-SBC with AT&T IP Flexible Reach SIP Trunk Service – Issue 1.1

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Sipera E-SBC with the AT&T IP Flexible Reach service using either **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 Sipera Systems E-SBC is a SIP security appliance that manages and protects the flow of SIP signaling and related media across trusted and un-trusted networks. Compliance testing focused on core enterprise Avaya endpoints traversing the LAN network through the Sipera E-SBC to the Avaya SIP infrastructure while the Sipera E-SBC enforced Denial of Service policies.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

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® Session Manager, Avaya Aura® Communication Manager 6.0.1 and Sipera E-SBC with the AT&T IP Flexible Reach service using either **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. A Sipera E-SBC is the point of connection between Avaya Aura® Session Manager and the AT&T IP Flexible Reach service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The AT&T IP Flexible Reach service is one of several SIP-based Voice over IP (VoIP) services offered to enterprises for a variety of voice communications needs. The AT&T IP Flexible Reach service allows enterprises in the U.S.A. to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites. The AT&T IP Flexible Reach service utilizes AVPN[1] or MIS/PNT[21] transport services.

For Compliance testing, Avaya Aura® Session Manager utilized the Sipera E-SBC. Sipera's E-SBC is the first Session Border Controller (SBC) designed from the ground up with the needs and requirements of small companies and enterprises in mind. Unlike SBCs that are repackaged telecommunications carrier products, the Sipera E-SBC provides all the functionality required for an enterprise to terminate SIP trunks without the complexity associated with typical SBCs.

Based on Sipera's extensive experience in SIP trunk deployments supporting hundreds of thousands of enterprise users, Sipera's E-SBC is the industry's first SBC to feature the unique SIP Trunk Integration Module (STIM), which dramatically simplifies the deployment of SIP trunks for any enterprise.

The STIM streamlines integration of SIP trunks into any of thousands of variations of enterprise SIP telephony environments, greatly reducing implementation timeframes. As a result, SIP trunk deployment in many standard configurations can occur in two hours or less.

Sipera's E-SBC and its STIM promote safe SIP trunking by reducing the complexity of SIP trunk termination and the interface into the telephony environment, ensuring proper configuration. In addition, advanced security features are available that include signature-based threat mitigation and the industry's best protection against toll fraud.

2. General Test Approach and Test Results

The general test approach was to make calls through Sipera E-SBC while DoS polices are in place using various codec settings and exercising common and advanced PBX features. Calls were made

[1] MIS/PNT does not support cRTP.

between the enterprise core Avaya SIP endpoints and the Sipera UC-Sec, the local SIP, H.323, Digital, Analog phones registered directly to Session Manager and Communication Manager.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows (see **Section 3.1** for examples) between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, the Sipera E-SBC, and the AT&T IP Flexible Reach service using AVPN or MIS/PNT transport.

The compliance testing was based on a test plan provided by AT&T, for the functionality required for certification as a solution supported on the AT&T network. Calls were made to and from the PSTN across the AT&T network (see **Section 3.1** for sample call flows). The following features were tested as part of this effort:

- SIP trunking.
- T.38 Fax.
- Passing of DTMF RFC 2833 events and their recognition by navigating automated menus.
- PBX features such as hold, resume, conference and transfer.

2.2. Test Results / Known Limitations

Interoperability testing of AT&T IP Flexible Reach version VNI22 was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **G.711 faxing is not supported between Avaya Aura® Communication Manager and the AT&T IP Flexible Reach 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.

- **Emergency 911/E911 Services Limitations and Restrictions** - Although AT&T provides 911/E911 calling capabilities, AT&T does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with AT&T IP Flexible Reach to complete 911/E911 calls; therefore, it is Customer's responsibility to ensure proper operation with its equipment/software vendor.

  While AT&T IP Flexible Reach services support E911/911 calling capabilities under certain Calling Plans, there are circumstances when that E911/911 service may not be available, as stated in the Service Guide for AT&T IP Flexible Reach found at http://new.serviceguide.att.com. Such circumstances include, but are not limited to, relocation of the end user's CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the Customer's location in the automatic location information database. Please review the AT&T IP Flexible Reach Service Guide in detail to understand the limitations and restrictions.

- **Avaya Network Call Redirection (NCR) must be disabled** (default) on the Communication Manager SIP trunk to the AT&T Flexible Reach service, otherwise connectivity issues may result in call scenarios involving Hold being signaled with "sendonly" (Communication Manager signals Hold with "sendonly" only when NCR is enabled).

2.3. Support

2.3.1. Avaya

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.

2.3.2. AT&T

AT&T customers may obtain support for the AT&T IP Flexible Reach service by calling (877) 288-8362.

2.3.3. Sipera

To contact Sipera Systems email support-team@sipera.com or call +1 866-861-3113 and +1 214-269-2424, the support portal is https://sipera.supportportal.com

3. Reference Configuration

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

- Avaya Aura® Session Manager provides core SIP routing and integration services that enables communications between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Avaya Aura® Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.

- Avaya Aura® System Manager provides a common administration interface for centralized management of all Avaya Aura® Session Manager instances in an enterprise.

- Avaya Aura® Communication Manager provides the voice communications services for a particular enterprise site. In the reference configuration, Avaya Aura® Communication Manager runs on an Avaya S8510 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 Avaya Aura® Communication Manager. In the reference configuration, an Avaya G450 Media

Gateway and a G650 Gateway is used. This solution is extensible to other Avaya Media Gateways.

- Avaya “desk” phones are represented with Avaya 4600 and 9600 Series IP Telephones running H.323 software, 9600 Series IP Telephones running SIP software, Avaya 6211 Series Analog Telephones, and Avaya one-X® Communicator, a PC based softphone.

- The Sipera E-SBC provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation between the AT&T IP Flexible Reach service and the enterprise internal network. UDP transport protocol is used between the Sipera E-SBC and the AT&T IP Flexible Reach service.

- An existing Avaya Modular Messaging system (in Multi-Site mode in this reference configuration) provides the corporate voice messaging capabilities in the reference configuration. The provisioning of Modular Messaging is beyond the scope of this document.

- Outbound calls were originated from a phone or fax provisioned on Avaya Aura® Communication Manager. Signaling passed from Avaya Aura® Communication Manager to Avaya Aura® Session Manager and on to the Sipera E-SBC, before being sent to the AT&T network for termination. Media was sent from the calling phone to the Avaya Aura® Communication Manager Media Processor initially on call setup, but when applicable, the media was redirected directly from the station (“shuffled”) via the Sipera E-SBC.

- Inbound calls were sent from AT&T, through the Sipera E-SBC to the Avaya Aura® Session Manager which routed the call to Avaya Aura® Communication Manager. Avaya Aura® Communication Manager terminated the call to the appropriate phone or fax extension. The H.323 phones on the enterprise side registered to the Avaya Aura® Communication Manager Procr. The SIP phones on the enterprise side registered to the Avaya Aura® Session Manager.

- Enterprise sites may have additional or alternate routes to PSTN using analog or digital TDM trunks. However these trunks were not available in the reference configuration.

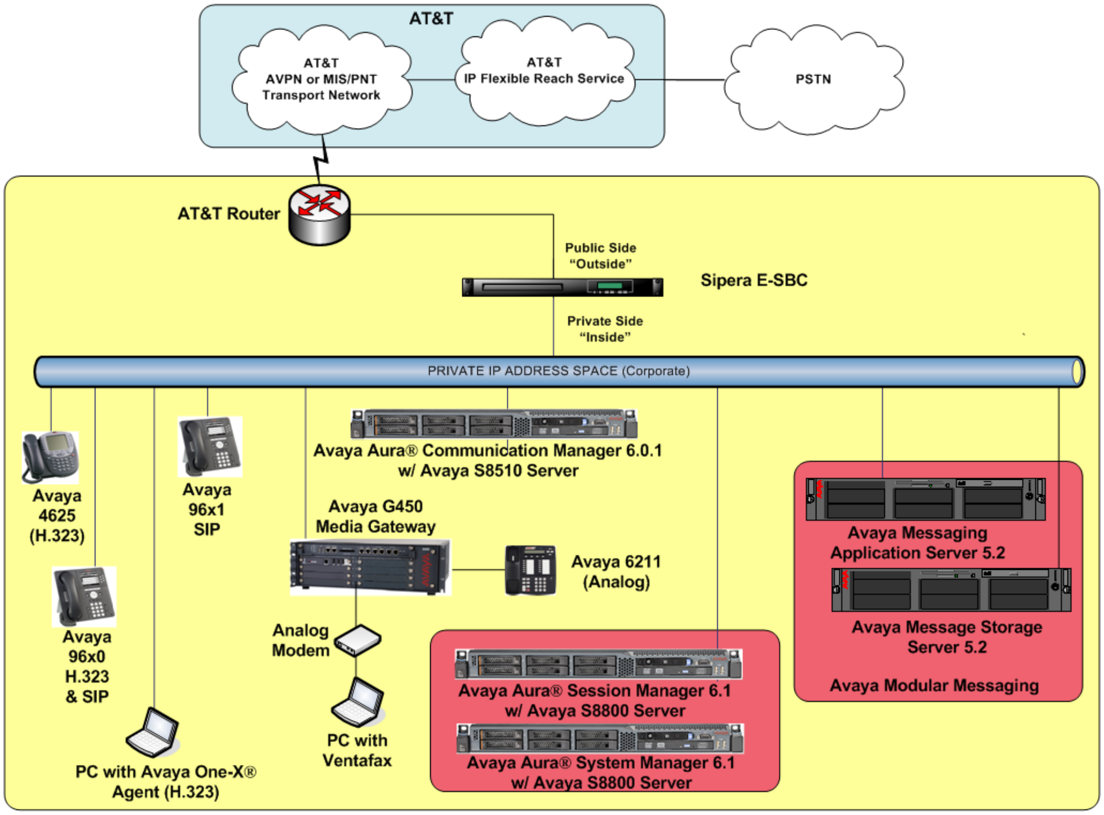

AT&T
AT&T AVPN or MIS/PNT Transport Network
AT&T IP Flexible Reach Service
PSTN
AT&T Router
Public Side "Outside"
Sipera E-SBC
Private Side "Inside"
PRIVATE IP ADDRESS SPACE (Corporate)
Avaya 4625 (H.323)
Avaya 96x1 SIP
Avaya Aura® Communication Manager 6.0.1 w/ Avaya S8510 Server
Avaya G450 Media Gateway
Avaya 6211 (Analog)
Avaya Messaging Application Server 5.2
Avaya Message Storage Server 5.2
Avaya Modular Messaging
Avaya 96x0 H.323 & SIP
Analog Modem
PC with Ventafax
Avaya Aura® Session Manager 6.1 w/ Avaya S8800 Server
Avaya Aura® System Manager 6.1 w/ Avaya S8800 Server
PC with Avaya One-X® Agent (H.323)

Figure 1: Avaya Interoperability Test Lab Configuration

3.1. Call Flows

To understand how inbound AT&T IP Flexible Reach service calls are handled by Session Manager and Communication Manager, three basic call flows are described in this section, however for brevity not all possible call flows are described.

3.1.1. Inbound

The first call scenario illustrated in the figure below is an inbound AT&T IP Flexible Reach service call that arrives on Session Manager and is subsequently routed to Communication Manager, which in turn routes the call to a phone, fax, or in some cases, a vector.

1. A PSTN phone originates a call to an AT&T IP Flexible Reach service number.
2. The PSTN routes the call to the AT&T IP Flexible Reach service network.

3. The AT&T IP Flexible Reach service routes the call to the Sipera E-SBC.
4. The Sipera E-SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to Communication Manager.
6. Depending on the called number, Communication Manager routes the call to a phone, a fax or a vector.

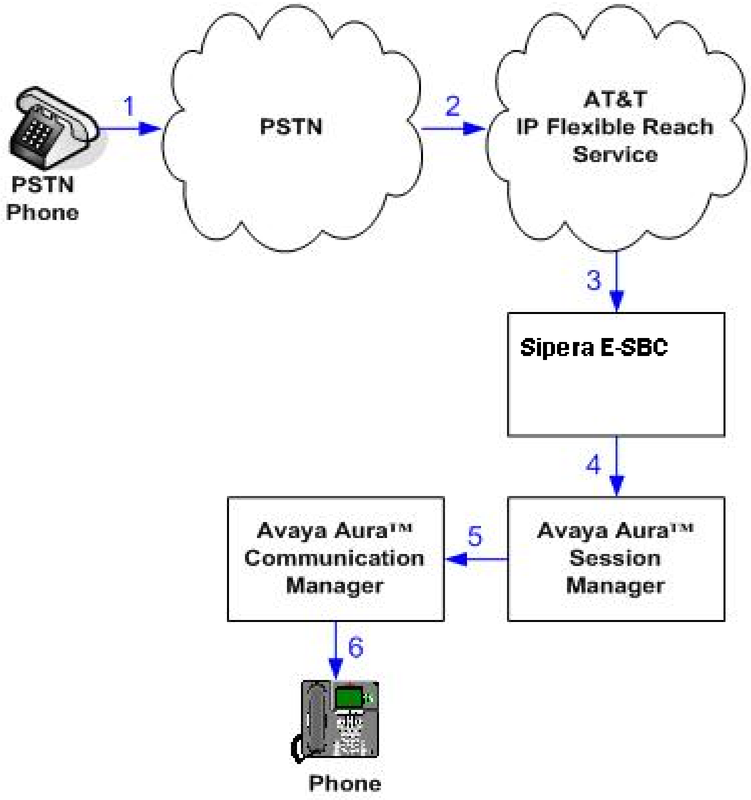


Figure 2: Inbound Call Flow

3.1.2. Outbound

The second call scenario illustrated in the figure below is an outbound call initiated on Communication Manager, routed to Session Manager and is subsequently sent to the Sipera E-SBC for delivery to AT&T IP Flexible Reach service.

1. A Communication Manager phone or fax originates a call to an AT&T IP Flexible Reach service number for delivery to PSTN.
2. Communication Manager routes the call to the Session Manager.
3. Session Manager applies any necessary SIP header adaptations and digit conversions, and based on configured Routing Policies, determines to where the call should be routed next. In this case, Session Manager routes the call to the Sipera E-SBC.

4. The Sipera E-SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to the AT&T IP Flexible Reach service.
5. The AT&T IP Flexible Reach service delivers the call to PSTN.

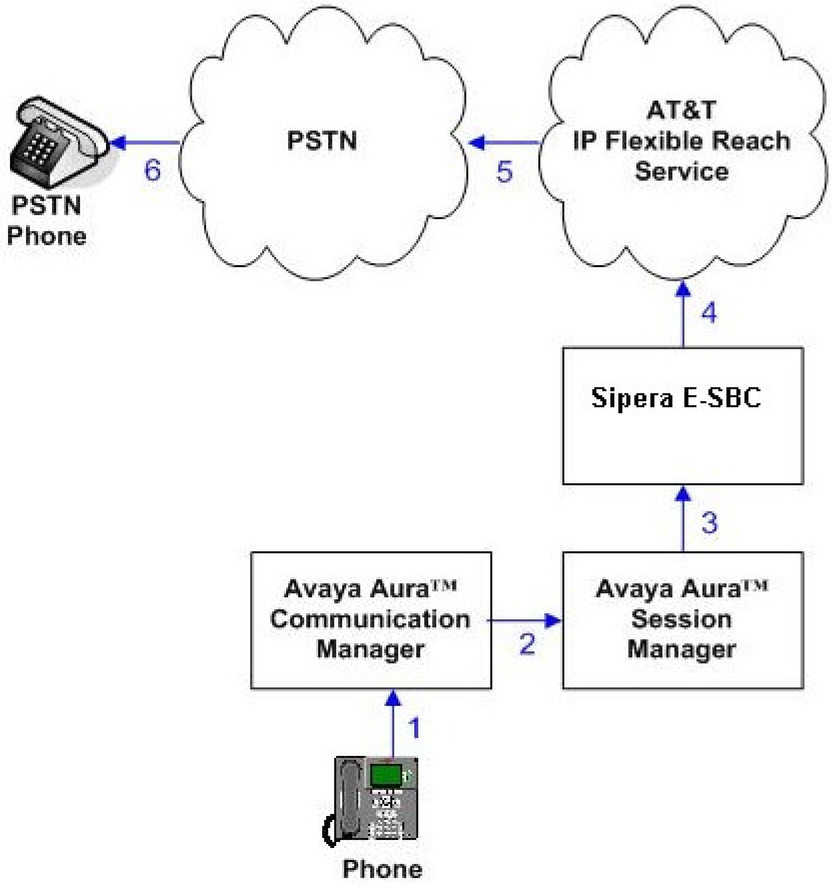


Figure 3 – Outbound Call Flow

3.1.3. Call Forward Re-direction

The third call scenario illustrated below is an inbound AT&T IP Flexible Reach service call that arrives on Session Manager and subsequently Communication Manager. Communication Manager routes the call to a destination station, however the station has set Call Forwarding to an alternate destination. Without answering the call, Communication Manager immediately redirects the call back to the AT&T IP Flexible Reach service for routing to the alternate destination.

Note – In cases where the alternate destination is an N11, NPA-555-1212, or 8xx number, then the AT&T IP Flexible Reach service requires the use of SIP Diversion Header for the redirected call to complete (see **Section 6.9**).

1. Same as the first call scenario in **Section 3.1.1**.
2. Because the Communication Manager phone has set Call Forward to another AT&T IP Flexible Reach service number, Communication Manager initiates a new call back out to Session Manager, the Sipera E-SBC, and to the AT&T IP Flexible Reach service network.
3. The AT&T IP Flexible Reach service places a call to the alternate destination and upon answer, Communication Manager connects the calling party to the target party.

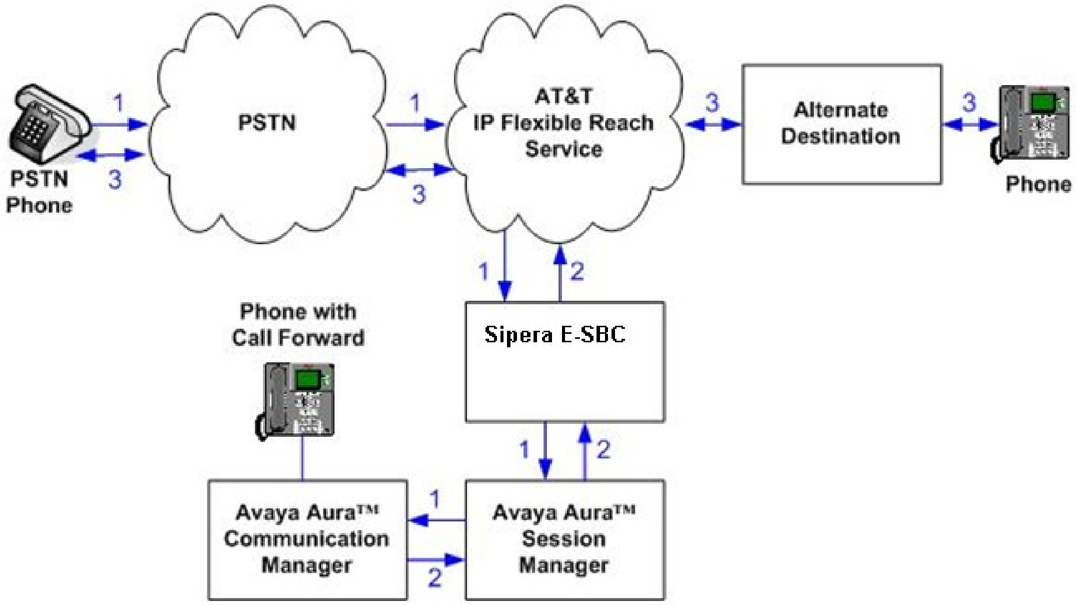

PSTN Phone
1
3
PSTN
1
3
AT&T IP Flexible Reach Service
3
Alternate Destination
3
Phone
1
2
Phone with Call Forward
Sipera E-SBC
1
2
Avaya Aura™ Communication Manager
1
2
Avaya Aura™ Session Manager

Figure 4: Inbound Call Redirected Off-net

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment:	Software:
Avaya S8510 Server	Avaya Aura® Communication Manager Release 6.0.1 load 510.1-19100
G650 Gateway TN2312BP (IPSI) TN2602AP (MedPro) TN799DP (CLAN) TN2224B (Digital Line Card) TN793B (Analog Line Card)	 HW36 FW 51 HW28 FW55 HW16 FW38 HW12 HW6
G450 Gateway	FW 30.12.1

Avaya S8800 Server	Avaya Aura® Session Manager 6.0 (6.1.4.0.614005)
Avaya S8800 Server	Avaya Aura® System Manager 6.1.0 (Build No. - 6.1.0.0.7345-6.1.5.115)
Sipera E-SBC	4.0.4.Q143
Avaya Modular Messaging (Application Server)	Avaya Modular Messaging (MAS) 5.2 Service Pack 5 Patch 1
Avaya Modular Messaging (Storage Server)	Avaya Modular Messaging (MSS) 5.2, Build 5.2-11.0
Avaya 9600-Series Telephones (H.323)	Release 030909 - H.323 - 4625 Release 3.0 – H.323 -9630 Release 6.0 - H.323 - 9608, 9621
Avaya 9600-Series Telephones (SIP)	SIP96XX_2_6_3_0.bin
Avaya One-X Communicator (H.323)	Release 6.0.1.16-SP1-25226
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
AT&T IP Flexible Reach Service using AVPN or MIS/PNT transport service connections.	VNI 22

5. Configure Avaya Aura® Session Manager

These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult [1] and [2] for further details if necessary. Configuration of Session Manager is performed from System Manager. To invoke the System Manager Common Console, launch a web browser, enter https://<*IP address of the System Manager server*>/SMGR in the URL, and log in with the appropriate credentials.

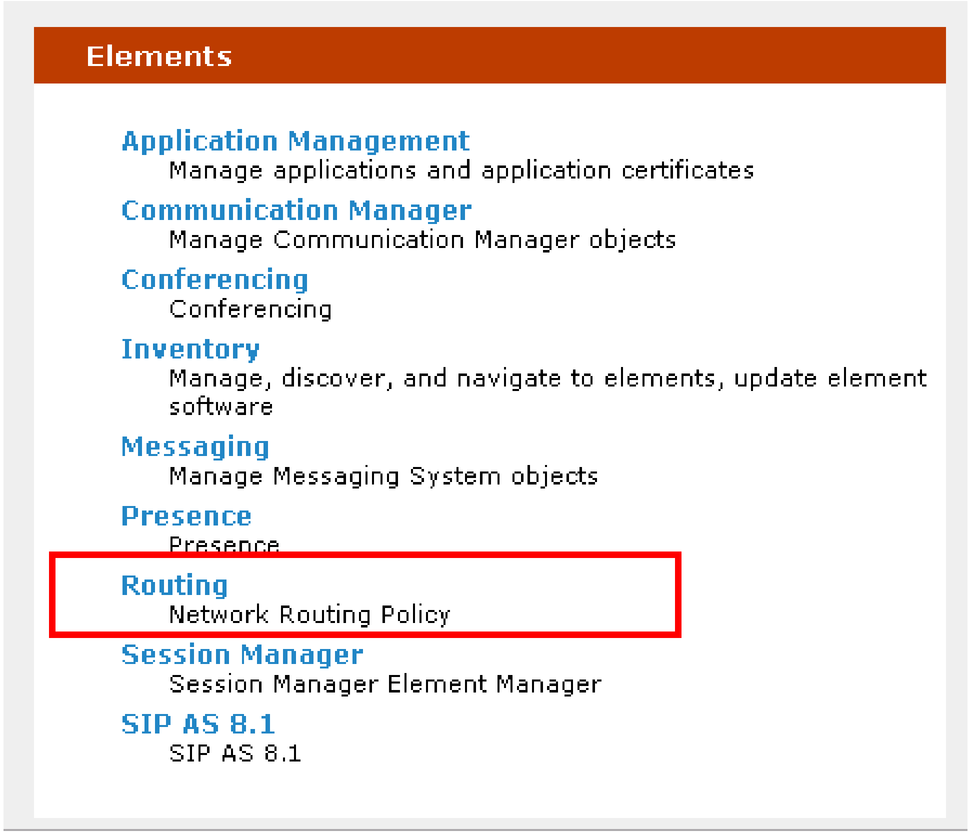
5.1. Routing Policies

Routing Policies define how Session Manager routes calls between SIP network elements. Routing Policies are dependent on the administration of several inter-related items:

- SIP Entities – SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- Entity Links – Entity Links define the SIP trunk/link parameters, e.g., ports, protocol (UDP/TCP/TLS), and trust relationship, between Session Manager instances and other SIP Entities.
- SIP Domains – SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS).
- Locations – Locations define the physical and/or logical locations in which SIP Entities reside. Call Admission Control (CAC) / bandwidth management may be administered for each location to limit the number of calls to and from a particular Location.

- Adaptations – Adaptations are used to apply any necessary protocol adaptations, e.g., modify SIP headers, and apply any necessary digit conversions for the purpose of inter-working with specific SIP Entities. For example, an AT&T-specific Adaptation could be used to remove SIP History-Info headers from SIP messages sent to the AT&T IP Flexible Reach service network. As another example, basic "Digit Conversion" Adaptations could be done in Session Manager to convert digit strings in "destination" (e.g., Request-URI) and "origination" (e.g. P-Asserted Identity) type headers, of SIP messages sent to and received from SIP Entities.
- Dial Patterns – A Dial Pattern specifies a set of criteria and a set of Routing Policies for routing calls that match the criteria. The criteria include the called party number and SIP domain in the Request-URI, and the Location from which the call originated. For example, if a call arrives at Session Manager and matches a certain Dial Pattern, then Session Manager selects one of the Routing Policies specified in the Dial Pattern. The selected Routing Policy in turn specifies the SIP Entity to which the call is to be routed. Note that Dial Patterns are matched after ingress Adaptations have already been applied.
- Time Ranges – Time Ranges specify customizable time periods, e.g., Monday through Friday from 9AM to 5:59PM, Monday through Friday 6PM to 8:59AM, all day Saturday and Sunday, etc. A Routing Policy may be associated with one or more Time Ranges during which the Routing Policy is in effect. For example, for a Dial Pattern administered with two Routing Policies, one Routing Policy can be in effect on weekday business hours and the other Routing Policy can be in effect on weekday off-hours and weekends. In the reference configuration no restrictions were placed on calling times.

To view the sequenced steps required for configuring network routing policies, click on "**Routing**" in the middle pane of the System Manager Common Console under the title "**Elements**".



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

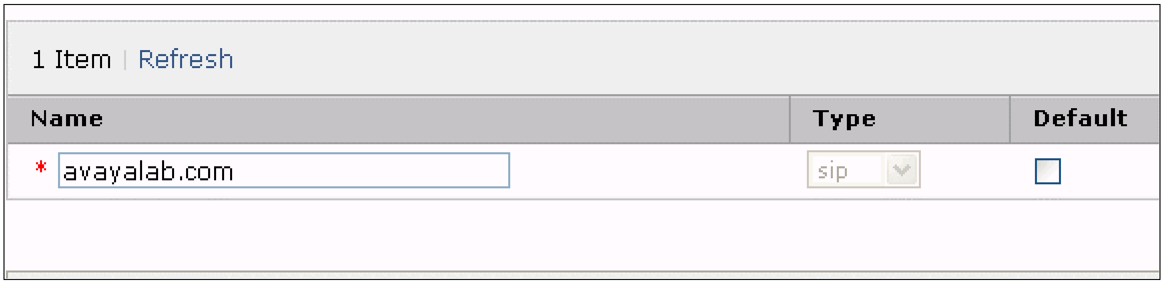
SIP AS 8.1
SIP AS 8.1

Figure 5: System Manager Elements Menu

5.2. SIP Domains

The steps in this section specify the SIP domains for which Session Manager is authoritative.

1. In the left pane under **Routing**, click on **Domains**. In the **Domain Management** page click on **New** (not shown).
2. Continuing in the **Domain Management** page, enter a SIP domain (e.g. **avayalab.com**) for **Name**
3. Select **Type sip.**
4. (Optional) Add notes.
5. Click on "**Commit**



1 Item | Refresh

Name	Type	Default
* avayalab.com	sip	□

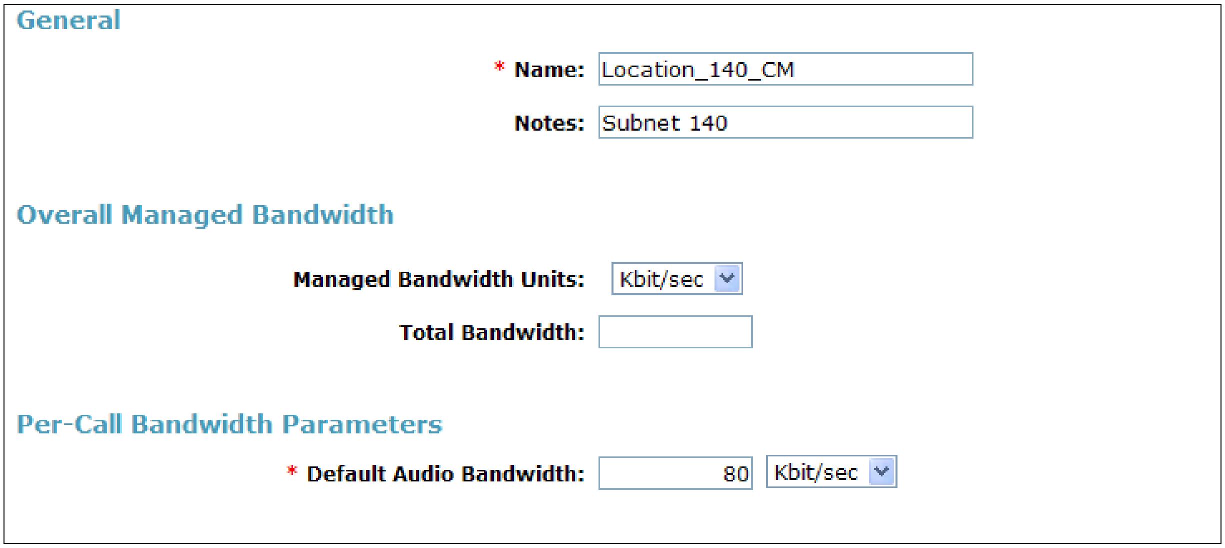
Figure 6: SIP Domain in Session Manager

5.3. Locations

The steps in this section define the physical and/or logical locations in which SIP Entities reside.

5.3.1. CM location

1. In the left pane under **Routing**, click on **Locations**. In the **Location** page click on **New** (not shown).
2. In the **Location Details** page, enter a descriptive **Name** (e.g. **Location_140_CM**).
3. [Optional] To limit the number of calls going to and from this Location, i.e., apply CAC, specify the **Managed Bandwidth** and **Average Bandwidth per Call**.
4. The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 5.4**), so it was not necessary to add a pattern.
5. Click on **Commit** (not shown).



General

* Name: Location_140_CM

Notes: Subnet 140

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

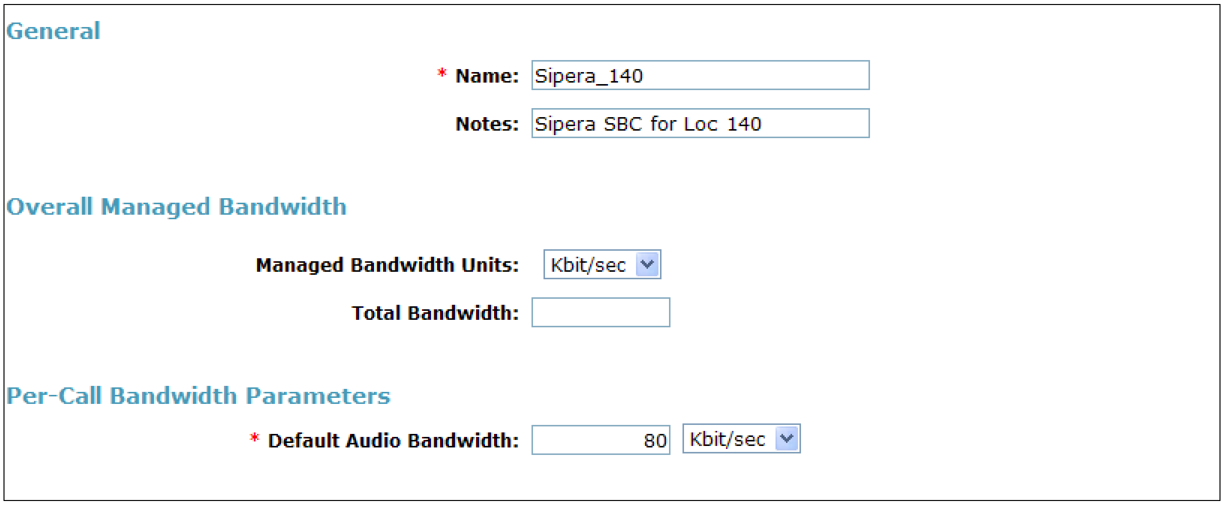
* Default Audio Bandwidth: 80 Kbit/sec

Figure 7: Creating a location for Communication Manager

5.3.2. Sipera Location

1. In the left pane under **Routing**, click on **Locations**. In the **Location** page click on **New** (not shown).
2. In the **Location Details** page, enter a descriptive **Name** (e.g. **Sipera_140**).
3. [Optional] To limit the number of calls going to and from this Location, i.e., apply CAC, specify the **Managed Bandwidth** and **Average Bandwidth per Call**.
4. The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample

configuration Locations are added to SIP Entities (**Section 5.4**), so it was not necessary to add a pattern.
5. Click on **Commit** (not shown).



General

* Name:	Sipera_140
Notes:	Sipera SBC for Loc 140

Overall Managed Bandwidth

Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	

Per-Call Bandwidth Parameters

* Default Audio Bandwidth:	80	Kbit/sec

Figure 8: Creating a location for Sipera E-SBC

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 (AT&T access) – This entity, and its associated entity link (using port 5060), is for calls between Communication Manager and the Sipera E-SBC. – **Section 5.4.2**
- Avaya Aura® Communication Manager (Local access) – This entity, and associated link (using port 5060), is for outbound calls to AT&T from Avaya SIP phones to Communication Manager. – **Section 5.4.3**
- Sipera E-SBC – This entity, and its associated entity link (using port 5060), is for calls between the Sipera E-SBC and AT&T. – **Section 5.4.4**

1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name –** Enter a descriptive name for the entity (e.g. **ASM, S8510_CM_601_procr_tg_5, S8510_CM601_clan, Sipera**).
- **FQDN or IP Address –** Enter the IP address of the entity. On the Session Manager select the network interface, (*not* the management interface), provisioned during installation (e.g. **10.80.150.206**).
- **Type –** Select the appropriate Entity Type. Eg. **Session Manager**, **CM**, **Other**.
- **Location** – Select location. Eg. **Location_150_SM**, **Location_140_CM**, **Sipera_140**(**Section 5.4**).

- **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.

4. SIP Link Monitoring – Select **Use Session Manager Configuration**.
5. Click **Commit (not shown)**.

Section 5.4 must be repeated for every **SIP Entity (i.e. Session Manager, Sipera, Communication Manager**. Once all entities have been created, **Entity Links** must be defined. These links can be defined within the **SIP Entity** screen or in the **Entity Links** section. If defined within the **SIP Entity** screen, the **Name** of the link is auto-created. If created in the **Entity Links** section, the **Name** is configurable. Here, the links are created within the **SIP Entity** screen and shown at the bottom of **Figure 13**.

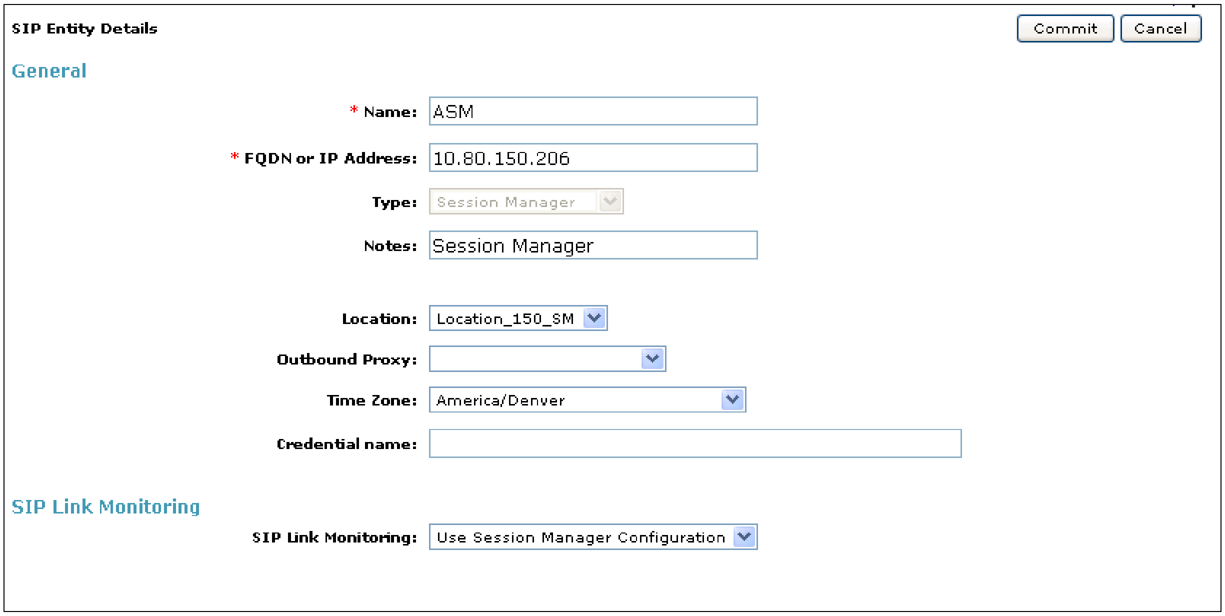
1. Under the SIP Entities section, select the name of your Session Manager.

- In the **Entity Links** section of the **SIP Entity Details** page click **Add** (A new line appears with the Session Manager listed as SIP Entity 1 that was defined in **Section 5.4.1**.
- Select the **Protocol** the SIP Entity 1 is to use to communicate with SIP Entity 2. (**TCP, TLS, UDP**)
- Enter the Port SIP Entity 1 is to use to communicate with SIP Entity 2. (eg. **5060**)
- Select SIP Entity 2 from the drop-down list.(e.g. **ASM, S8510_CM_601_procr_tg_5, S8510_CM601_clan, Sipera**)
- Enter the Port SIP Entity 2 is to use to communicate with SIP Entity 1. (eg. **5060**)
- Enter the Connection Policy desired. (Eg. "**Trusted**", "**Trusted HA**", "**Untrusted**")

6. Click on **Commit** (not shown).

These entries enable Session Manager to accept SIP requests on the specified ports/protocols. In addition, Session Manager will associate SIP requests containing the IP address of Session Manager (10.80.150.206) in the host part of the Request-URI

5.4.1. ASM Link



SIP Entity Details

General

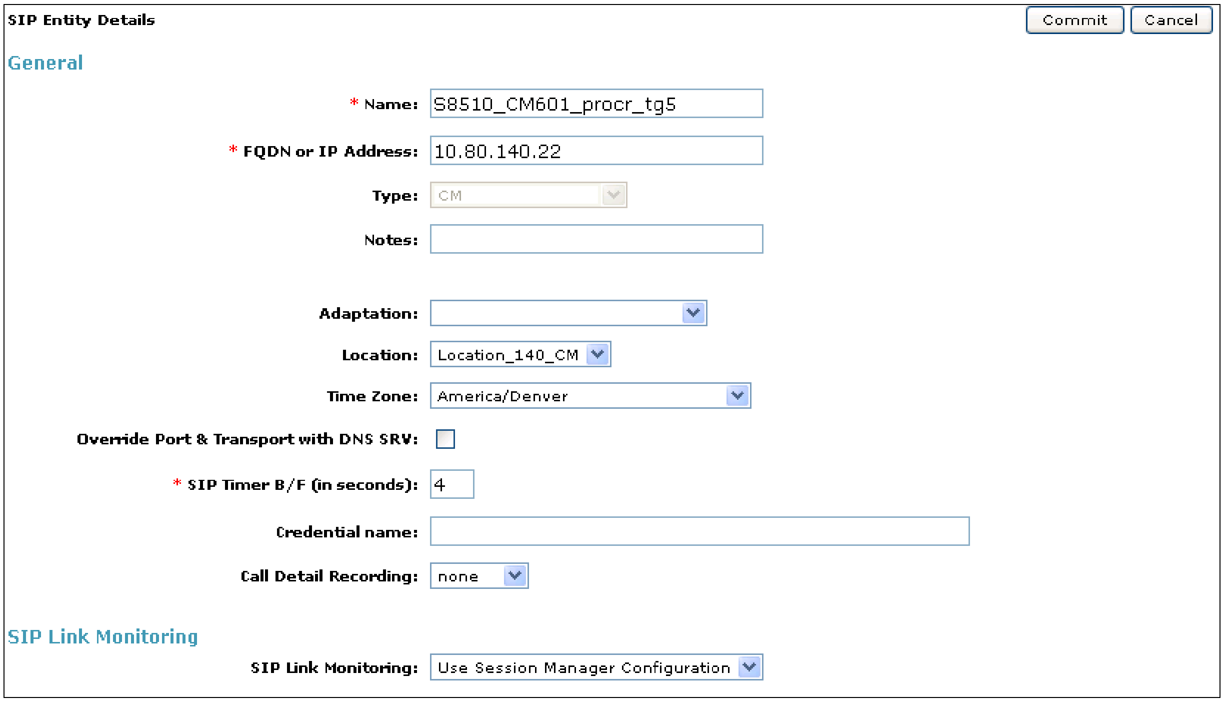
* Name: ASM
* FQDN or IP Address: 10.80.150.206
Type: Session Manager
Notes: Session Manager
Location: Location_150_SM
Outbound Proxy:
Time Zone: America/Denver
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Figure 9: Creating an Entity for Session Manager

5.4.2. Avaya Aura® Communication Manager (AT&T Access)



SIP Entity Details

General

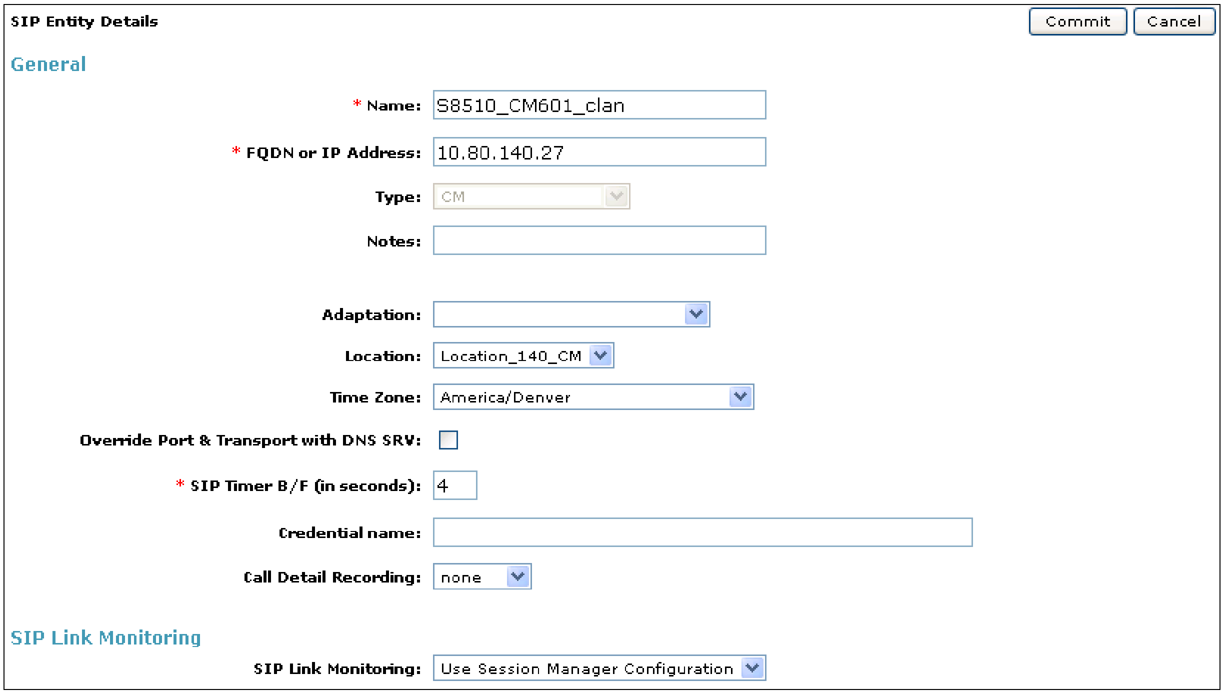
* Name: S8510_CM601_procr_tg5
* FQDN or IP Address: 10.80.140.22
Type: CM
Notes:
Adaptation:
Location: Location_140_CM
Time Zone: America/Denver
Override Port & Transport with DNS SRV: □
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Figure 10: Creating an Entity for Communication Manager Procr

5.4.3. Avaya Aura® Communication Manager (Local access)



SIP Entity Details

Commit | Cancel

General

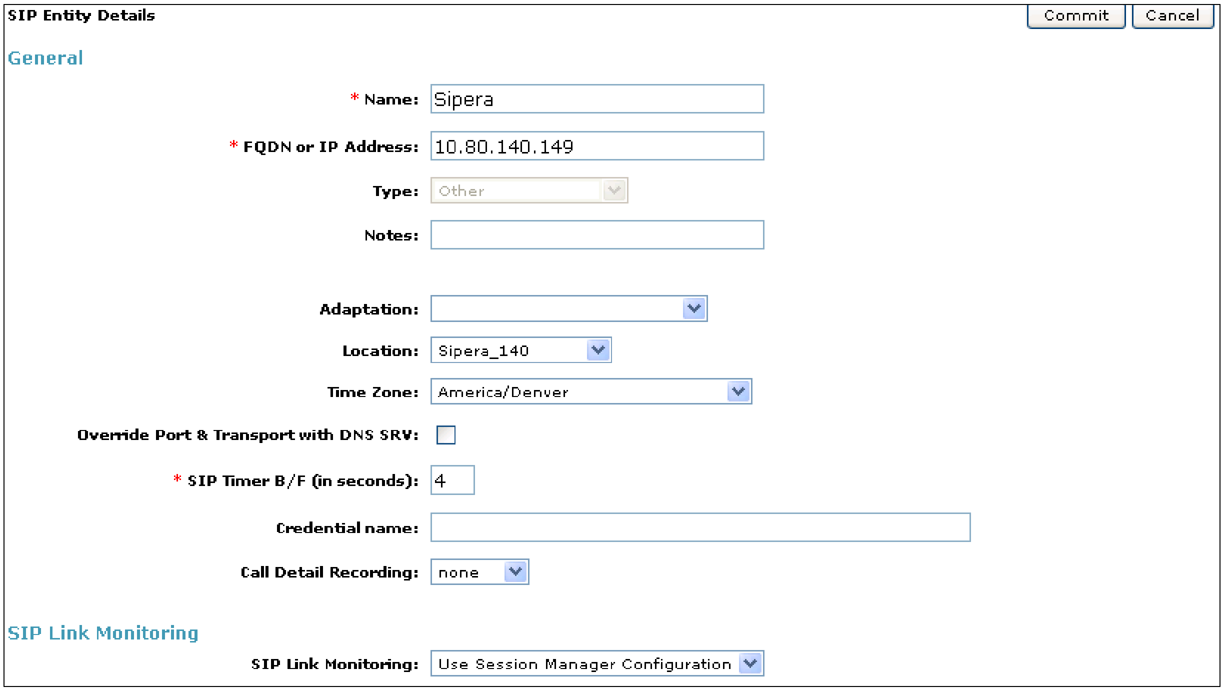
* Name:	S8510_CM601_clan
* FQDN or IP Address:	10.80.140.27
Type:	CM
Notes:	
Adaptation:	
Location:	Location_140_CM
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

Figure 11: Creating an Entity for Communication Manager Clan

5.4.4. Sipera E-SBC



SIP Entity Details

Commit | Cancel

General

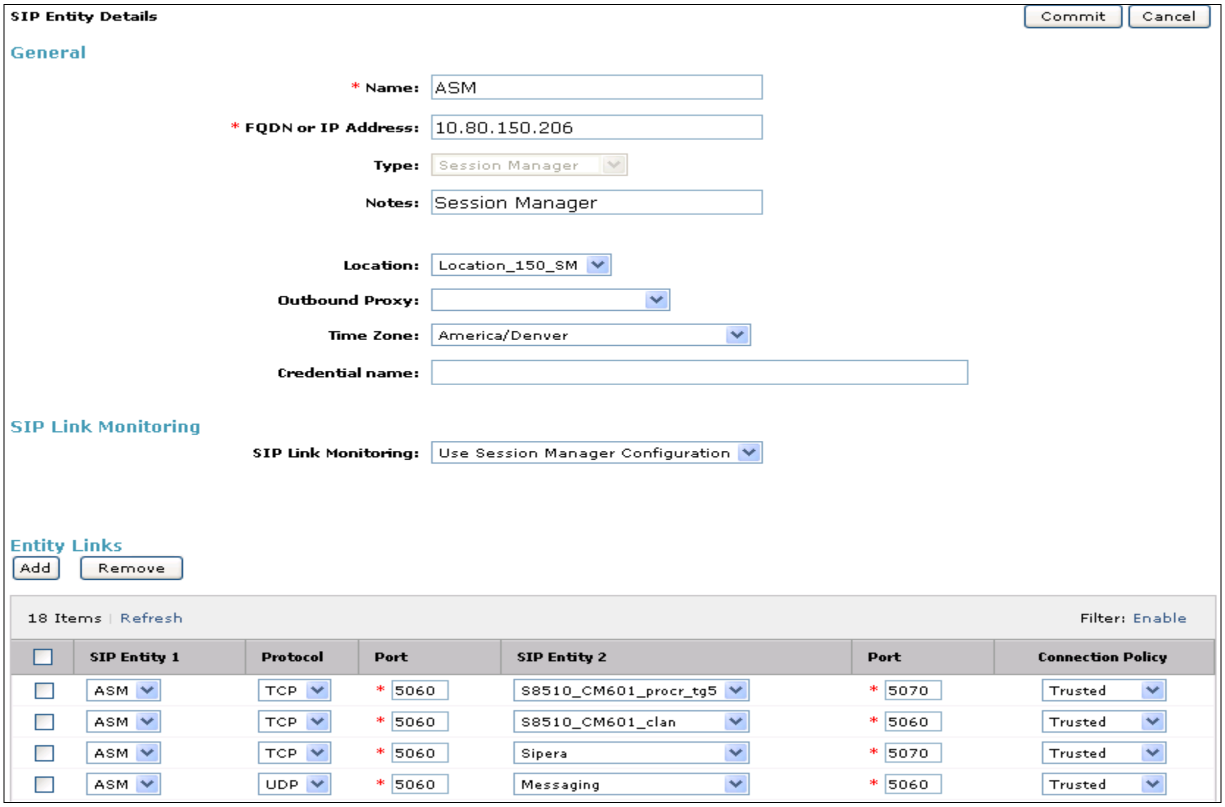
* Name:	Sipera
* FQDN or IP Address:	10.80.140.149
Type:	Other
Notes:	
Adaptation:	
Location:	Sipera_140
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	□
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

Figure 12: Creating an Entity for Sipera E-SBC

5.4.5. ASM with Associated Entity Links



* Name: ASM

* FQDN or IP Address: 10.80.150.206

Type: Session Manager

Notes: Session Manager

Location: Location_150_SM

Outbound Proxy:

Time Zone: America/Denver

Credential name:

SIP Link Monitoring: Use Session Manager Configuration

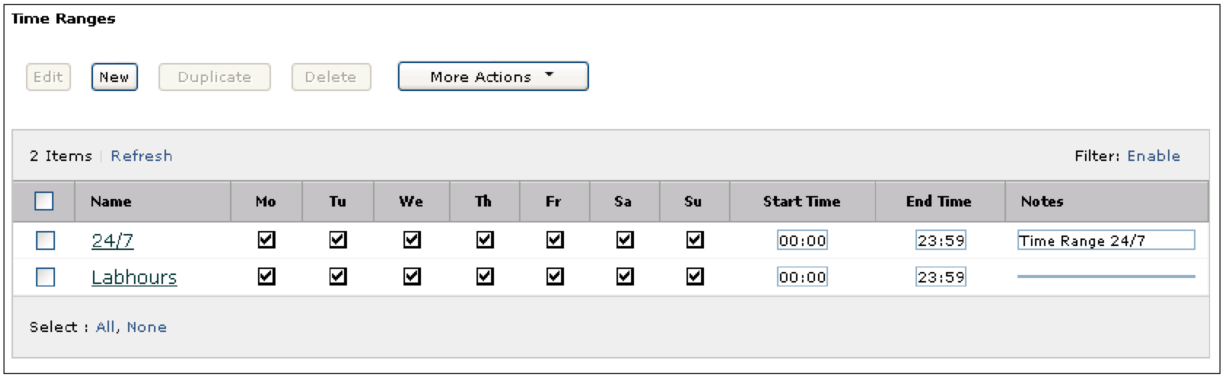
18 Items

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
□	ASM	TCP	* 5060	S8510_CM601_procr_tg5	* 5070	Trusted
□	ASM	TCP	* 5060	S8510_CM601_clan	* 5060	Trusted
□	ASM	TCP	* 5060	Sipera	* 5070	Trusted
□	ASM	UDP	* 5060	Messaging	* 5060	Trusted

Figure 13: Creating a Entity Links for Entities

5.5. Time Ranges

1. In the left pane under **Routing**, click on **Time Ranges**. In the **Time Ranges** page click on **New** (not shown).
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**.
3. Click on **Commit (not shown)**.
4. Repeat Steps 1 – 3 to provision additional time ranges.



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

Figure 14: Creating Time Ranges

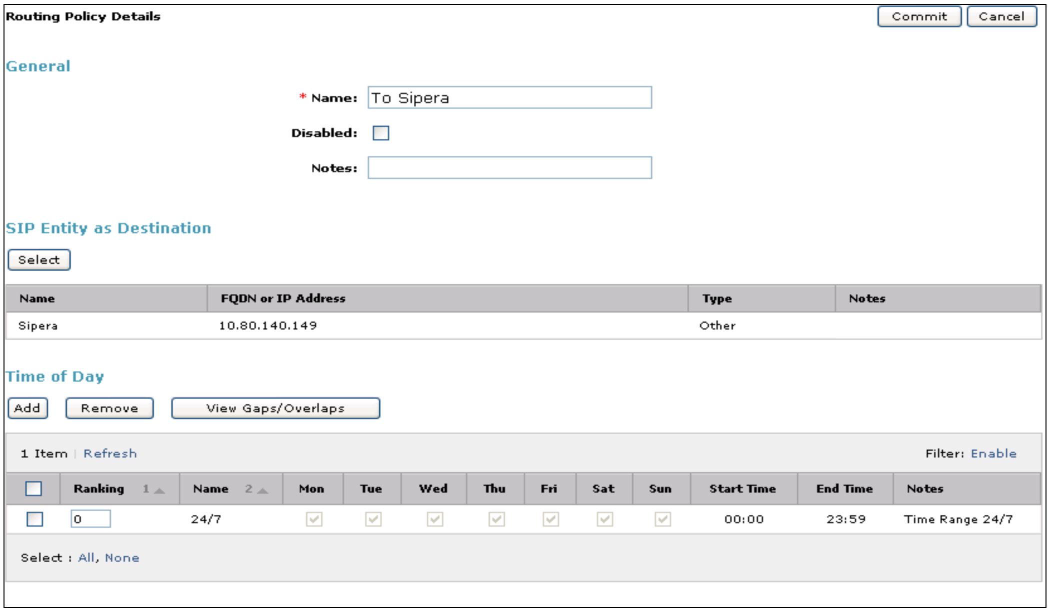
5.6. Routing Policies

In this section, Routing Policies are administered for routing calls to the following SIP Entities:

- To AT&T network via the Sipera E-SBC (5.6.1).
- To Avaya Aura® Communication Manager from AT&T (5.6.2).
- To Avaya Aura® Communication Manager from Avaya SIP phones (5.6.3).

5.6.1. Routing Policy for Routing to the AT&T Flexible Reach Service

1. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to AT&T (**To Sipera**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select**.
4. In the **SIP Entity List** page select the SIP Entity administered in **Section 5.4.4** or the Sipera E-SBC (**Sipera**), (not shown) and click on **Select**.
5. Returning to the Routing Policy Details page in the Time of Day section, click on Add.
6. In the **Time Range List** page, check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.5**, and click on **Select**.
7. Returning to the **Routing Policy Details** page, in the **Time of Day** section, enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on **Commit**.
8. Note that once the **Dial Patterns** are defined (**Section 5.7**) they will appear in the **Dial Pattern** section.
9. No **Regular Expressions** were used in the reference configuration.
10. Click on **Commit**.



Routing Policy Details

General

* Name: To Sipera

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Sipera	10.80.140.149	Other	

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

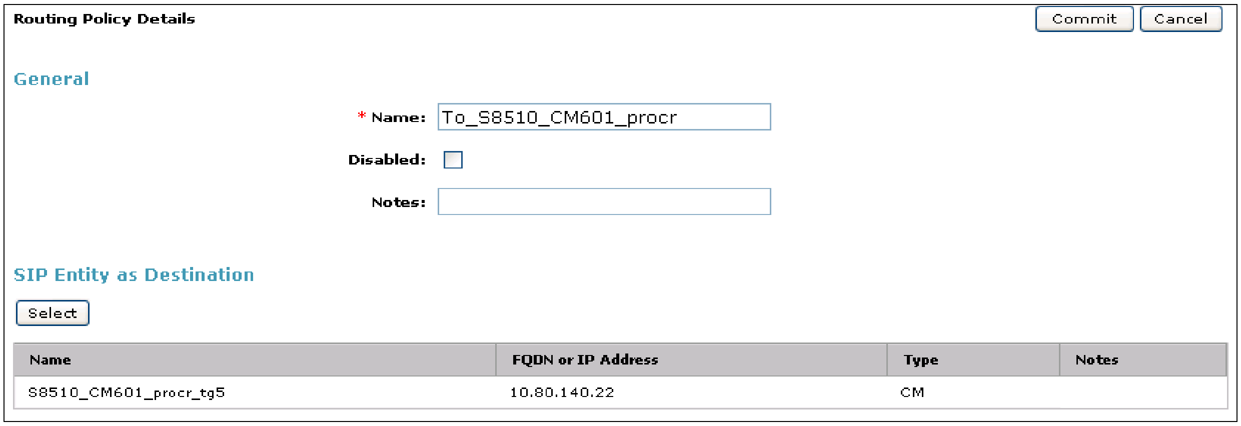
Select : All, None

Figure 15: Routing Policy to Sipera

5.6.2. Routing Policy for Routing to Avaya Aura® Communication Manager

Repeat **Section 5.6.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Communication Manager (**To_S8510_CM601_procr**) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for Communication Manager (**S8510_CM601_procr**) and click on **Select**.
- See **Section 5.7** for the associated Dial Patterns.



Routing Policy Details

General

* Name: To_S8510_CM601_procr

Disabled: □

Notes:

SIP Entity as Destination

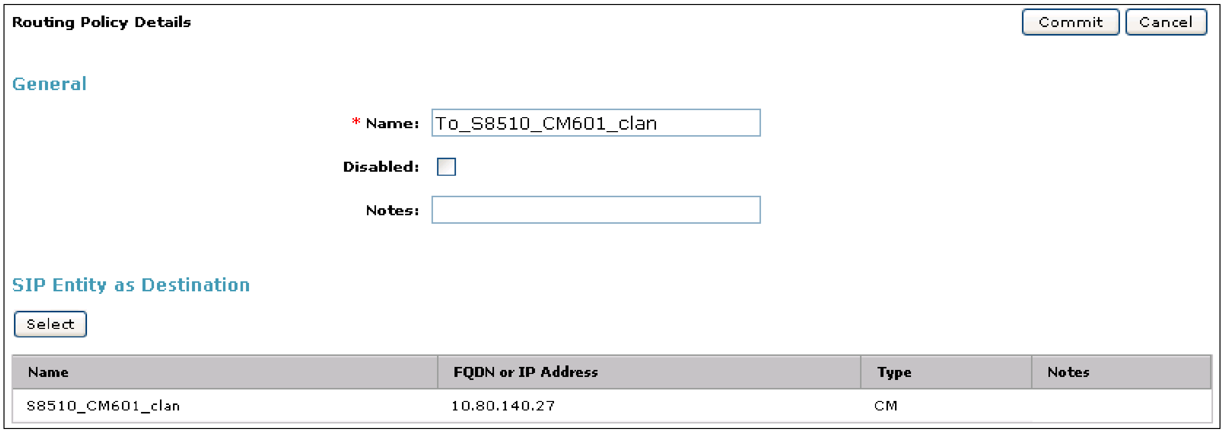
Name	FQDN or IP Address	Type	Notes
S8510_CM601_procr_tg5	10.80.140.22	CM	

Figure 16: Routing Policy to Communication Manager procr

5.6.3. Routing Policy for Outbound calls from SIP Phones

Repeat **Section 5.6.1** with the following differences:

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Communication Manager from SIP phones (S8510_CM601_clan) and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.3** for Communication Manager (**To_S8510_CM601_clan**) and click on "**Select**".
- See **Section 5.7** for the associated Dial Patterns.



Routing Policy Details

General

* Name: To_S8510_CM601_clan

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
S8510_CM601_clan	10.80.140.27	CM	

Figure 17: Routing Policy to Communication Manager Clan

5.7. Dial Patterns

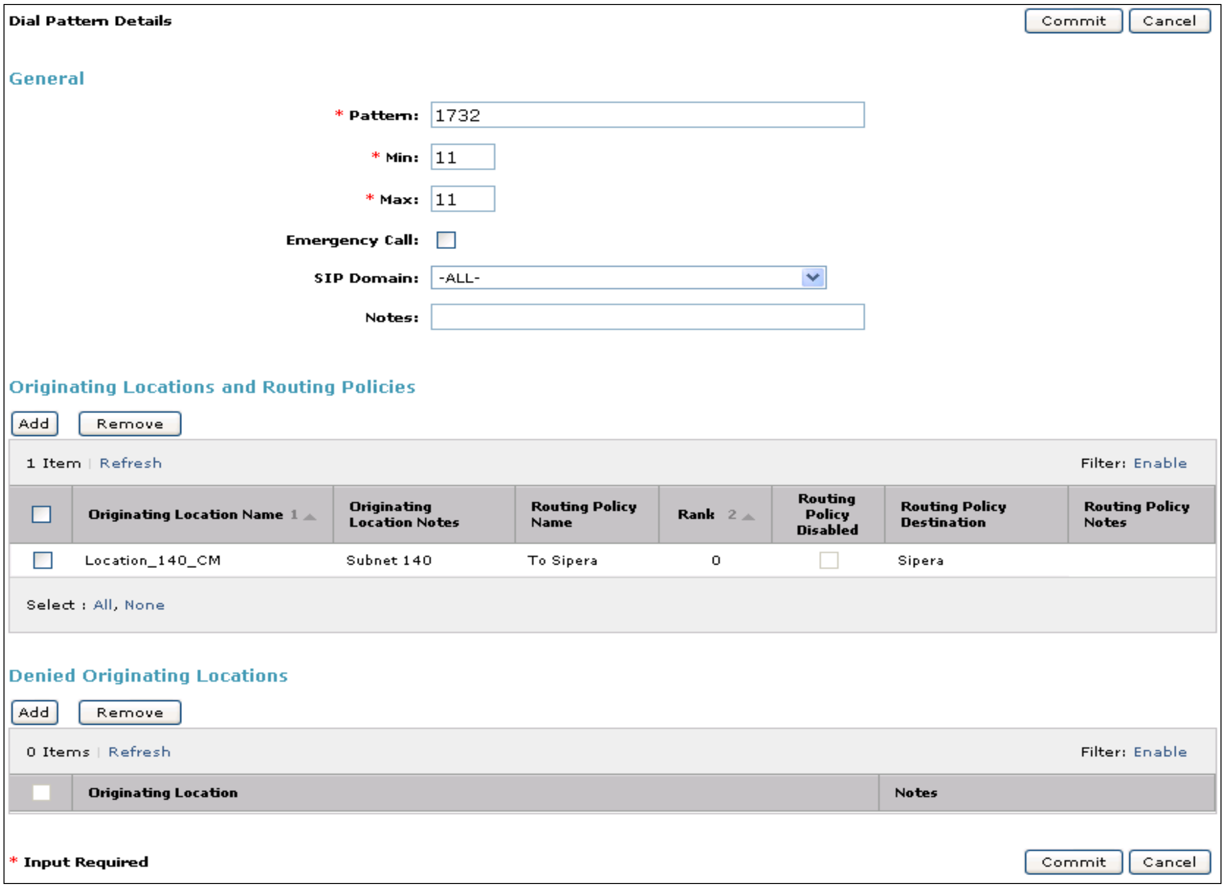
In this section, Dial Patterns are administered matching the following calls:

- Inbound/outbound PSTN calls via AT&T IP Flexible Reach service (5.7.1).
- Calls to/from 10-digit local dial plan numbers associated with extensions on Communication Manager (5.7.2)

5.7.1. Matching Outbound AT&T IP Flexible Reach Service Calls

In this example, pattern 1732 is defined for outbound calls to PSTN numbers starting with 1732xxxxxxx.

1. In the left pane under **Routing**, click on **Dial Patterns**. In the **Dial Patterns** page click on **New** (not shown).
2. In the **General** section of the **Dial Pattern Details** page, provision the following:
    - **Pattern** – Enter matching patterns for outbound dialed digits, **1732**
    - **Min** and **Max** – Enter **11**.
    - **SIP Domain** – Select one of the SIP Domains defined in **Section 5.2** or **-ALL-**, to select all of those 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.
        a. **Note** – As only one domain was administered for the reference configuration (**avayalab.com**), the same result is achieved whether **avayalab.com** or **All** is specified.
    - (Optional) Add any notes as desired.



Dial Pattern Details

General

* Pattern: 1732

* Min: 11

* Max: 11

Emergency Call: □

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

1 Item | Refresh Filter: Enable

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Location_140_CM	Subnet 140	To Sipera	0	□	Sipera	

Select : All, None

Denied Originating Locations

0 Items | Refresh Filter: Enable

□	Originating Location	Notes

* Input Required

Figure 18: Outbound Dial Pattern Example

3. In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on **Add**.
4. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Location_140_CM** (see **Section 5.3**). 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.
5. In the Routing Policies section of the Originating Location and Routing Policy List page, check the checkbox corresponding to the Routing Policy To_Sipera administered for routing calls to the AT&T IP Flexible Reach service in Section 5.6.1.

5.7.2. Matching Inbound Calls to Avaya Aura® Communication Manager

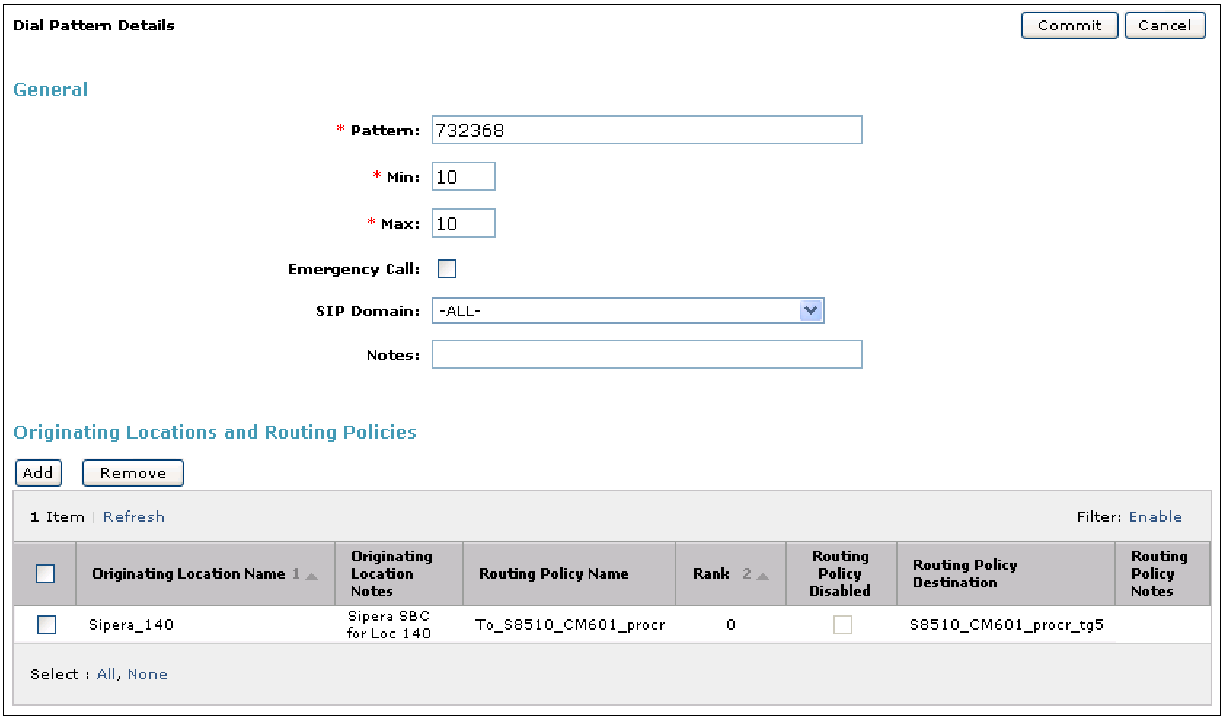
Repeat the steps from **Section 5.7.1** with the following entries for inbound calls to Communication Manager:

- 314332xxxx, 4386, and 732368xxxx (inbound calls from AT&T)

1. In the **General** section of the **Dial Pattern Details** page, provision the following:
   - **Pattern** – In the reference configuration, AT&T sends 10 digit called numbers with the format 732320xxxx. Enter **732320**.
   - **Min** and **Max** – Enter **10**.

- **SIP Domain –ALL**

2. In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Sipera_140**.
3. In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **To_S8510_CM601_procr.**
4. Repeat steps 1 through 3 for the remaining inbound matching dial patterns.
5. Returning to the **Dial Pattern Details** page click on **Commit**.



General

* Pattern:	732368
* Min:	10
* Max:	10
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Sipera_140	Sipera SBC for Loc 140	To_S8510_CM601_procr	0	□	S8510_CM601_procr_tg5	

Figure 19: Inbound Dial Pattern Example

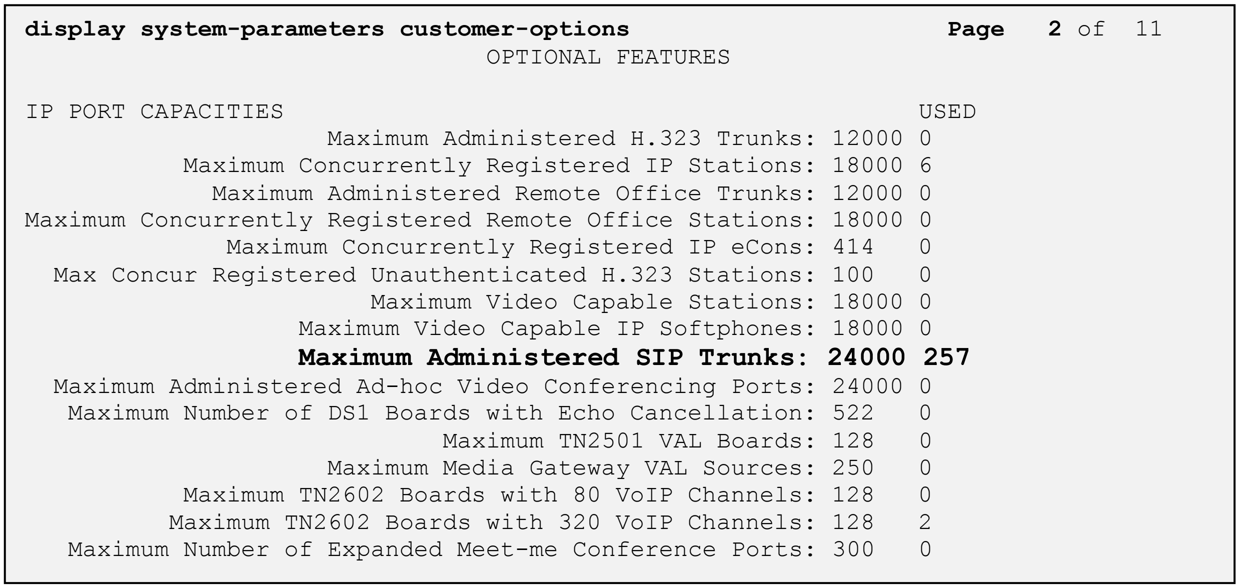
6. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for connecting to Session Manager and ultimately AT&T IP Flexible Reach service. Two SIP trunks are established between Communication Manager and the Session Manager, one for use by signaling traffic (procr interface) and one for use by registered SIP endpoints (Clan interface). It is assumed the general installation of Communication Manager and Avaya G450 has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual public IP addresses of the network elements and public PSTN numbers are not revealed.

6.1. Licensing and Capacity

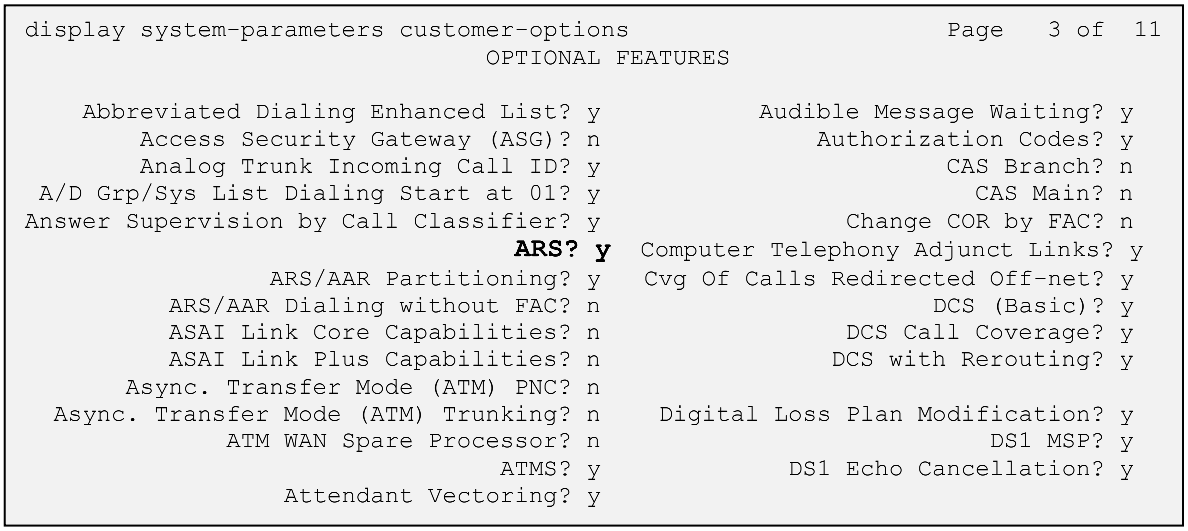
Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **24000** SIP trunks are available and **257** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.



```
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 6
             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 0
                   Maximum Video Capable IP Softphones: 18000 0
                   Maximum Administered SIP Trunks: 24000 257
  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   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

Figure 20: OPTIONAL FEATURES

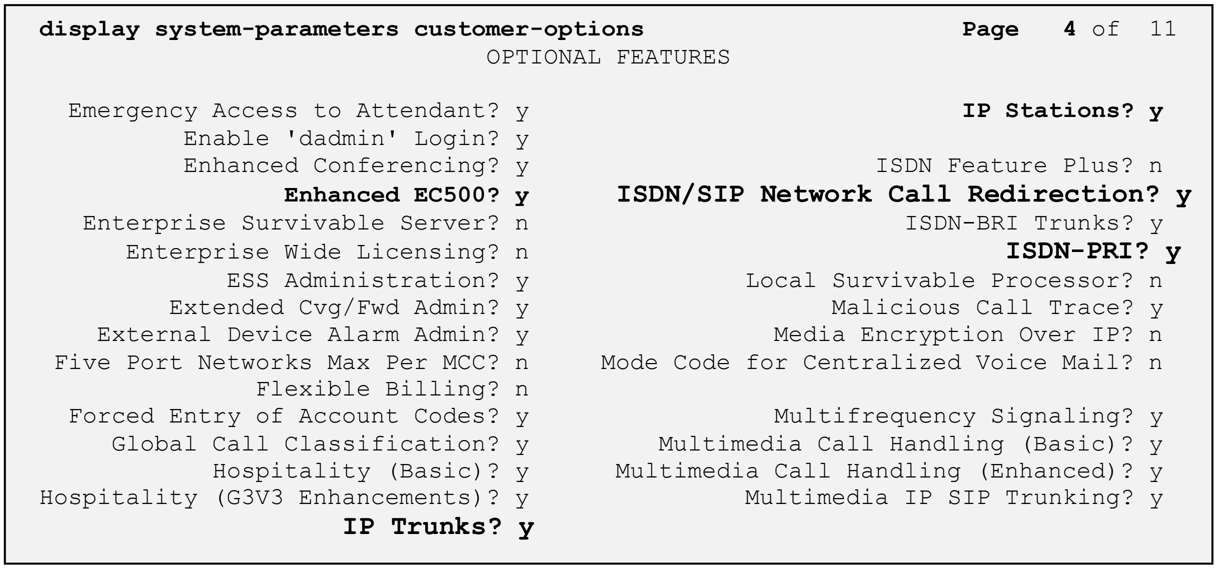
On **Page 3** of the **system-parameters customer-options** form, verify that **ARS** is enabled.



```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                 ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

Figure 21: OPTIONAL FEATURES

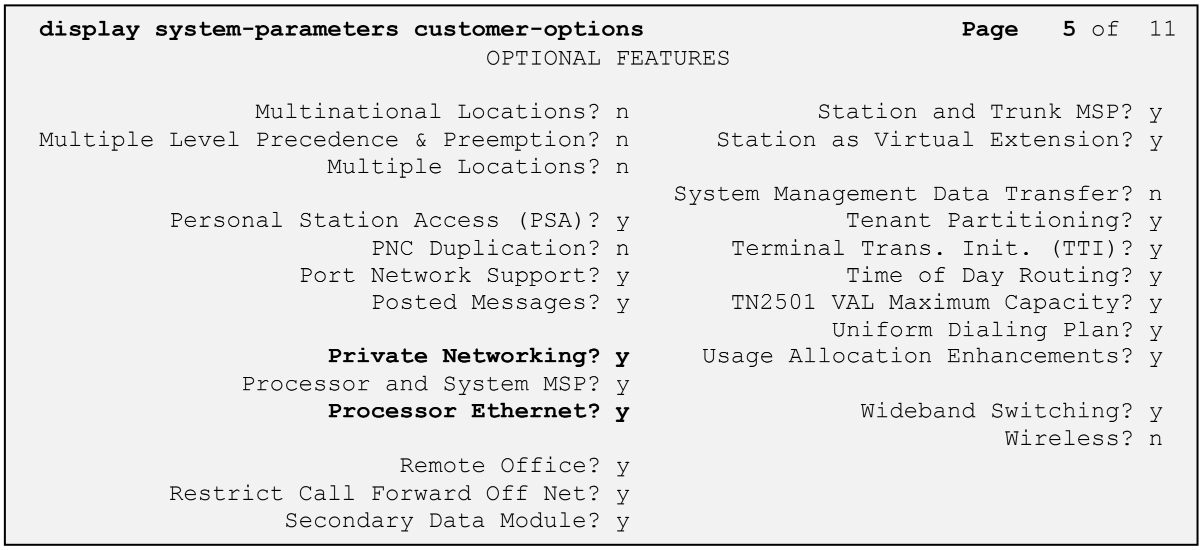
On **Page 4** of the **System-Parameters customer-options** form, verify that **Enhanced EC500**, **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging will be required for the call flows, verify that the **ISDN/SIP Network Call Redirection** feature is enabled.



```
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
```

Figure 22: OPTIONAL FEATURES

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



```
display system-parameters customer-options                      Page   5 of  11
                               OPTIONAL FEATURES

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

Figure 23: OPTIONAL FEATURES

On **Page 6** of the **system-parameters customer-options** form, verify that any required call center features are enabled. In the sample configuration, vectoring is used to refer calls to alternate destinations using SIP NCR (Network Call Redirect). Vector variables are used to include User-User Information (UUI) with the referred calls.

```
display system-parameters customer-options                    Page   6 of  11
                          CALL CENTER OPTIONAL FEATURES
                           Call Center Release: 6.0
                               ACD? y                            Reason Codes? y
                      BCMS (Basic)? y                Service Level Maximizer? n
        BCMS/VuStats Service Level? y              Service Observing (Basic)? y
 BSR Local Treatment for IP & ISDN? y     Service Observing (Remote/By FAC)? y
                 Business Advocate? n              Service Observing (VDNs)? y
                   Call Work Codes? y                            Timed ACW? y
     DTMF Feedback Signals For VRU? y                     Vectoring (Basic)? y
                 Dynamic Advocate? n                  Vectoring (Prompting)? y
     Expert Agent Selection (EAS)? y              Vectoring (G3V4 Enhanced)? y
                         EAS-PHD? y               Vectoring (3.0 Enhanced)? y
                 Forced ACD Calls? n     Vectoring (ANI/II-Digits Routing)? y
              Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
         Lookahead Interflow (LAI)? y                     Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y      Vectoring (Best Service Routing)? y
   Multiple Call Handling (Forced)? y                  Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y              Vectoring (Variables)? y
```

Figure 24: CALL CENTER OPTIONAL FEATURES

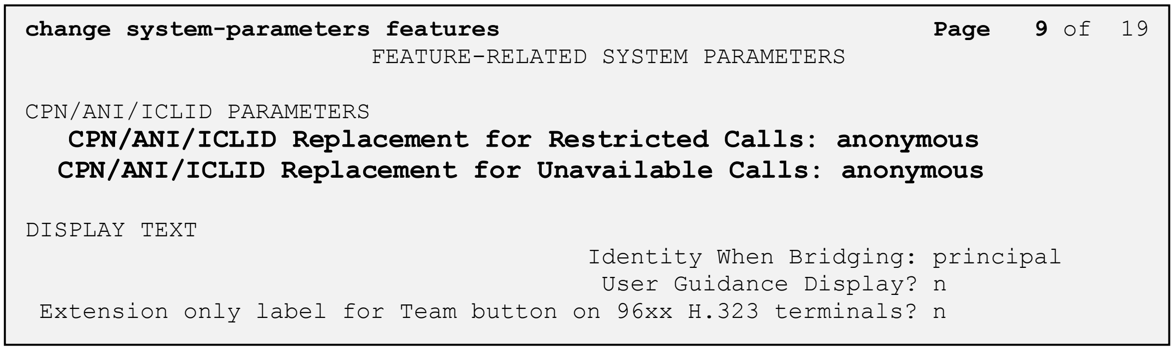
6.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** to allow incoming calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to transfer back to the PSTN then leave the field set to **none**.

```
change system-parameters features                              Page   1 of  19
                              FEATURE-RELATED SYSTEM PARAMETERS
                                 Self Station Display Enabled? n
                                   Trunk-to-Trunk Transfer: all
                 Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                         Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                   AAR/ARS Dial Tone Required? y
```

Figure 25: FEATURE-RELATED SYSTEM PARAMETERS

On **Page 9,** verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both.

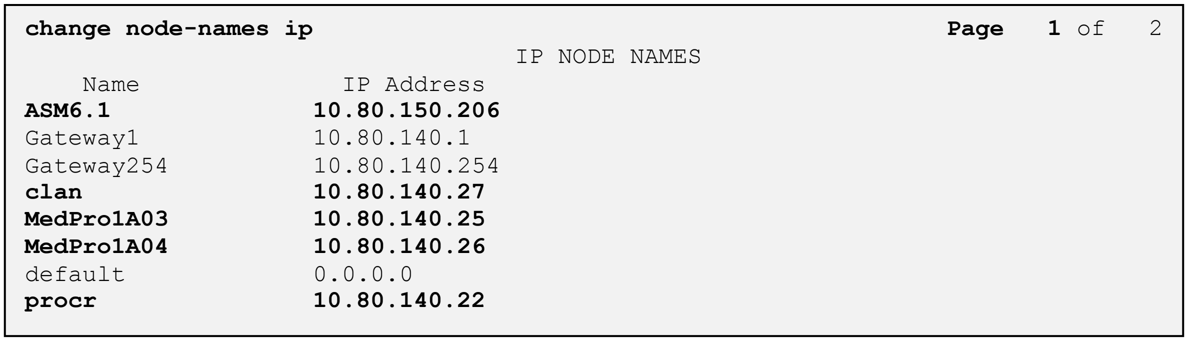


```
change system-parameters features                               Page   9 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

CPN/ANI/ICLID PARAMETERS
   CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous

DISPLAY TEXT
                                       Identity When Bridging: principal
                                        User Guidance Display? n
 Extension only label for Team button on 96xx H.323 terminals? n
```

Figure 26: FEATURE-RELATED SYSTEM PARAMETERS

6.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been defined for the IP addresses of the Clan of the G650, the PROCR interface of the Avaya Server running Communication Manager and for the Session Manager. These node names will be needed for defining the service provider signaling group in **Section 6.8**.



```
change node-names ip                                             Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
ASM6.1              10.80.150.206
Gateway1            10.80.140.1
Gateway254          10.80.140.254
clan                10.80.140.27
MedPro1A03          10.80.140.25
MedPro1A04          10.80.140.26
default             0.0.0.0
procr               10.80.140.22
```

Figure 27: IP NODE NAMES

6.4. IP Interface for procr

The **add ip-interface procr** or **change ip-interface procr** command can be used to configure 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.

```
change 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: 10.80.140.22

           Subnet Mask: /24
```

Figure 28: IP INTERFACES

The output for the **list registered-ip stations** shows that IP endpoint registrations are to the **Clan**.

```
 list registered-ip-stations
                              REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
7689          9620      IP_Phone    y  10.80.140.99
              1         6.010f         10.80.140.27
7690          9630      IP_Phone    y  10.80.140.98
              1         6.010f         10.80.140.27
7691          9630      IP_Phone    y  10.80.140.95
              1         6.010f         10.80.140.27
7692          9650      IP_Phone    y  10.80.140.97
              1         3.102S         10.80.140.27
7693          9630      IP_Phone    y  10.80.140.96
              1         3.102S         10.80.140.27
```

Figure 29: REGISTERED IP STATIONS

6.5. G450 Media Gateway

In the reference configuration an Avaya G450 Media Gateway is used for media resources and to support various interface cards (e.g. MM711 Analog card). The G450 registers to Communication Manager. This requires provisioning on both Communication Manager and the G450.

6.5.1. G450 Provisioning for Registration to Communication Manager

1. Log into the G450 (via console or network connections) using appropriate credentials. Note that the console prompt will appear similar to **G450-???#,** where **???** means the G450 is not registered. Once the G450 registers, the prompt will change to **G450-001#** (where 001 is the Media Gateway reference number provisioned in Communication Manager (see **Section 6.5.2**).

2. Enter **set mgc list x.x.x.x**, where **x.x.x.x** is the IP address of the Communication Manager Procr (e.g. 10.80.140.22)

3. Enter **show system** and note the G450 serial number. This will be used to provision the G450 on Communication Manager.

```
 G450-001(super)# show system
System Name                 :
System Location             :
System Contact              :
Uptime (d,h:m:s)            : 36,05:29:11
Call Controller Time        : 13:23:15 02 JUL 2011
Serial No                   : 11N510737929
 Model                      : G450
HW Ready for FIPS           : No
Chassis HW Vintage          : 1
Chassis HW Suffix           : A
Mainboard HW Vintage        : 2
Mainboard HW Suffix         : B
```

Figure 30: G450 system

6.5.2. Communication Manager Provisioning for the G450

1. Enter **add media gateway x**, where **x** is the next available Media Gateway reference number (e.g. **1**).
2. Enter **Type: G450**
3. Enter a descriptive name.
4. Enter the G450 Serial Number from **Section 6.5.1**.
5. Enter a network Region (e.g. **1**).
6. Leave other values to default (these other values may be changed for other configurations beyond the scope of this document).

Once the G450 is registered the **Registered?** field will change from **n** to **y** and other fields will self-populate.

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

                   Type: g450
                   Name: G450
              Serial No: 11N510737929
           Encrypt Link? y                  Enable CF? n
         Network Region: 1                   Location: 1
                                            Site Data:
          Recovery Rule: 1

             Registered?  y
  FW Version/HW Vintage: 31 .18 .1  /1
       MGP IPV4 Address: 10.80.140.15
       MGP IPV6 Address:
  Controller IP Address: 10.80.140.22
            MAC Address: b4:b0:17:90:8c:30
```

Figure 31: MEDIA GATEWAY 1

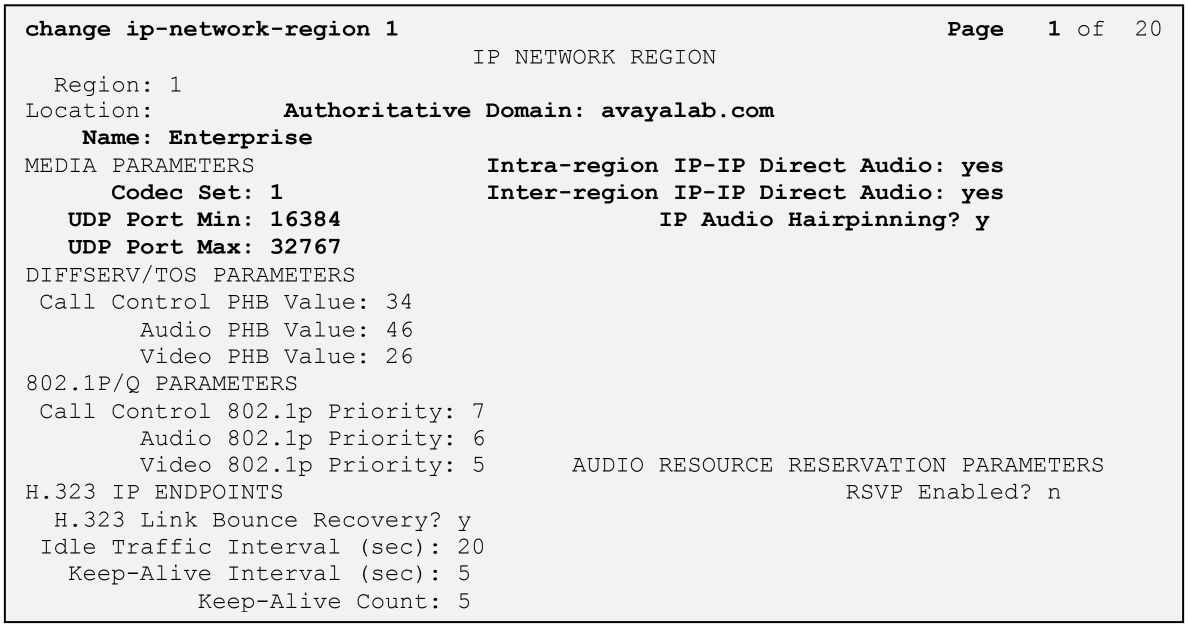
6.6. IP Network Region

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.

6.6.1. IP Network Region 1 – Enterprise Region

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

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avayalab.com**. This name appears in the "From" header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field (e.g. **Enterprise**).
- Enable **IP-IP Direct Audio** (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Set both **Intra-region** and **Inter-region IP-IP Direct Audio** to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- **UDP Port Min**: - Set to **16384 (AT&T requirement).**
- **UDP Port Max**: - Set to **32767 (AT&T requirement).**
- Set the **Codec Set** field to the IP codec set defined in **Section 6.7**
- Default values can be used for all other fields.



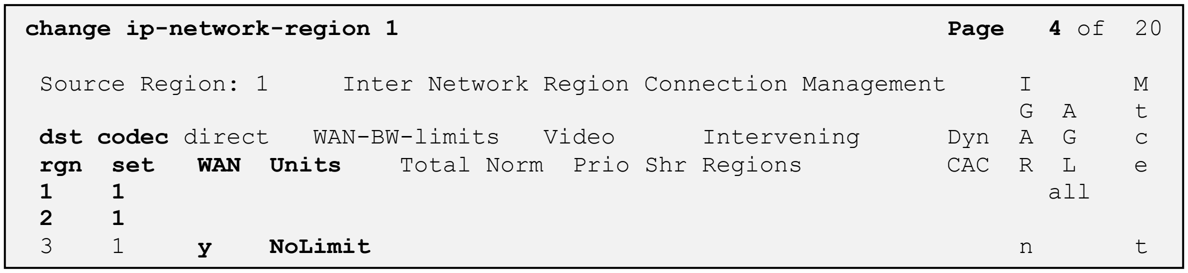
```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avayalab.com
    Name: Enterprise
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 16384                      IP Audio Hairpinning? y
   UDP Port Max: 32767
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 34
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 7
        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
```

Figure 32: IP NETWORK REGION 1

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 **1** (this means Region 1 is permitted to talk to region 2 and they will use codec set 1 to do so). The **WAN** and **Units** columns will self populate with **Y** and **No Limit**.
- 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    1
 3    1     y    NoLimit                                             n       t
```

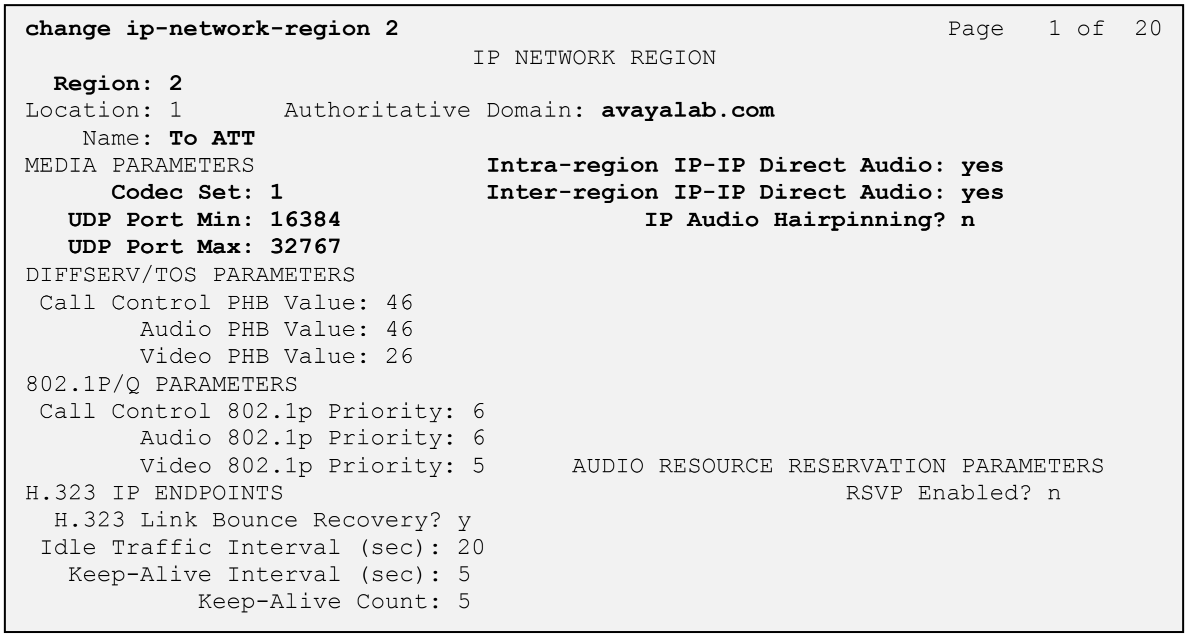
Figure 33: Inter Network Region Connection Management

6.6.2. IP Network Region 2 – AT&T Region

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

1. Repeat the steps in Section 6.6.1 with the following changes:

- Page 1
  a. Enter a descriptive name (e.g. **To ATT**)
  b. Enter 1 for the Codec Set parameter.



```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avayalab.com
    Name: To ATT
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
```

Figure 34: IP NETWORK REGION 2

- Page 4
  a. Verify that codec **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    1     y    NoLimit                                              n       t
 2    1                                                                 all
 3
```

Figure 35: Inter Network Region Connection Management

6.7. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, codecs G.729 and G.711MU were tested using ip-codec-set 1. To use these codecs, enter **G.729** and **G.711MU** in the **Audio Codec** column of the table in the order of preference. Default values can be used for all other fields. Silence suppression is normally set to **n** and packet size is standard at **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.729           n          2        20
 2: G.711MU         n          2        20
```

Figure 36: IP Codec Set

On **Page 2**, set **Fax** to **t.38-standard** for fax support.

```
change ip-codec-set 1                                           Page   2 of   2
                          IP Codec Set
                              Allow Direct-IP Multimedia? n
                Mode                 Redundancy
    FAX         t.38-standard         0
    Modem       off                   0
    TDD/TTY     US                    3
    Clear-channel   n                 0
```

Figure 37: IP Codec Set

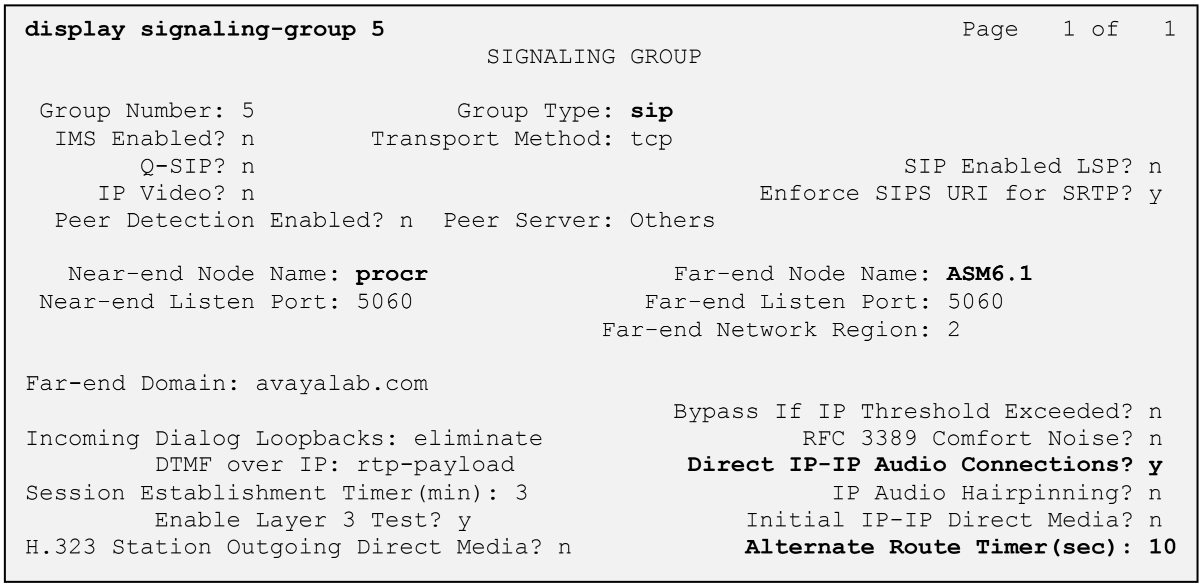
Note: Although a 20ms ptime with the G729 codec is the default on Communication Manager and is supported, there is a substantial bandwidth savings when using a ptime of 30ms with the G729 codec on AT&T VPN (AVPN) Transport.

6.8. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Session Manager. This signaling group will be used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 5 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). For ease of troubleshooting during testing, part of the compliance test was conducted with the **Transport Method** set to **tcp**. The transport method specified here is used between the Communication Manager and Session Manager.
- If desired the **Peer Detection Enabled** can be set to **y** and the **Peer Server** set to **SM** if desired. This will prepend outgoing phone numbers with the + sign.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061 and for TCP the well-known port value is 5060). The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5060**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of the PROCR as defined in the **node-names ip** screen shot in **section 6.3**.
- Set the **Far-end Node Name** to **ASM6.1**. This node name maps to the IP address of the Session Manager interface as defined in the **node-names ip** screen shot in **Section 6.3**.
- Set the **Far-end Network Region** to the IP network region for the service provider in **Section 6.6**.
- Set the **Far-end Domain** to the domain of the enterprise (usually an IP Address or a domain name) – here **avayalab.com** is used.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint.
- Set **Initial IP-IP Direct Media** to **n**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. Both Direct and Initial IP-IP Direct Media need to be set as indicated for Early Media to be Enabled.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **10**. This defines the number of seconds the that Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

Signaling group from the **procr** interface to Session Manager.



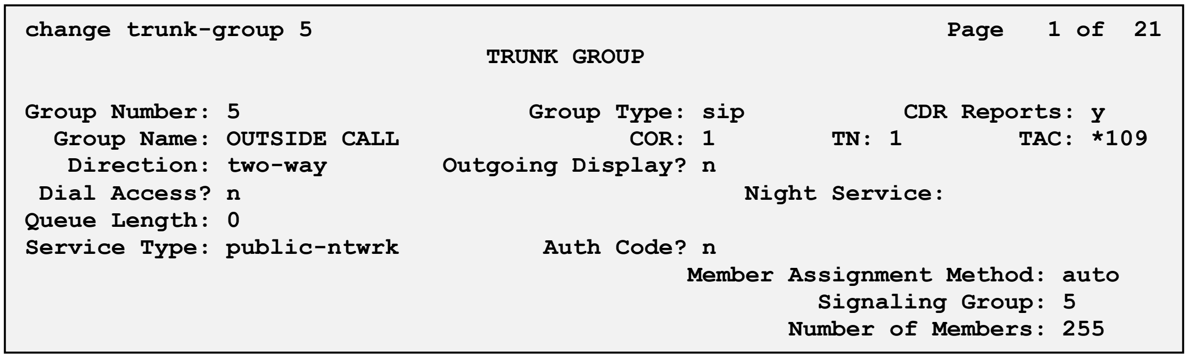
```
display signaling-group 5                                       Page   1 of   1
                                SIGNALING GROUP

 Group Number: 5              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? n  Peer Server: Others

   Near-end Node Name: procr                 Far-end Node Name: ASM6.1
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 2

Far-end Domain: avayalab.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): 10
```

Figure 38: SIGNALING GROUP

6.9. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 6.8**. For the compliance test, trunk group 5 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group shown in the previous step.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.
- Default values were used for all other fields.

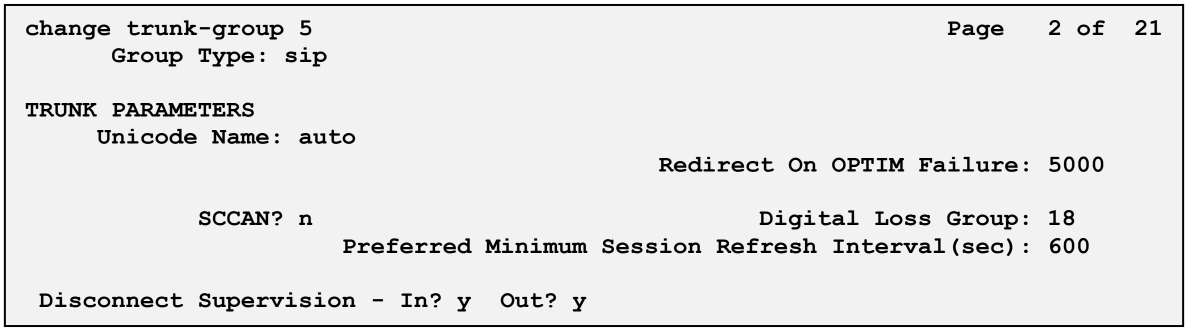


```
change trunk-group 5                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 5                   Group Type: sip          CDR Reports: y
  Group Name: OUTSIDE CALL               COR: 1        TN: 1        TAC: *109
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 5
                                                     Number of Members: 255
```

Figure 39: TRUNK GROUP

On **Page 2**, the **Redirect On OPTIM Failure** value is the amount of time (in milliseconds) that Communication Manager will wait for a response (other than 100 Trying) to a pending INVITE sent to an EC500 remote endpoint before selecting another route. If another route is not defined, then the call is cancelled after this interval. This time interval should be set to a value comparable to the **Alternate Route Timer** on the signaling group form described in **Section 6.8**.

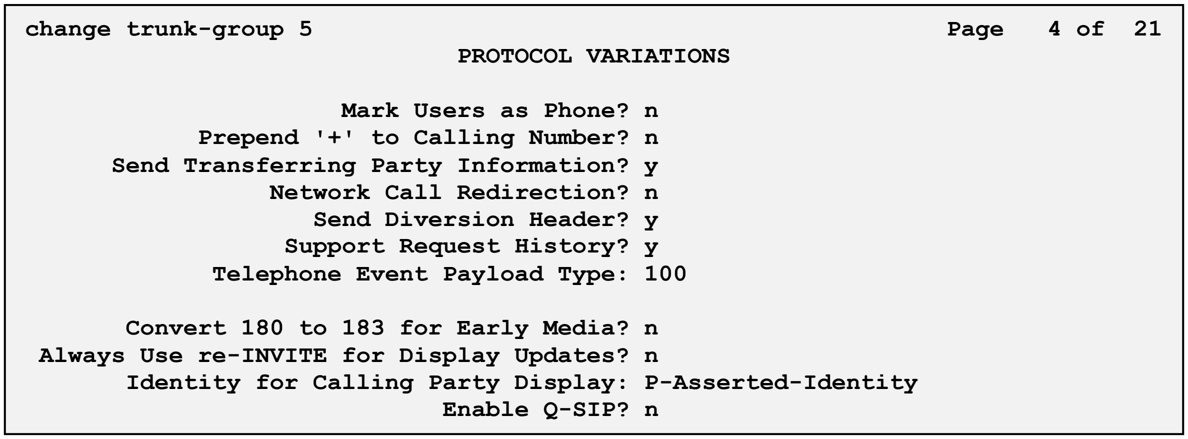
Verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **5000** milliseconds was used.



```
change trunk-group 5                                            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): 600

 Disconnect Supervision - In? y  Out? y
```

Figure 40: TRUNK GROUP

On **Page 4**, the **Network Call Redirection** field must be set to **n** as stated in **Section 2.2**. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios. Set the **Telephone Event Payload Type** to **100**, the value preferred by AT&T IP Flexible Reach.



```
change trunk-group 5                                            Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y
                 Network Call Redirection? n
                    Send Diversion Header? y
                  Support Request History? y
             Telephone Event Payload Type: 100

       Convert 180 to 183 for Early Media? n
 Always Use re-INVITE for Display Updates? n
       Identity for Calling Party Display: P-Asserted-Identity
                             Enable Q-SIP? n
```

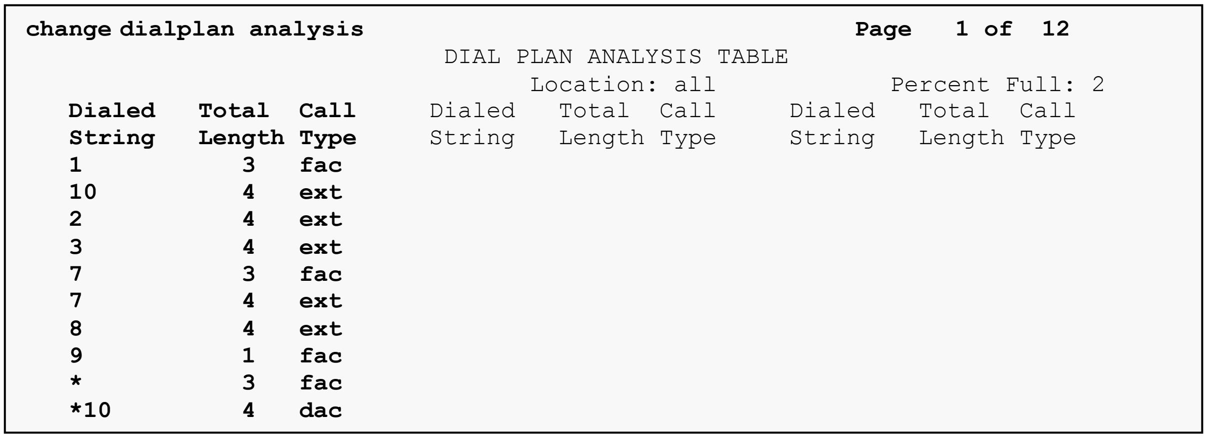
Figure 41: PROTOCOL VARIATIONS

6.10. Dial Plan

6.10.1. Global Dial Plan Settings

Enter the **change dialplan analysis** command to provision the dial plan.

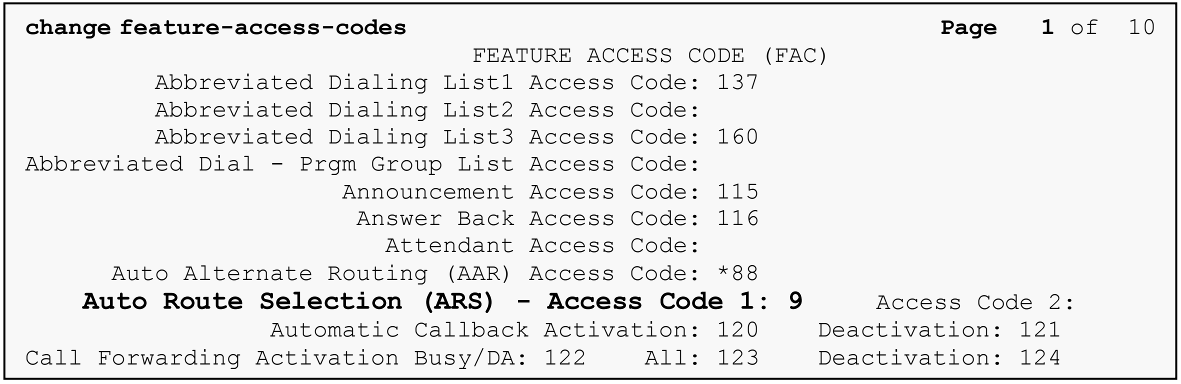
- 4-digit dial access codes (indicated with a **Call Type** of **dac**) beginning with the digit ***10** (e.g. Trunk Access Codes (TACs) defined for trunk groups in this reference configuration conform to this format).
- 4-digit extensions with a **Call Type** of **ext** beginning with the digits **7xxx** (e.g. Local extensions for Communication Manager stations, agents, and Vector Directory Numbers (VDNs) in this reference configuration conform to this format).
- 1-digit facilities access code (indicated with a **Call Type** of **fac**) (e.g. **9** access code for outbound ARS dialing and **8** for AAR local dialing).
- 3-digit facilities access codes (e.g. * and # for Agent logon/logoff).



```
change dialplan analysis                                  Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all            Percent Full: 2
   Dialed    Total  Call      Dialed   Total  Call      Dialed   Total  Call
   String    Length Type      String   Length Type      String   Length Type
   1           3    fac
   10          4    ext
   2           4    ext
   3           4    ext
   7           3    fac
   7           4    ext
   8           4    ext
   9           1    fac
   *           3    fac
   *10         4    dac
```

Figure 42: DIAL PLAN ANALYSIS TABLE

Use the **change feature-access-codes** command to configure ***9*** as the **Auto Route Selection (ARS) – Access Code 1**.



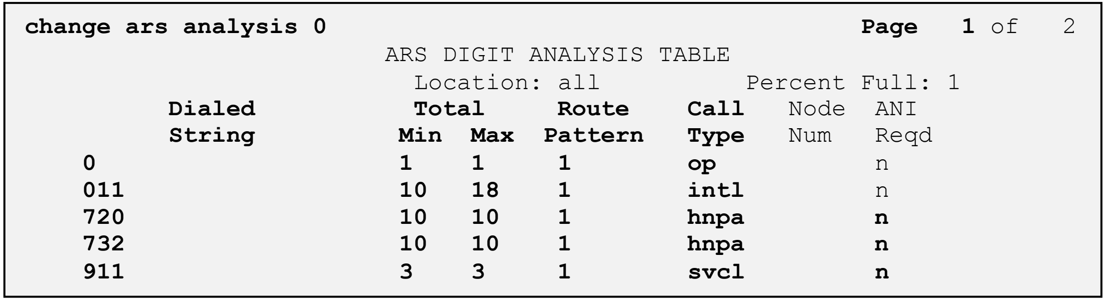
```
change feature-access-codes                                     Page   1 of  10
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: 137
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code: 160
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: 115
                       Answer Back Access Code: 116
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *88
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: 120    Deactivation: 121
Call Forwarding Activation Busy/DA: 122    All: 123    Deactivation: 124
```

Figure 43: FEATURE ACCESS CODE (FAC)

6.10.2. Outbound Dial Settings

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the Session Manager. In the sample configuration, the single digit 9 is used as the ARS access code. Enterprise callers will dial 9 to reach an "outside line". This common configuration is illustrated below with little elaboration.

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. The example below shows a subset of the dialed strings tested as part of the compliance test. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the Session Manager (as defined next).



```
change ars analysis 0                                         Page   1 of   2
                         ARS DIGIT ANALYSIS TABLE
                           Location: all          Percent Full: 1
          Dialed            Total     Route     Call   Node  ANI
          String           Min  Max  Pattern    Type   Num   Reqd
    0                      1    1      1        op           n
    011                    10   18     1        intl         n
    720                    10   10     1        hnpa         n
    732                    10   10     1        hnpa         n
    911                    3    3      1        svcl         n
```

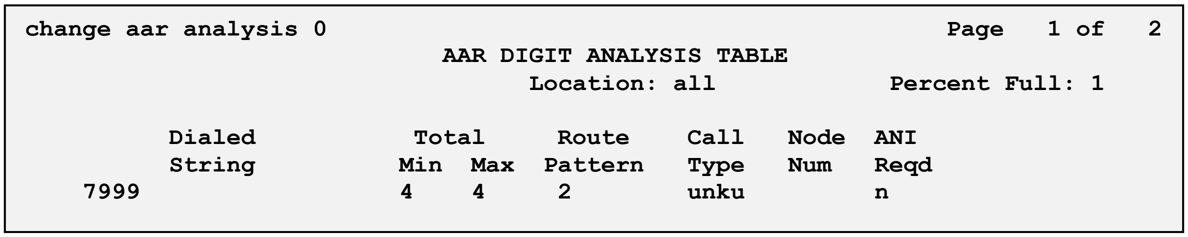
Figure 44: ARS DIGIT ANALYSIS TABLE

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for the service provider trunk route pattern in the following manner. The example below shows the values used for route pattern 1 during the compliance test.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter the outbound trunk group for the Session Manager. For the compliance test, trunk group 5 was used.
- **FRL**: Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk**: **4** The prefix mark (**Pfx Mrk**) of four suppress a user-dialed prefix digit 1. Used, for example, when calls route to a server that rejects calls with a prefix digit 1.
- **LAR**: **next**

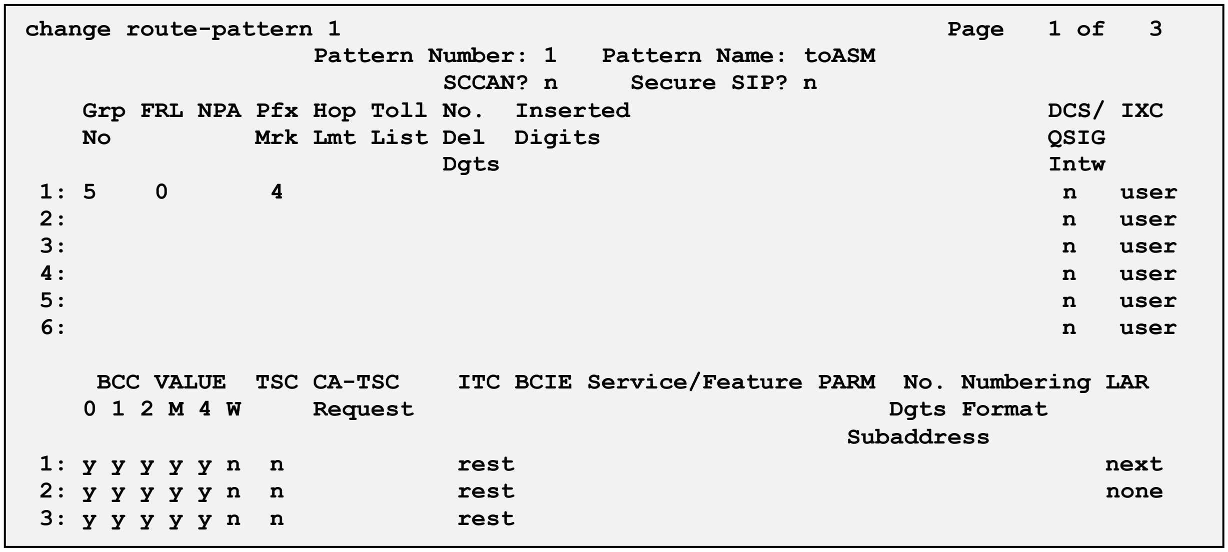
The AAR table is selected based on the caller dialing the AAR access code (e.g. "*88") as defined in **Section 6.10.1**. The access code is removed and the AAR table matches the remaining dialed digits and sends then to the designated route-pattern.

- 1. In the **Dialed String** column enter **7999**.
- 2. In the **Min** and **Max** columns enter the corresponding matching digit lengths, (e.g. **4** and **4**).
- 3. In the Route Pattern column select a route-pattern to be used for these calls (e.g.**2**).
- 4. In the **Call Type** column 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
    7999                  4    4     2        unku         n
```

Figure 45: AAR DIGIT ANALYSIS TABLE



```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: toASM
                             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: 5    0       4                                                      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                                         next
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest
```

Figure 46: ROUTE PATTERN

6.10.3. Outbound Number Presentation

For AT&T Flexible Reach service call admission control purposes, calling number origination SIP header contents (e.g. From, Contact, and PAI) are converted to public numbers (previously identified by AT&T), instead of Communication Manager local extensions. However, Avaya Modular Messaging looks for Communication Manager extensions in these headers for mail-box processing. These functions may be accomplished using the Communication Manager **private-numbering** form.

1. Converting Communication Manager extensions to AT&T DIDs.

Using the **change private -numbering 0** command, enter.

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. **4**).
- **Ext Code –** Enter the Communication Manager extension (e.g. **7691**).
- **Trk Grp(s)** – Enter the number of the AT&T trunk group (e.g. **5**).
- **CPN Prefix** – Enter the corresponding AT&T DID (e.g **7323680193**) used for the specified extension (e.g. **7691**).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g. **10**).

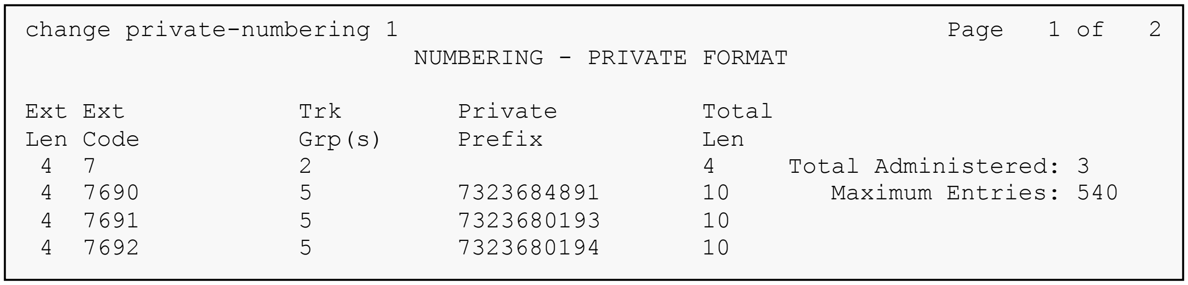
2. Repeat Step 1 for each extension/DID conversion required.

3. Passing Communication Manager extensions to Modular Messaging.

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. **4**)

- **Ext Code –** Enter the broadest wildcard match necessary to cover extensions with coverage to Modular Messaging (e.g. **7** to cover the provisioned extension range 4xxxx)
- **Trk Grp(s)** – Enter the number of the Local trunk group (e.g. **2**).
- **CPN Prefix** – Leave blank.
- **CPN Len** – Enter the total number of extension digits (e.g. **4**).

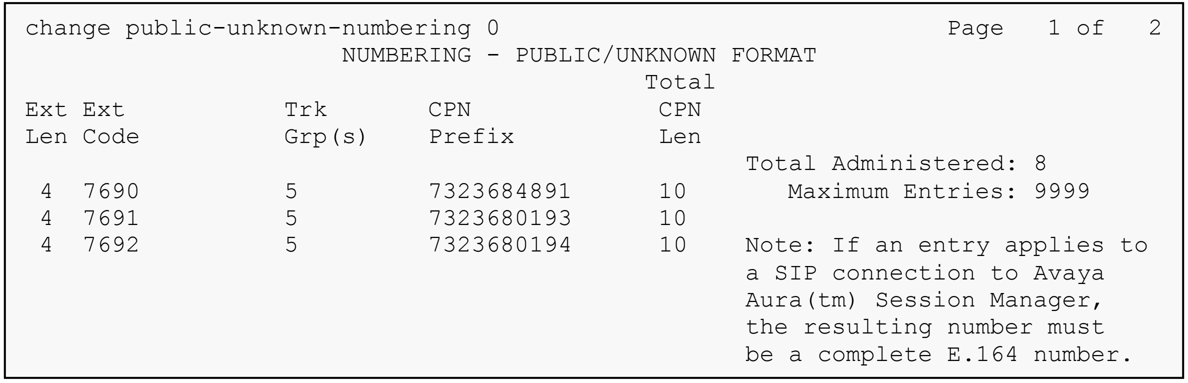
For example any extension beginning with 7 and 4 digits long will remain unchanged for trunk 2 (Modular Messaging processing). However, when 4 digit extension 7691 calls out to Session Manager, the originating number will be converted to 7323680193 .



```
change private-numbering 1                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 4  7                2                           4     Total Administered: 3
 4  7690             5          7323684891       10       Maximum Entries: 540
 4  7691             5          7323680193       10
 4  7692             5          7323680194       10
```

Figure 47: NUMBERING – PRIVATE FORMAT

Communication Manager Diversion Header processing (see **Section 6.9**) uses the contents of the public-unknown-numbering form to populate the calling number field. Therefore any extension to AT&T DID conversions specified in the private-numbering form should be specified in the public-unknown-numbering table as well.

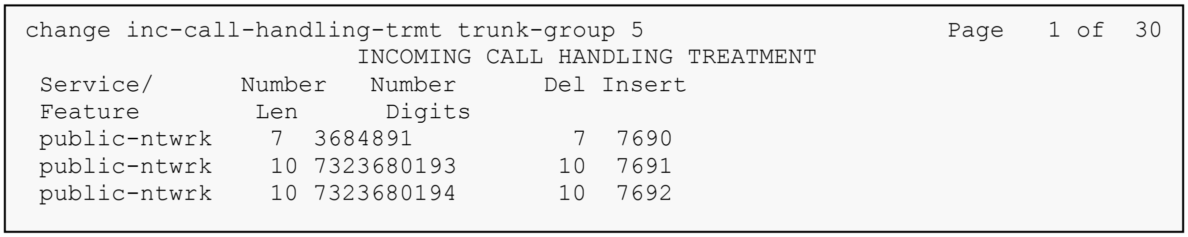


```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                          Total
Ext Ext             Trk       CPN          CPN
Len Code            Grp(s)    Prefix       Len
                                                 Total Administered: 8
 4  7690            5         7323684891      10      Maximum Entries: 9999
 4  7691            5         7323680193      10
 4  7692            5         7323680194      10     Note: If an entry applies to
                                                 a SIP connection to Avaya
                                                 Aura(tm) Session Manager,
                                                 the resulting number must
                                                 be a complete E.164 number.
```

Figure 48: NUMBERING - PUBLIC/UNKNOWN FORMAT

6.10.4. Inbound Dial Settings

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. This can also be done on Session Manager with an Adaptation. The number sent by AT&T IP Flexible Reach can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of the number **732-368-0193** to extension **7691**.



```
change inc-call-handling-trmt trunk-group 5                     Page   1 of  30
                       INCOMING CALL HANDLING TREATMENT
 Service/      Number   Number      Del Insert
 Feature        Len      Digits
 public-ntwrk    7  3684891           7  7690
 public-ntwrk    10 7323680193       10  7691
 public-ntwrk    10 7323680194       10  7692
```

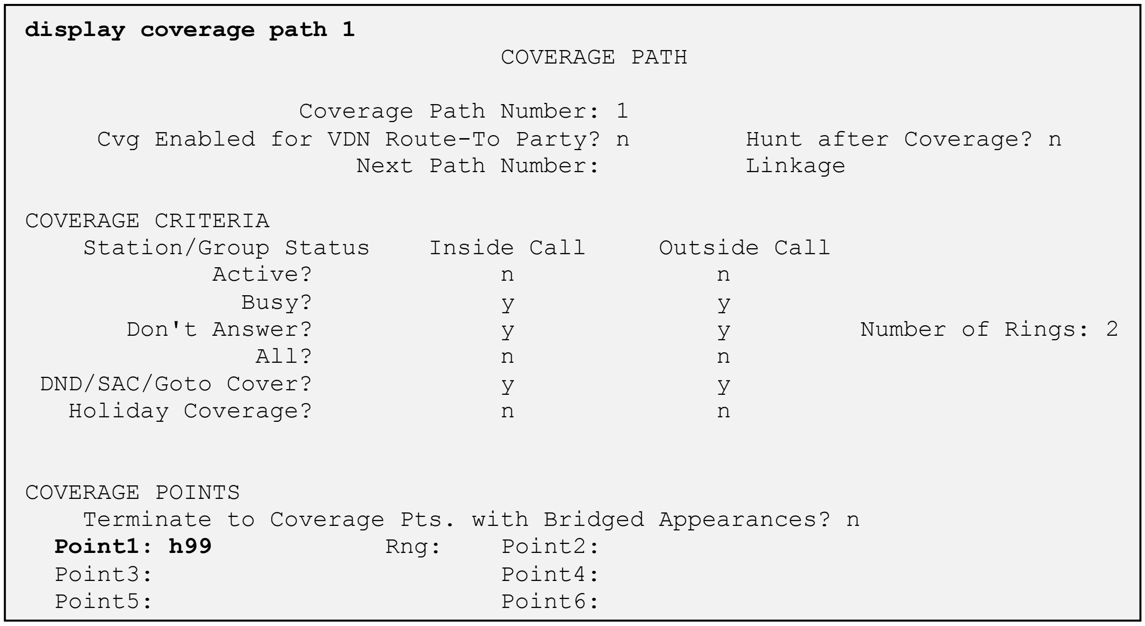
Figure 49: INCOMING CALL HANDLING TREATMENT

6.11. Modular Messaging Configuration

Although not specifically related to AT&T IP Flexible Reach, this section shows the hunt group used for access to Avaya Modular Messaging. In the sample configuration, users with voice mail have a coverage path containing hunt group 99. Users can dial extension 7999 to reach Modular Messaging (e.g., for message retrieval

Note - The administration of Communication Manager Call Center elements – hunt groups, vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes.

Hunt group 99 is used in the reference configuration to verify Modular Messaging coverage functionality. The hunt group (e.g. **99**) is defined with the 4 digit Modular Messaging pilot number (e.g. **7999**). The hunt group is associated with a coverage path (e.g.**h99**) and the coverage path is assigned to a station (e.g. **7691**). Communication Manager will use the AAR access code ***88** (defined in **Section 6.10.2**) to dial Modular Messaging (e.g. 7999).



```
display coverage path 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: 2
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h99             Rng:    Point2:
  Point3:                         Point4:
  Point5:                         Point6:
```

Figure 50: COVERAGE PATH

```
display hunt-group 99                                           Page   1 of  60
                                  HUNT GROUP

            Group Number: 99                               ACD? n
              Group Name: MM                             Queue? n
         Group Extension: 7999                          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
```

Figure 51: HUNT GROUP

```
display hunt-group 99                                           Page   2 of  60
                                  HUNT GROUP

                      Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle          Routing Digits
                                                   (e.g., AAR/ARS Access Code)
     7999                      MM                         *88
```

Figure 52: HUNT GROUP

```
display station 7691                                            Page   1 of   5
                                     STATION

Extension: 7691                         Lock Messages? n               BCC: 0
     Type: 9630                         Security Code: 1234             TN: 1
     Port: S00012                     Coverage Path 1: 1               COR: 1
     Name: 9608                       Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 7691
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n
```

Figure 53: STATION 7691

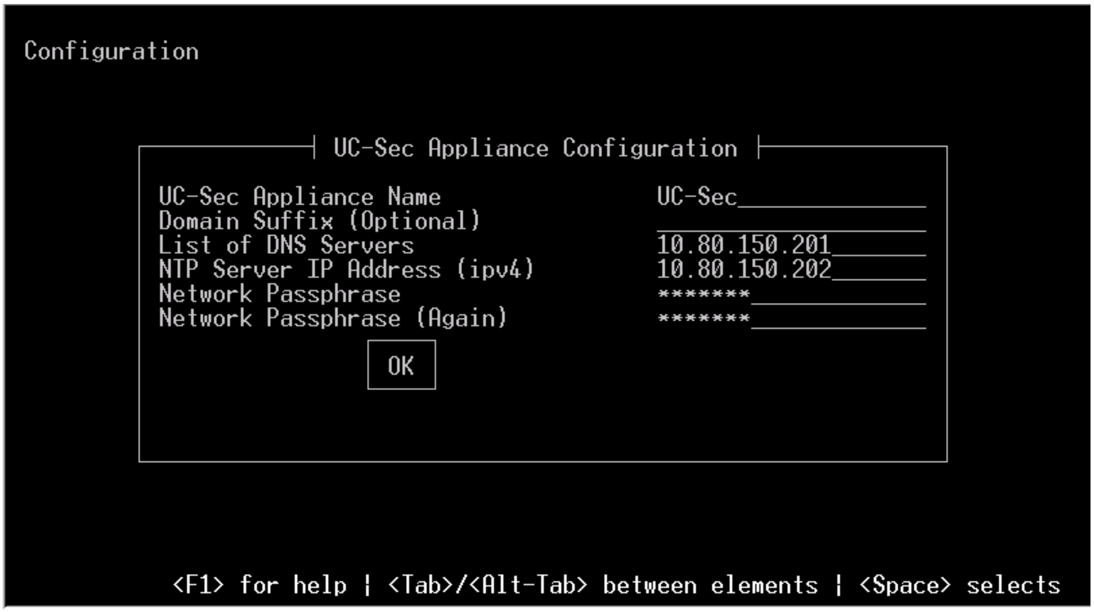
7. Sipera E-SBC Configuration

7.1. Initial Installation

The following sections describe the provisioning of the Sipera E-SBC. Only the Sipera provisioning required for the reference configuration is described in these Application Notes.

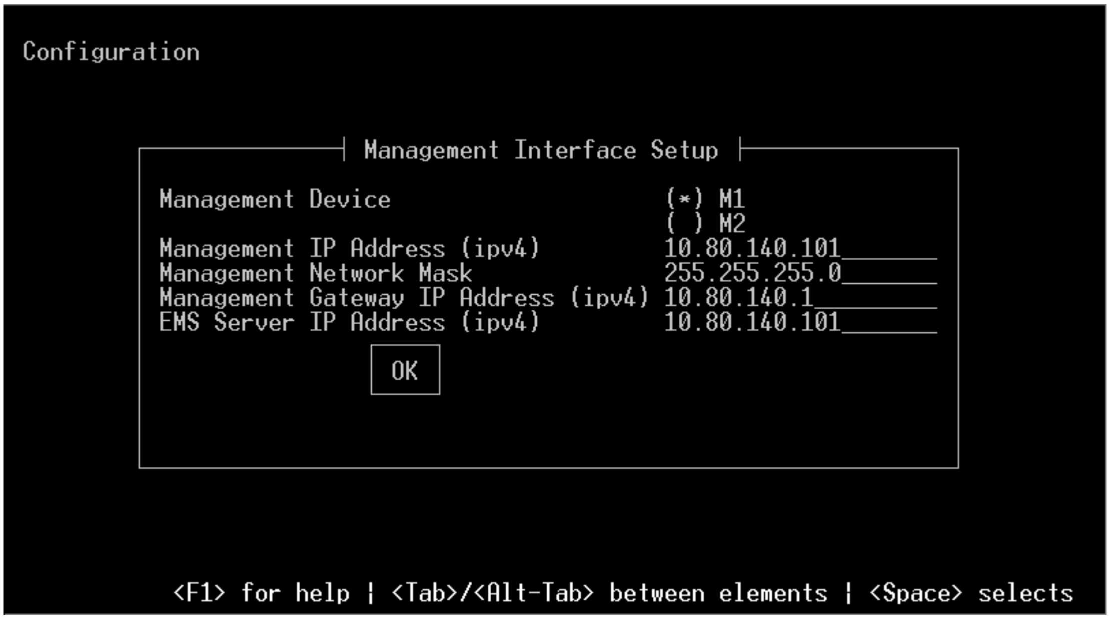
The standalone Sipera E-SBC was configured via a serial console port connection and via an IP connection once the basic system config was completed. The following are the steps for configuring the basic configuration:

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.
5. A DOS-based menu will appear.
6. Select **UC Sec Configuration (See Figure 54)**
7. In Installation Type: **EMS + UC-SEC** (for single-box installations, see **Figure 55**)
8. Select **EMS + UC SEC Appliance Config**
9. Continue through the menus and fill in the appropriate information, as in **Figure 56** and **Figure 57**.
10. You are returned to the main menu
11. Select **Done** (not shown).
12. The box will be rebooted, and once it is done, it will prompt you for the password for "root" and then user "ipcs". Enter appropriate passwords for each.
13. The initial installation is complete and any further configuration will be done in the web interface.



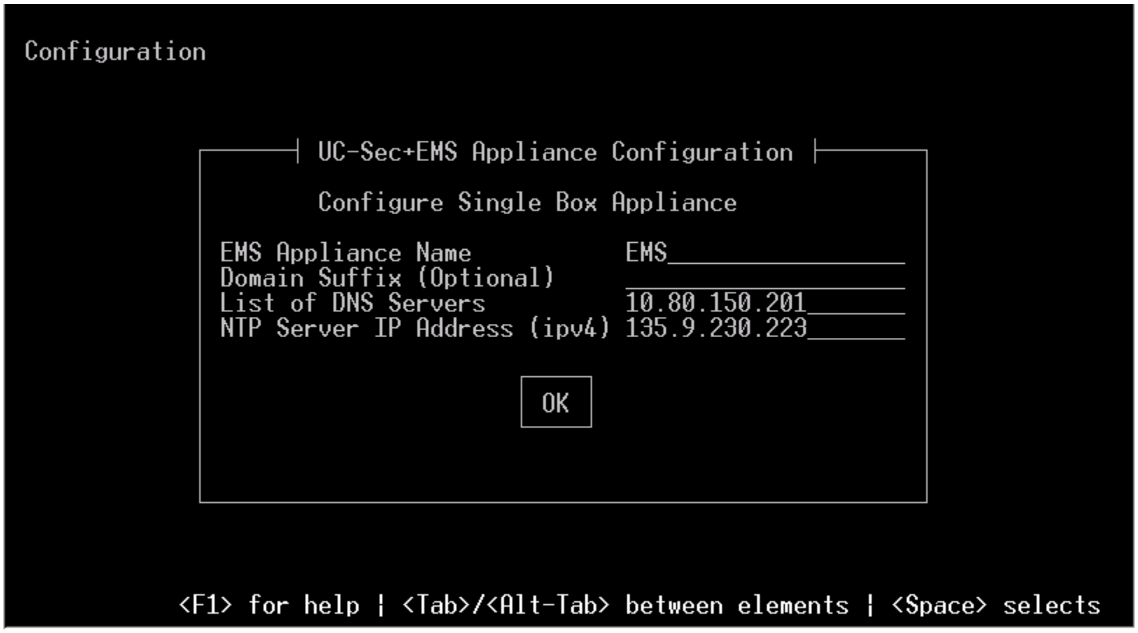
```
Configuration

            UC-Sec Appliance Configuration

   UC-Sec Appliance Name              UC-Sec______________
   Domain Suffix (Optional)           ____________________
   List of DNS Servers                10.80.150.201_______
   NTP Server IP Address (ipv4)       10.80.150.202_______
   Network Passphrase                 *******_____________
   Network Passphrase (Again)         *******_____________

                  OK

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

Figure 54: E-SBC Initial Configuration Screen 1



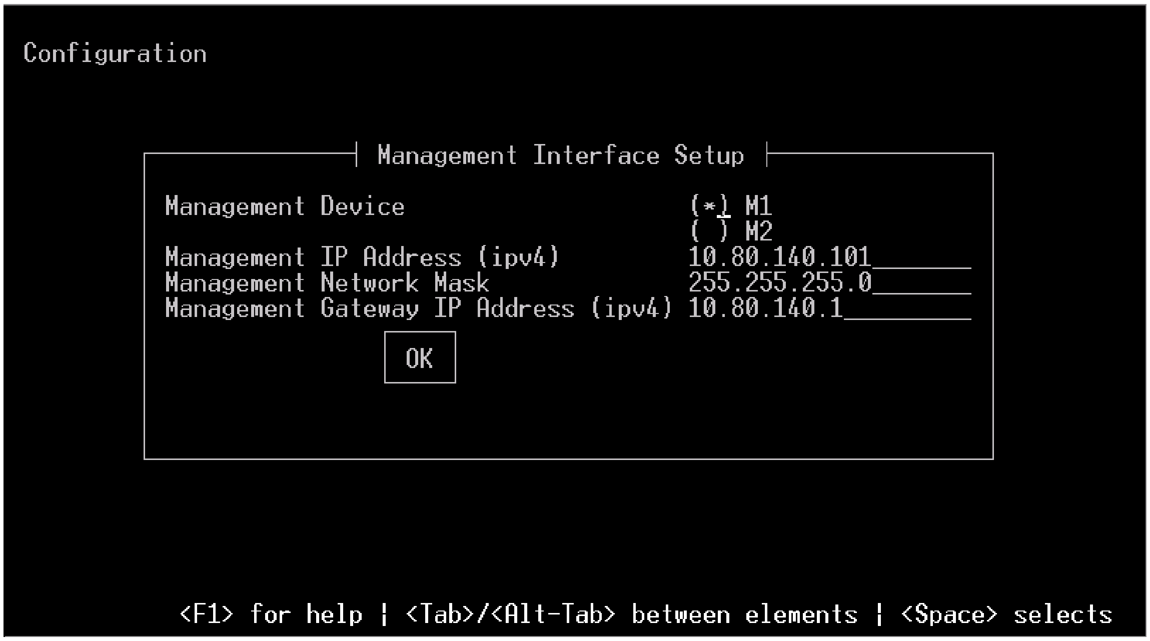
```
Configuration

          ┤ Management Interface Setup ├
Management Device                      (*) M1
                                       ( ) M2
Management IP Address (ipv4)           10.80.140.101_______
Management Network Mask                255.255.255.0_______
Management Gateway IP Address (ipv4)   10.80.140.1_________
EMS Server IP Address (ipv4)           10.80.140.101_______
                 OK

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

Figure 55: E-SBC Initial Configuration Screen 2



```
Configuration

        ┤ UC-Sec+EMS Appliance Configuration ├
        Configure Single Box Appliance

EMS Appliance Name            EMS_________________
Domain Suffix (Optional)      ____________________
List of DNS Servers           10.80.150.201_______
NTP Server IP Address (ipv4)  135.9.230.223_______

                     OK

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

Figure 56: E-SBC Initial Configuration Screen 3



```
Configuration

              ┤ Management Interface Setup ├
   Management Device                      (*) M1
                                          ( ) M2
   Management IP Address (ipv4)           10.80.140.101________
   Management Network Mask                255.255.255.0________
   Management Gateway IP Address (ipv4)   10.80.140.1__________
                      OK

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

Figure 57: E-SBC Initial Configuration Screen 4

7.2. Advanced Configuration

Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP of the E-SBC)

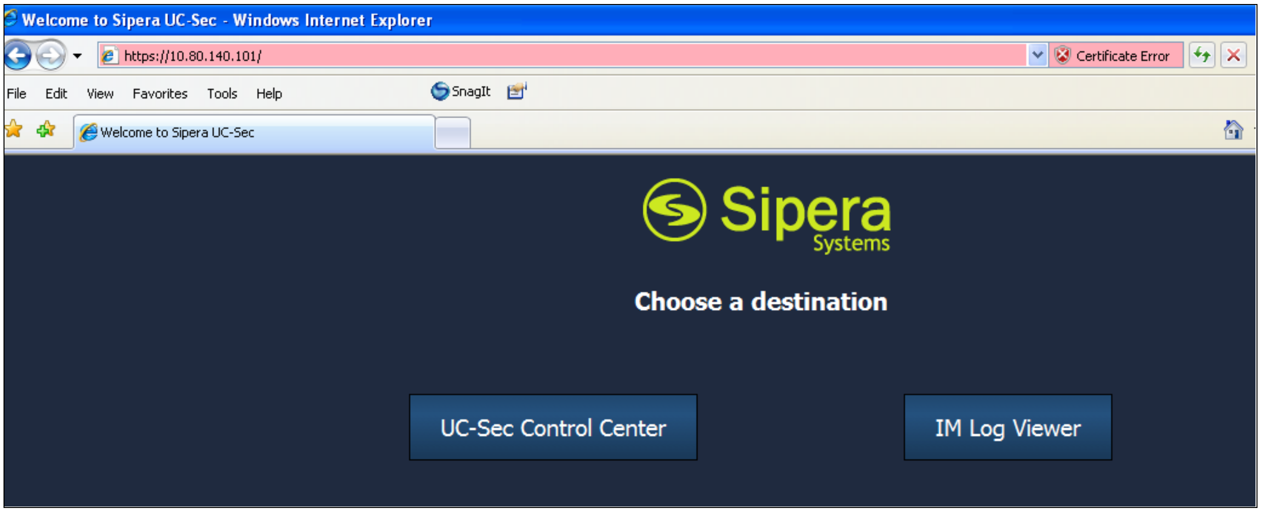
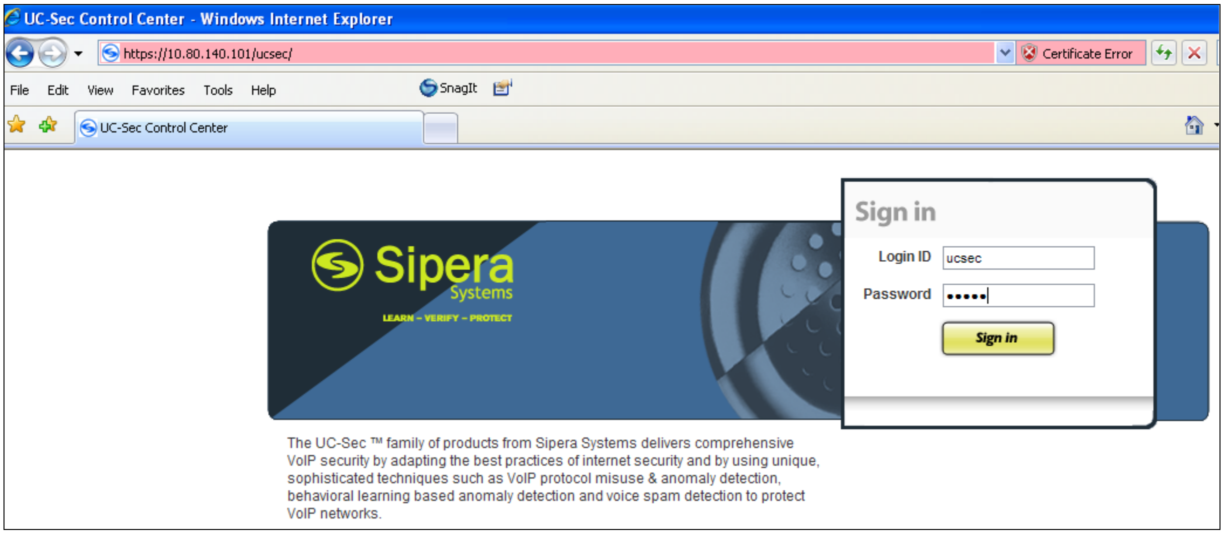


Figure 58: Web Interface

Select **UC-Sec Control Center** and enter the login ID and password.


UC-Sec Control Center - Windows Internet Explorer
https://10.80.140.101/ucsec/
Certificate Error
File Edit View Favorites Tools Help
SnagIt
UC-Sec Control Center
Sipera Systems
LEARN – VERIFY – PROTECT
Sign in

Login ID: ucsec

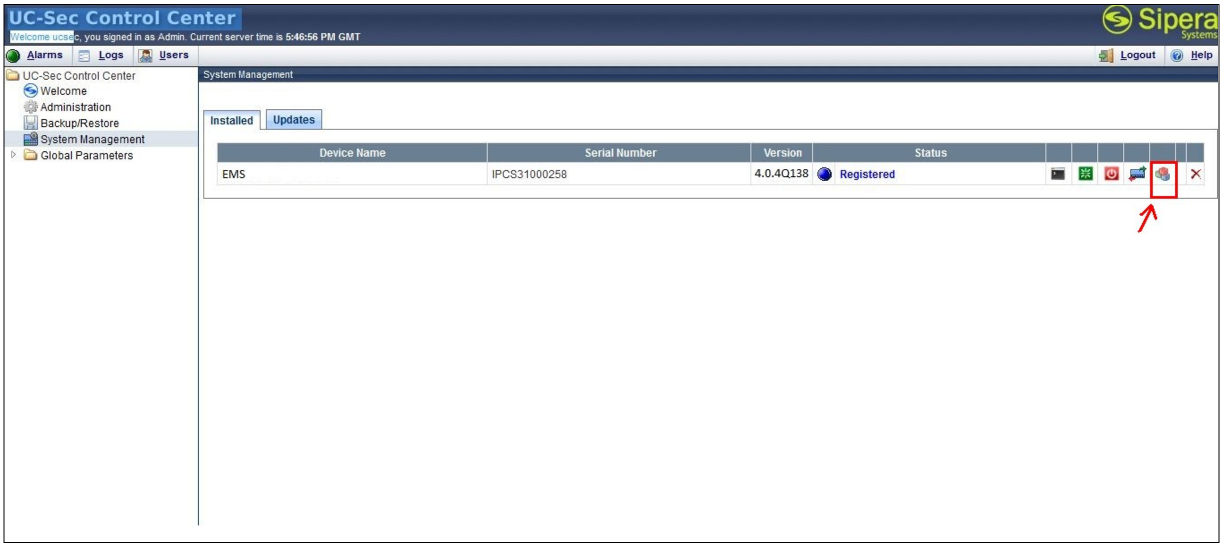
Password: •••••

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.

Figure 59: E-SBC Login

7.3. System Management

When it is the first time the user accesses the Sipera system through the web interface, the user needs to configure some basic parameters. Click on the **System Management**, the user will see the screen as below:



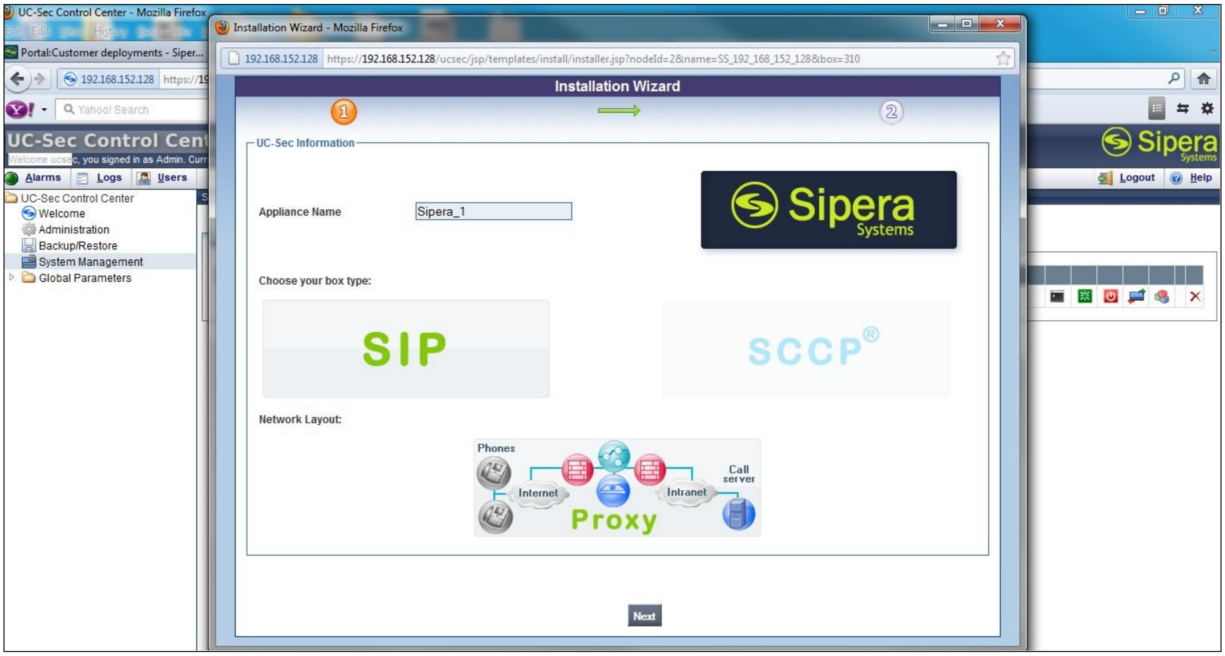
Welcome ucsec, you signed in as Admin. Current server time is 5:46:56 PM GMT

Device Name	Serial Number	Version	Status
EMS	IPCS31000258	4.0.4Q138	Registered

Figure 60: System Management at the first time login

The initial status of the E-SBC is “Registered”, as shown in above diagram. User should then click on **install** button (highlighted in red in **Figure 60**). It will come to next page, as shown in Figure 61. The user should type in an appropriate Applicance name, choose **SIP**, and then click

next.


Installation Wizard

UC-Sec Information

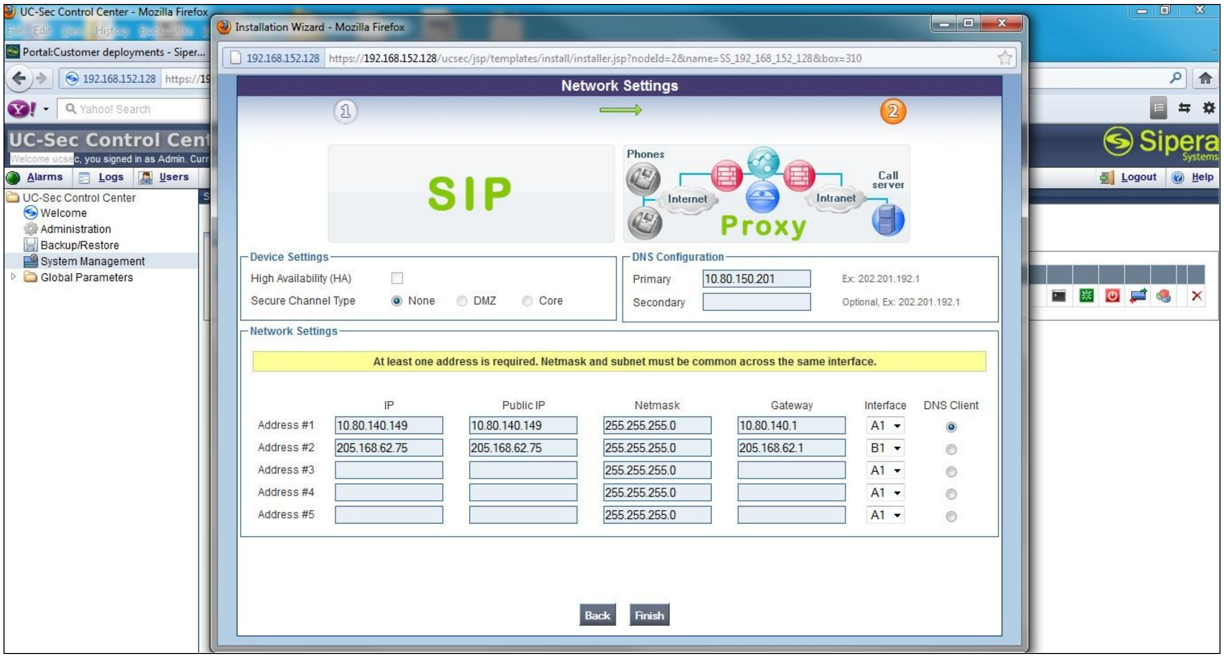
Appliance Name: Sipera_1

Choose your box type: SIP

Network Layout:

Figure 61: Install Device

The user will then see the next screen, as shown in Figure 62, and should enter the primary DNS, the IP of the data network interfaces, gateway, and choose appropriate interface. Click **Finish**


Network Settings

Device Settings

- High Availability (HA): □
- Secure Channel Type: ● None ○ DMZ ○ Core

DNS Configuration

- Primary: 10.80.150.201 Ex: 202.201.192.1
- Secondary: Optional, Ex: 202.201.192.1

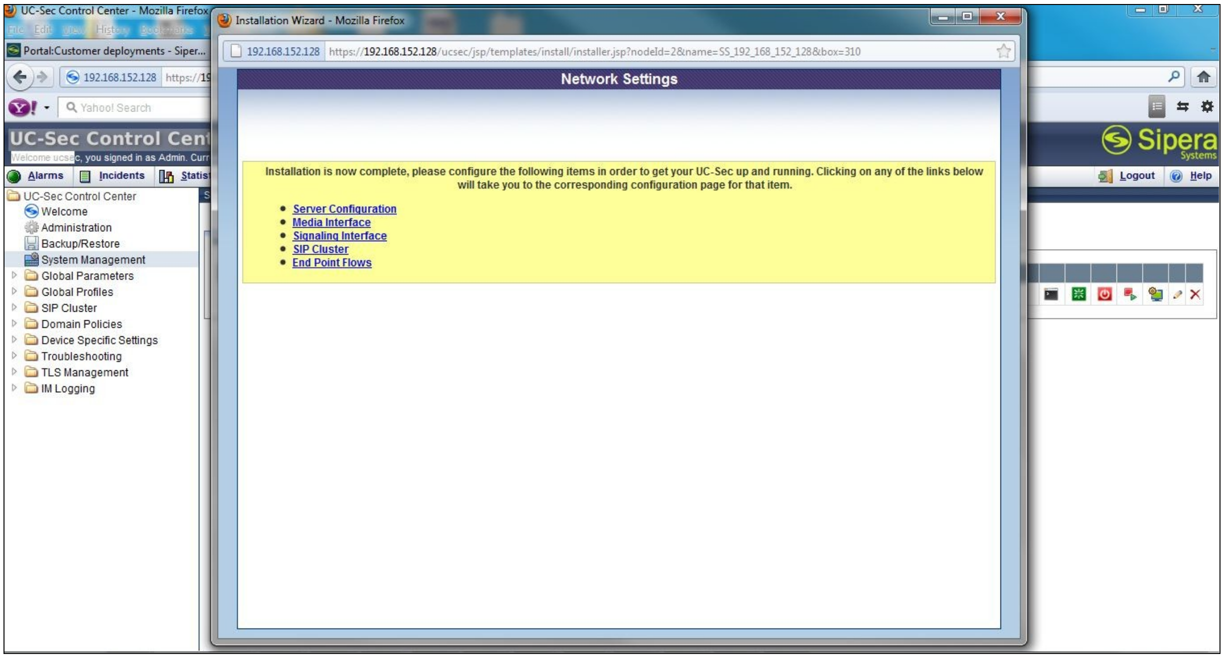
Network Settings

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	10.80.140.149	10.80.140.149	255.255.255.0	10.80.140.1	A1	●
Address #2	205.168.62.75	205.168.62.75	255.255.255.0	205.168.62.1	B1	○
Address #3			255.255.255.0		A1	○
Address #4			255.255.255.0		A1	○
Address #5			255.255.255.0		A1	○

Figure 62: Network Settings

Then the user will see the next screen, as shown in Figure 63. It just shows a rough guideline of what else should be configured. Simply close that window.



Network Settings

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

Figure 63: Network Settings.

7.4. Global Profiles

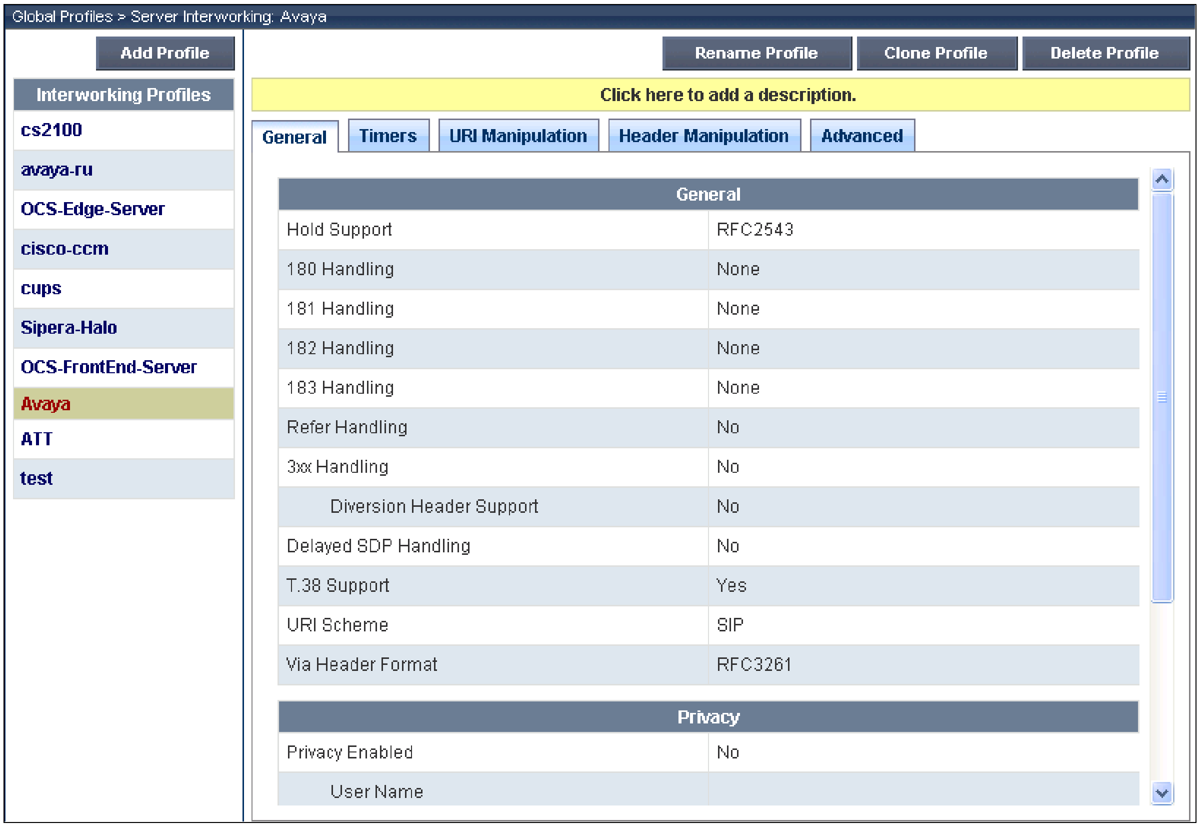
When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.4.1. Server Internetworking Avaya Side

Server Internetworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and t38.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Internetworking**
3. Select **Add Profile**
4. On 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. Hit **Next**
5. At the **Privacy** tab
    a. Hit **Next**
6. At the **Internetworking Profile** tab
    a. Hit **Next**.
7. On the **Advanced** Tab

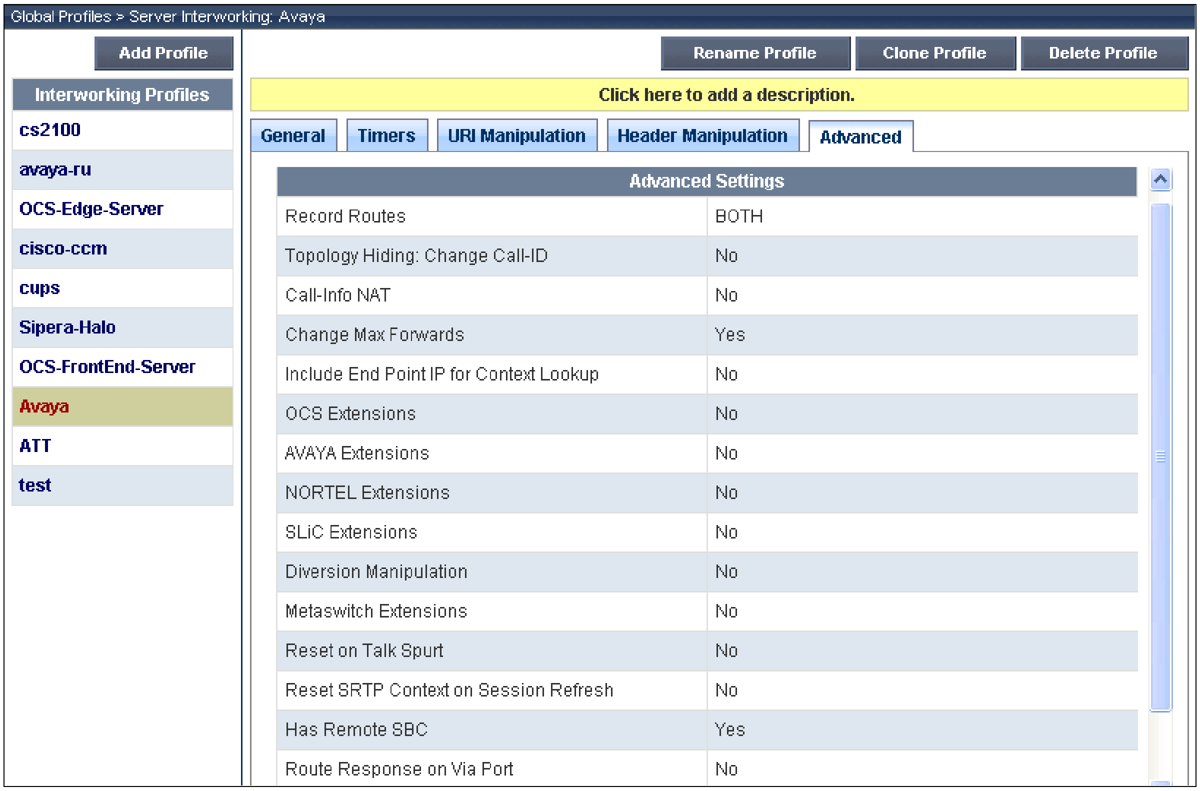
8. Hit **Next**
9. Click **Finish** (not shown)



General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	

Figure 64: Server Internetworking - Avaya

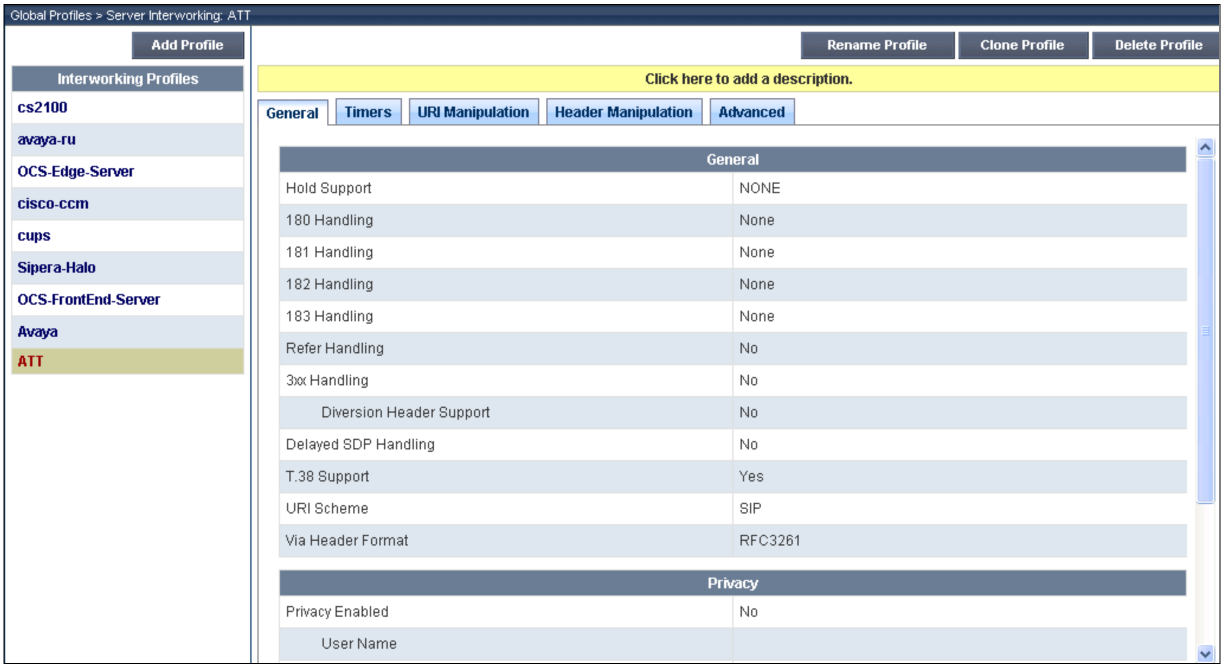


Advanced Settings	
Record Routes	BOTH
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
NORTEL Extensions	No
SLiC Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt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

Figure 65: Server Internetworking – Avaya – Advanced Tab

7.4.2. Server Internetworking – AT&T side

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Internetworking**
3. Select **Add Profile**
4. On the **General** Tab:
    a. Enter profile name**: ATT**
    b. **Check T38 Support → Yes**
    c. All other options on the General Tab can be left at default
    d. Hit **Next**
5. At the **Privacy** tab
    a. Hit **Next**
6. At the **Internetworking Profile** tab
    a. Hit **Next**.
7. On the **Advanced** Tab
8. Hit **Next**
9. Click **Finish**



Global Profiles > Server Interworking: ATT

Interworking Profiles
cs2100
avaya-ru
OCS-Edge-Server
cisco-ccm
cups
Sipera-Halo
OCS-FrontEnd-Server
Avaya
ATT

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

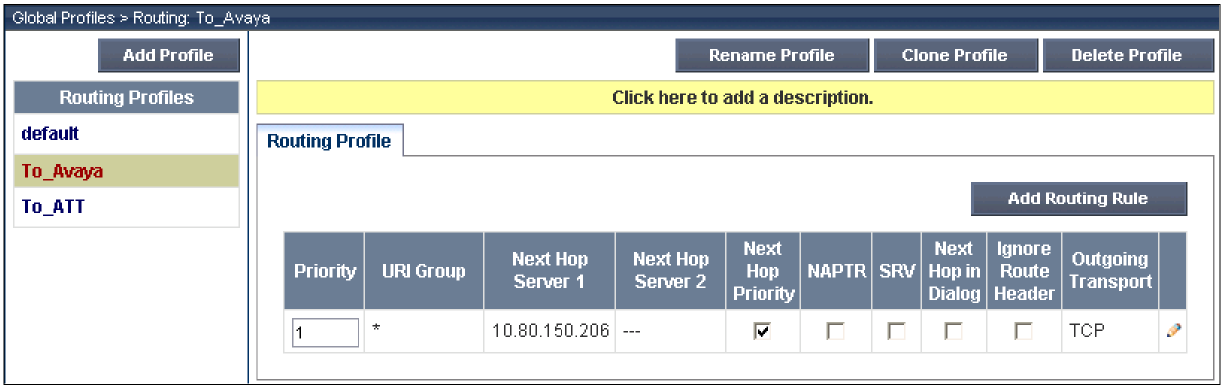
Privacy	
Privacy Enabled	No
User Name	

Figure 66: Server Internetworking – AT&T

7.4.3. 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: **To_Avaya**
5. Hit **Next**
6. **Next Hop Server 1: 10.80.150.206 (Session Manager IP address)**
7. Select **Routing Priority Based on Next Hop Server**
   a. **Outgoing Transport: TCP**
   b. Click **Finish**



Global Profiles > Routing: To_Avaya

Routing Profiles
default
To_Avaya
To_ATT

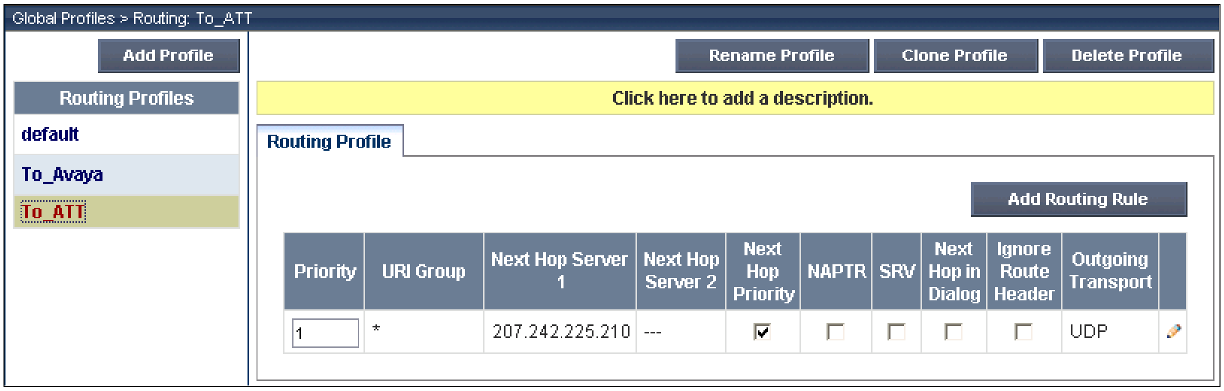
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.80.150.206	---	☑	□	□	□	□	TCP

Figure 67: Routing – To_Avaya

7.4.4. Routing –AT&T 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: **To_ATT**
5. Hit **Next**
6. **Next Hop Server 1: 207.242.225.210 (IP Address provided by AT&T)**
    a. Select **Routing Priority Based on Next Hop Server**
    b. **Outgoing Transport: UDP**
    c. Click **Finish**



Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport	
1	*	207.242.225.210	---	☑	□	□	□	□	UDP	✎

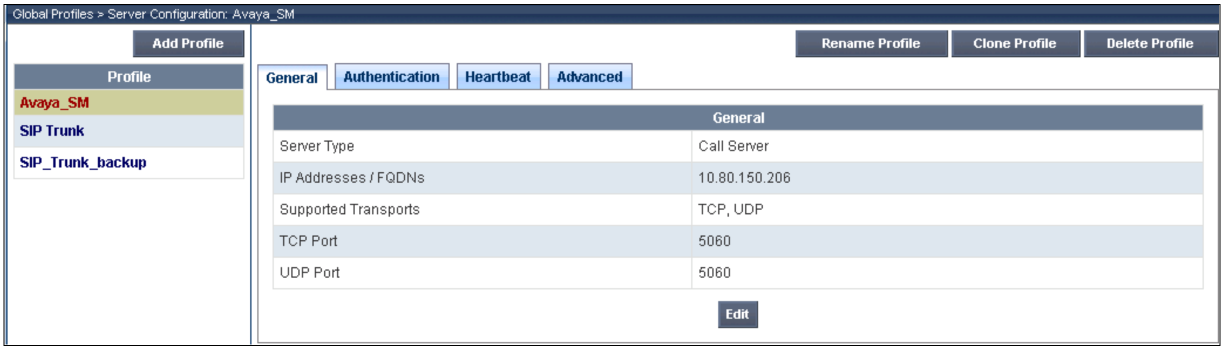
Figure 68: Routing – To_ATT

7.4.5. Server Configuration– Avaya SM

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 the **Server Configuration**
3. Select **Add Profile, enter profile name: Avaya SM**
4. On the **Add Server Configuration Profile** Tab:
    a. Select Server Type**: Call Server**
    b. **IP Address: 10.80.150.206 (Session Manager IP Address)**
    c. **Supported Transports**: Check **UDP** and **TCP**
    d. **TCP Port:5060**
    e. **UDP Port: 5060**
    f. Hit **Next**

5. At the **Authentication** tab
    a. hit **Next**
6. At the **Heartbeat** tab
    a. Hit **Next**.
7. On the **Advanced** Tab
    a. Select **Avaya** for Interworking Profile
    b. Hit **Next**
8. Click **Finish**



General	
Server Type	Call Server
IP Addresses / FQDNs	10.80.150.206
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

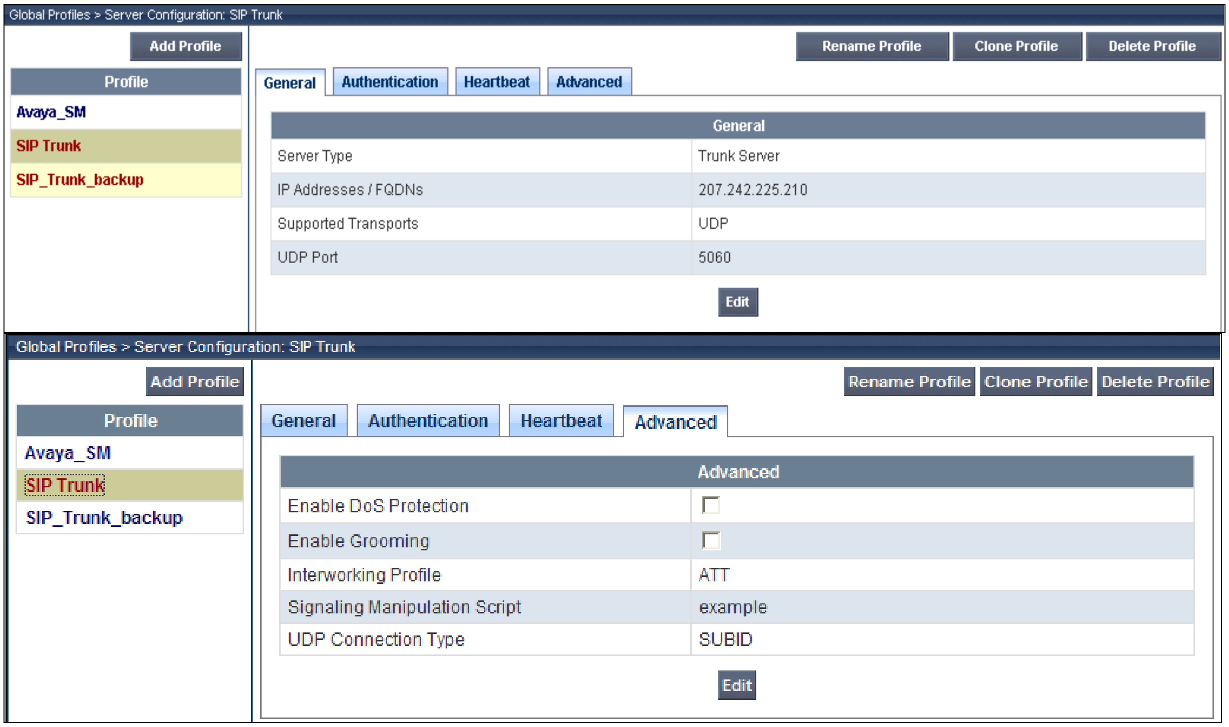
Figure 69: Server Config Avaya_SM

7.4.6. Server Configuration– AT&T side

The **Server Configuration** screen contains fourtabs: **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, server type, heartbeat signaling parameters and some advanced options.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**
4. **Name: SIP Trunk**
5. On the **Add Server Configuration Profile** Tab:
    a. Select Server Type**: Trunk Server**
    b. **IP Address: 207.242.225.210 (AT&T Trunk Server)**
    c. **Supported Transports**: Check **UDP**
    d. **UDP Port: 5060**
    e. Hit **Next**
6. At the **Authentication** tab
    a. Hit **Next**
9. At the **Heartbeat** tab (This tab will be seen again in Redundancy **Section 7.7)**
    b. Hit **Next**.
7. On the **Advanced** Tab
    a. Select **ATT** for interworking profile
    b. For **Signaling Manipulation Script** select **Example** (this will be created in **Section 7.4.9** below)
    c. Hit **Next**

8. Click **Finish**



General	
Server Type	Trunk Server
IP Addresses / FQDNs	207.242.225.210
Supported Transports	UDP
UDP Port	5060

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

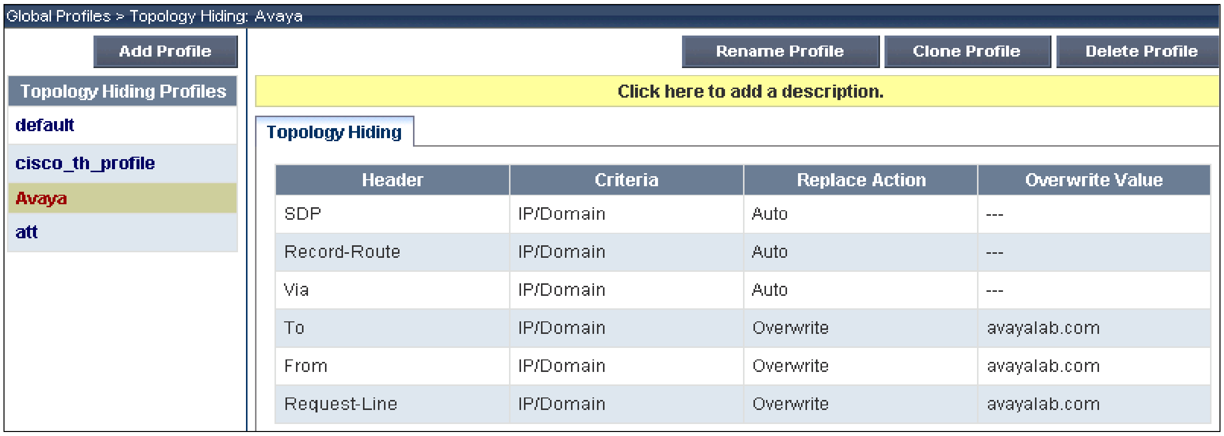
Figure 70: Server Config – To AT&T (General and Advanced Tab shown)

7.4.7. 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 the **Topology Hiding**
3. Click **default** profile and select **Clone Profile**
4. **Enter Profile Name: 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**: avayalab.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**: avayalab.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**: avayalab.com**

8. Click **Finish**

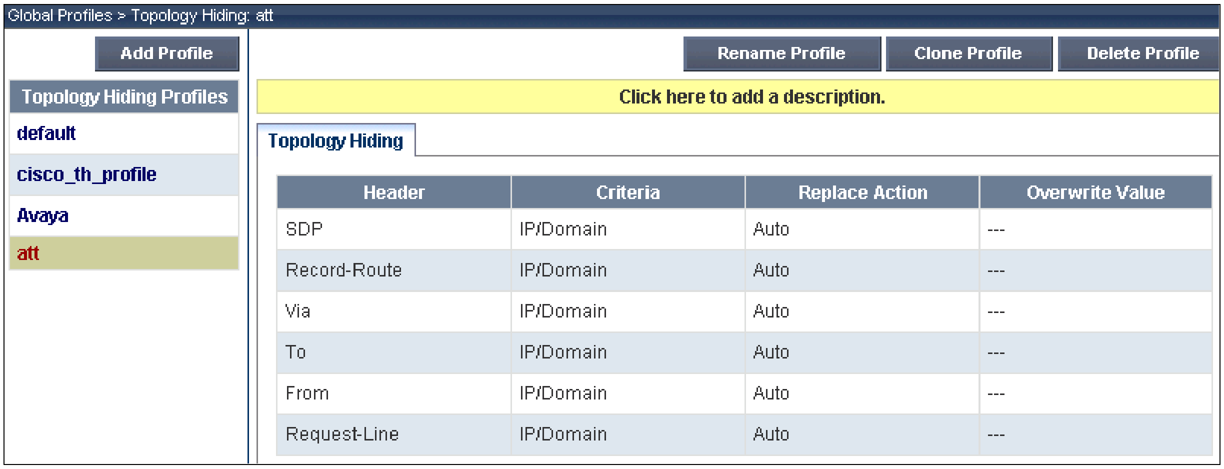


Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Overwrite	avayalab.com
From	IP/Domain	Overwrite	avayalab.com
Request-Line	IP/Domain	Overwrite	avayalab.com

Figure 71: Topology Hiding Avaya

7.4.8. Topology Hiding – AT&T side

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Topology Hiding**
3. Click **default** profile and select **Clone Profile**
4. Enter Profile Name**: att**
5. Leave all Replace Action to **"Auto"**
6. Click **Finish**



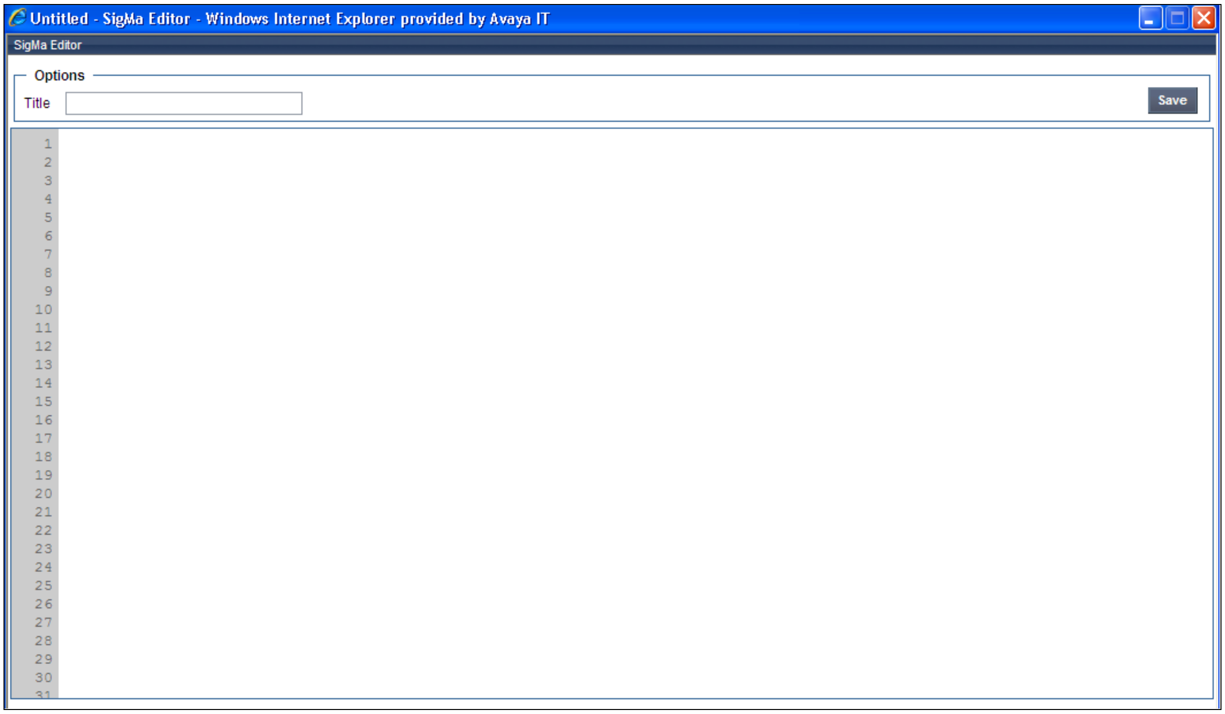
Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---

Figure 72: Topology Hiding AT&T

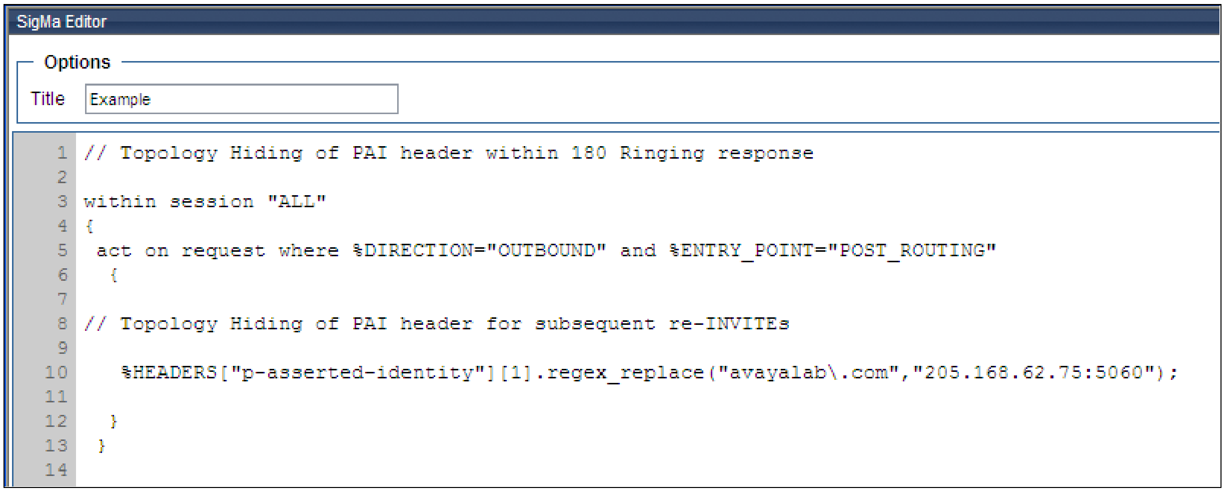
7.4.9. Signaling Manipulation

This feature adds the ability to add, change and delete any of the headers and other information in a SIP message. The feature will add the ability to configure such manipulation at each flow level in a highly flexible manner using a proprietary scripting language.

1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Signaling Manipulation**
3. Click the **Add Script** button (not shown) to add a new script, or select an existing script to edit. If adding a script, a screen such as the following is displayed.
4. Enter a title in the upper left
5. Enter the text to manipulate headers
6. Click **Save**.


Untitled - SigMa Editor - Windows Internet Explorer provided by Avaya IT
SigMa Editor
Options
Title
Save

In the tested environment, the following Sigma script was used to strip the PAI header out of the 180 Ringing messages.



Title: Example

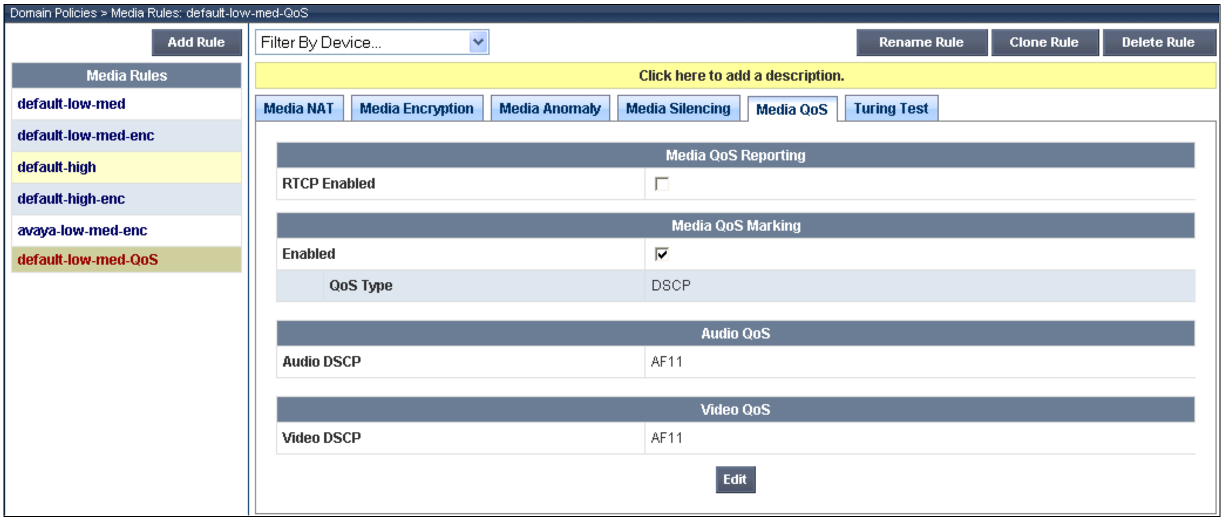
```
// Topology Hiding of PAI header within 180 Ringing response

within session "ALL"
{
 act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {

// Topology Hiding of PAI header for subsequent re-INVITEs

   %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com","205.168.62.75:5060");

  }
 }

```

7.5. 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. Media Rules

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

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **Media Rules**
3. Select the **default-low-med** Rule
4. Select **Clone Rule** button
    a. Name**: default-low-med-QOS**
    b. Click **Finish**
5. Highlight the rule just created: **default-low-med-QOS**
    a. Select the **Media QOS** tab
    b. Click the **Edit** button
    c. Check the **Media QOS Marking** Enabled
    d. Check the **DSCP** box
    e. **Audio:** Select **AF11** from the drop-down
    f. **Video**: Select **AF11** from the drop-down
    g. Click **Finish**



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

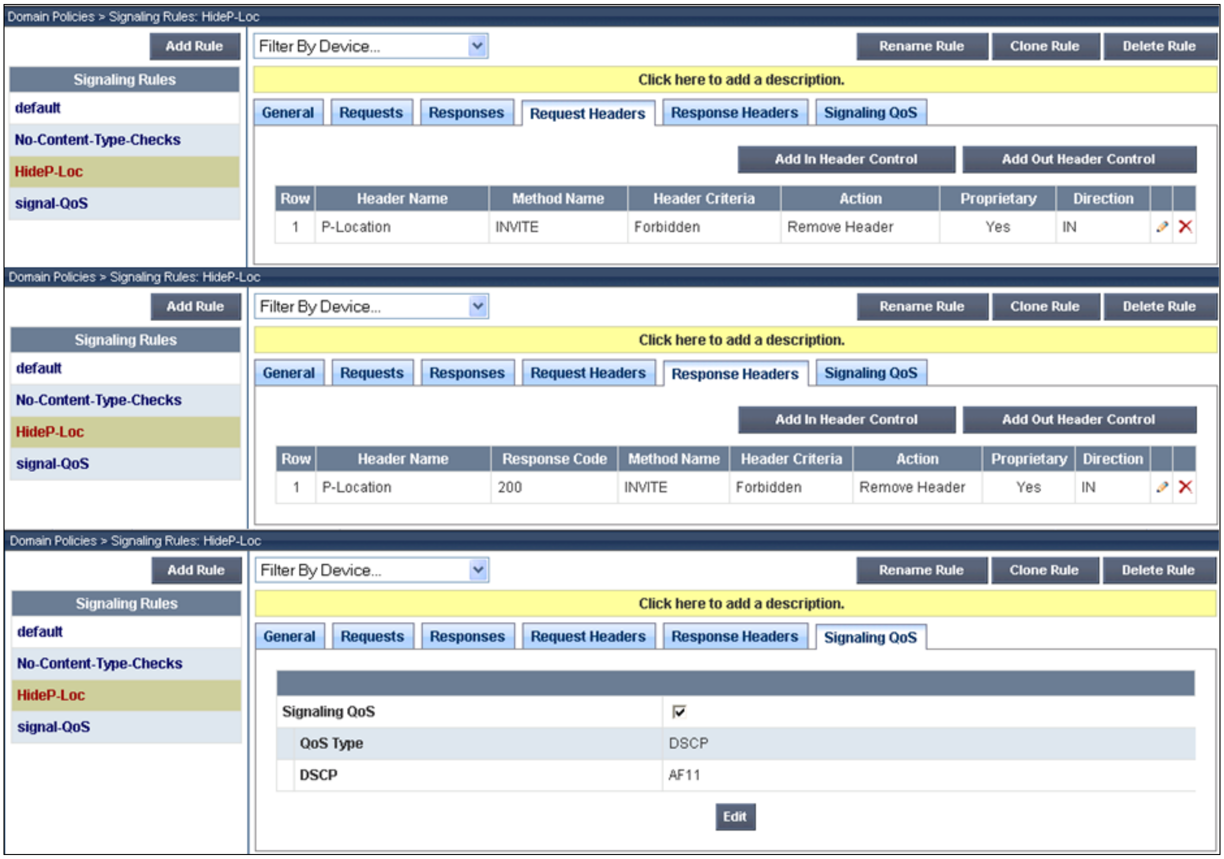
Figure 73: Media Rule

7.5.1. Signaling Rules

This signaling rule is being created to strip the P-location information from the SIP messages before sending it on the service provider.

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

3. Select **Add Rule**
4. Name**: HideP-Loc**
5. Hit **Next**
    a. On the **Signaling Rule** page leave all as default
6. Hit **Next**
    a. On the **Signaling QOS** page
    b. Select **DSCP**
    c. Select **AF11** from the drop-down box
7. Select **Finish**
8. 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. **Presence Action: Remove Header**
    g. Click **Finish**
9. 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. **Presence Action: Remove Header**
    h. Click **Finish**



Domain Policies > Signaling Rules: HideP-Loc

Request Headers:

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

Domain Policies > Signaling Rules: HideP-Loc

Response Headers:

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

Domain Policies > Signaling Rules: HideP-Loc

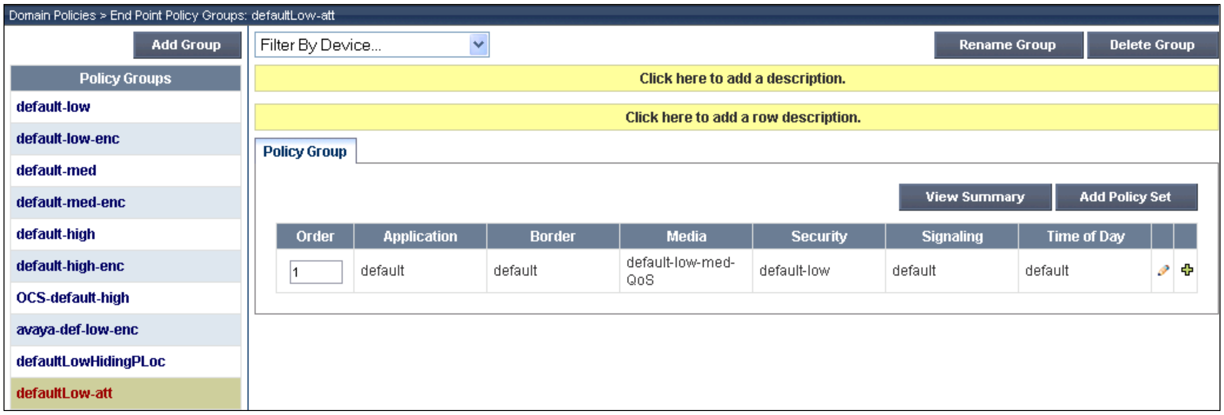
Signaling QoS:

Signaling QoS	☑
QoS Type	DSCP
DSCP	AF11

Figure 74: Signaling Rules – Hide P-Location

7.5.2. Endpoint Policy Groups – for AT&T Flow

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **End Point Policy Groups**
3. Select **Add Group**
4. **Name: defaultLow-att**
    a. **Application Rule: default**
    b. **Border Rule: default**
    c. **Media Rule: default-low-med-QOS**
    d. **Security Rule: default-low**
    e. **Signaling Rule: default**
    f. **Time of Day: default**
5. **Select Finish**

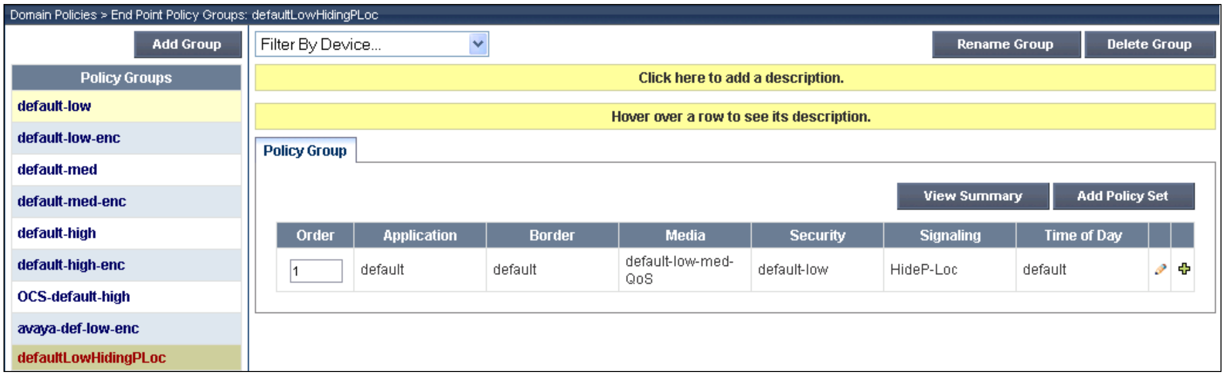


Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-low-med-QoS	default-low	default	default

Figure 75: End Point Policy – defaultLow-att

7.5.3. Endpoint Policy Groups – for Avaya Flow

1. Select **Domain Policies** from the menu on the left-hand side
2. Select the **End Point Policy Groups**
3. Select **Add Group**
4. **Name: defaultLowHidingPLoc**
    a. **Application Rule: default**
    b. **Border Rule: default**
    c. **Media Rule: default-low-med-QOS**
    d. **Security Rule: default-low**
    e. **Signaling Rule: HideP-Loc**
    f. **Time of Day: default**
5. Select **Finish**



Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-low-med-QoS	default-low	HideP-Loc	default

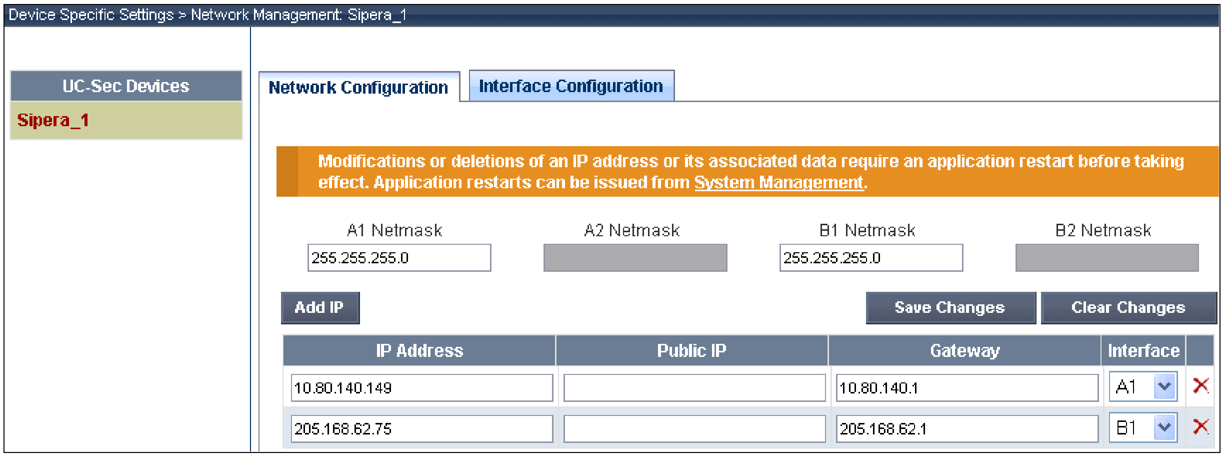
Figure 76: End Point Policy – defaultLowHidingPLoc

7.6. Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. 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.

7.6.1. Network Management

1. Select **Device Specific Settings** from the menu on the left-hand side
2. Select **Network Management**
3. In case the network interfaces has been configured as in section 7.3, and no change are needed, go to step 6. Otherwise if change is needed, go to step 4 to change it.
4. Enter in the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces.
5. Select the physical interface used in the Interface column



Device Specific Settings > Network Management: Sipera_1

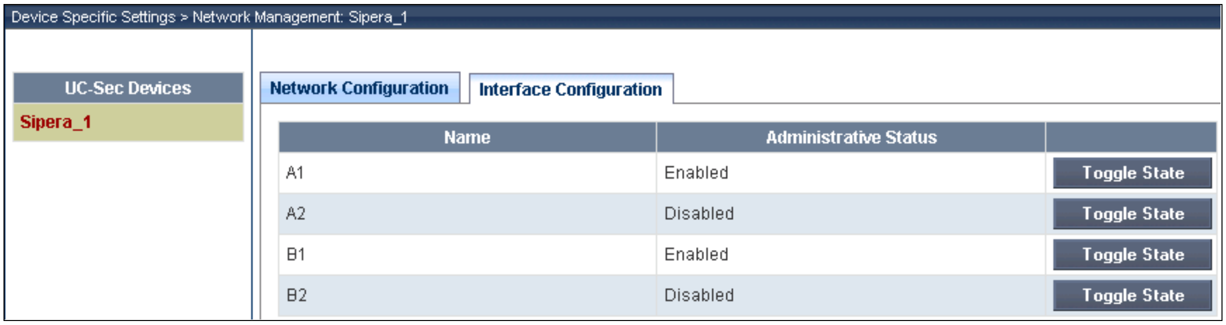
Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.0		255.255.255.0	

IP Address	Public IP	Gateway	Interface
10.80.140.149		10.80.140.1	A1
205.168.62.75		205.168.62.1	B1

Figure 77: Network Management

6. Select the **Interface Configuration Tab**.
7. Toggle the State of the physical interfaces being used.



Device Specific Settings > Network Management: Sipera_1

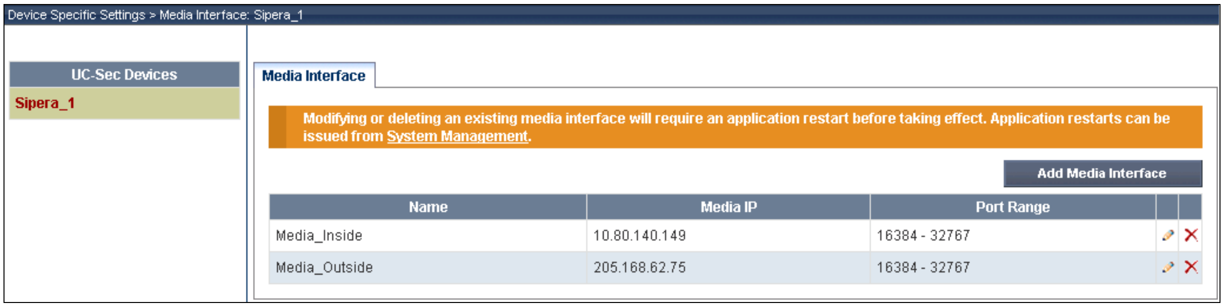
Name	Administrative Status	
A1	Enabled	Toggle State
A2	Disabled	Toggle State
B1	Enabled	Toggle State
B2	Disabled	Toggle State

Figure 78: Interface Configuration

7.6.2. Media Interfaces

AT&T requires customers to use RTP ports in the range of 16384 – 32767. Before this range can be configured as shown here, the default ports on the Sipera must be changed. See **Section 7.6.1**. 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: 10.80.140.149** (Internal Address toward Session Manager)
   c. **Port Range: 16384 - 32767**
   d. Click **Finish**
4. Select **Add Media Interface**
   a. **Name: Media_Outside**
   b. **Media IP: 205.168.62.75** (External Internet Address toward at&t trunk)
   c. **Port Range: 16384 - 32767**
   d. Click **Finish**



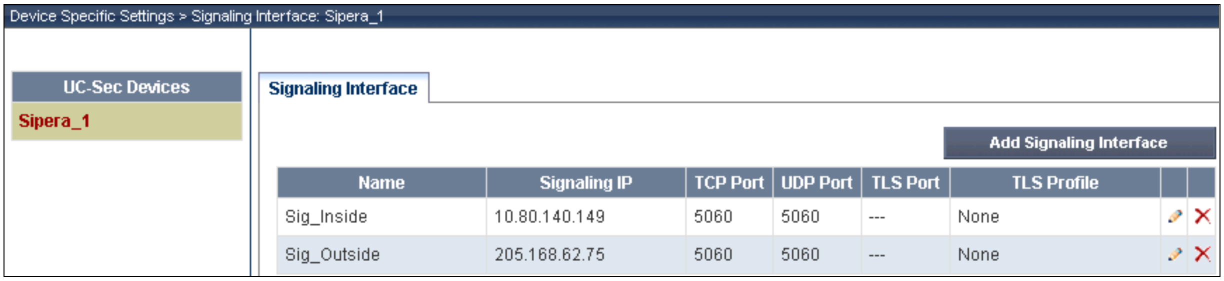
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range
Media_Inside	10.80.140.149	16384 - 32767
Media_Outside	205.168.62.75	16384 - 32767

Figure 79: Media Interface

7.6.3. 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: 10.80.140.149 (Internal Address toward Session Manager)**
   c. **TCP Port: 5060**
   d. **UDP Port: 5060**
   e. Click **Finish**
4. Select **Add Media Interface**
   a. **Name: Sig_Outside**
   b. **Media IP: 205.168.62.75 (External Internet Address toward at&t trunk)**
   c. **TCP Port: 5060**
   d. **UDP Port: 5060**
   e. Click **Finish**



Device Specific Settings > Signaling Interface: Sipera_1

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
Sig_Inside	10.80.140.149	5060	5060	---	None
Sig_Outside	205.168.62.75	5060	5060	---	None

Figure 80: Signaling Interface

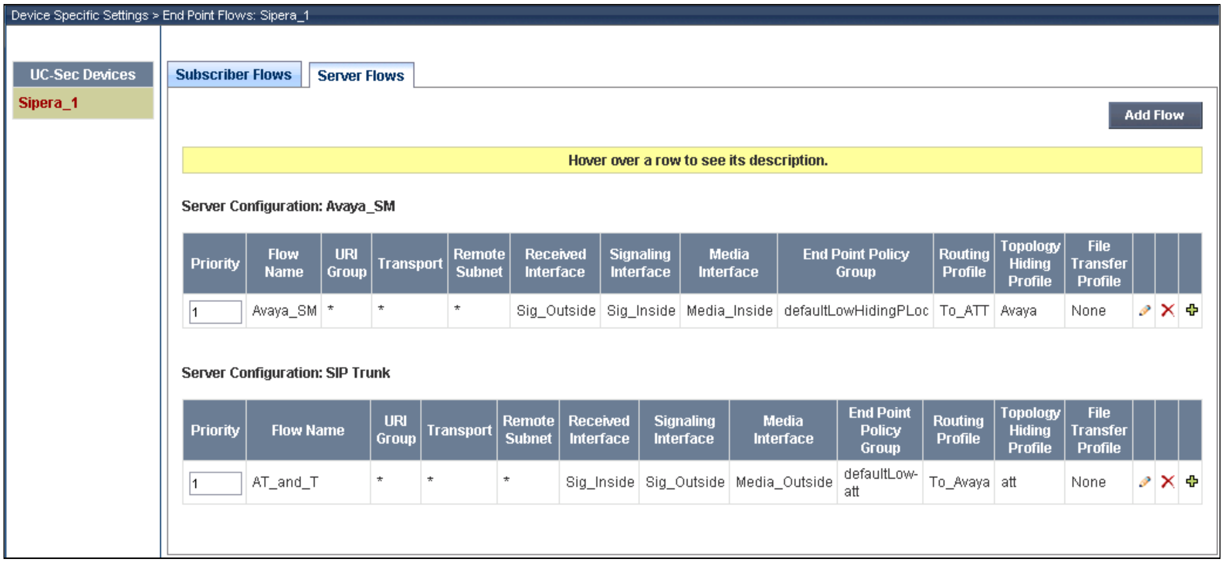
7.6.4. End Point Flows – Avaya_SM

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**
5. **Name: Avaya_SM**
   a. **Server Configuration**: **Avaya_SM**
   b. **URI Group: ***
   c. **Transport: ***
   d. **Remote Subnet: ***
   e. **Received Interface**: **Sig_Outside**
   f. **Signaling Interface: Sig_Inside**
   g. **Media Interface**: **Media_Inside**
   h. **End Point Policy Group: defaultLowHidingPLoc**
   i. **Routing Profile: To_ATT**
   j. **Topology Hiding Profile: Avaya**
   k. **File Transfer Profile: None**
   l. Click **Finish**

7.6.5. End Point Flows – SIP Trunk

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**
5. **Name: SIP Trunk**
   a. **Server Configuration: SIP Trunk**
   b. **URI Group: ***
   c. **Transport: ***
   d. **Remote Subnet: ***
   e. **Received Interface: Sig_Inside**
   f. **Signaling Interface: Sig_Outside**
   g. **Media Interface: Media_Outside**
   h. **End Point Policy Group**: **defaultLow-att**
   i. **Routing Profile: To_Avaya**

j. **Topology Hiding Profile: att**
k. **File Transfer Profile: None**
l. Click **Finish**


Device Specific Settings > End Point Flows: Sipera_1
UC-Sec Devices
Sipera_1
Subscriber Flows
Server Flows
Add Flow
Hover over a row to see its description.

Server Configuration: Avaya_SM

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	✎	✗	✚

Server Configuration: SIP Trunk

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	AT_and_T	*	*	*	Sig_Inside	Sig_Outside	Media_Outside	defaultLow-att	To_Avaya	att	None	✎	✗	✚

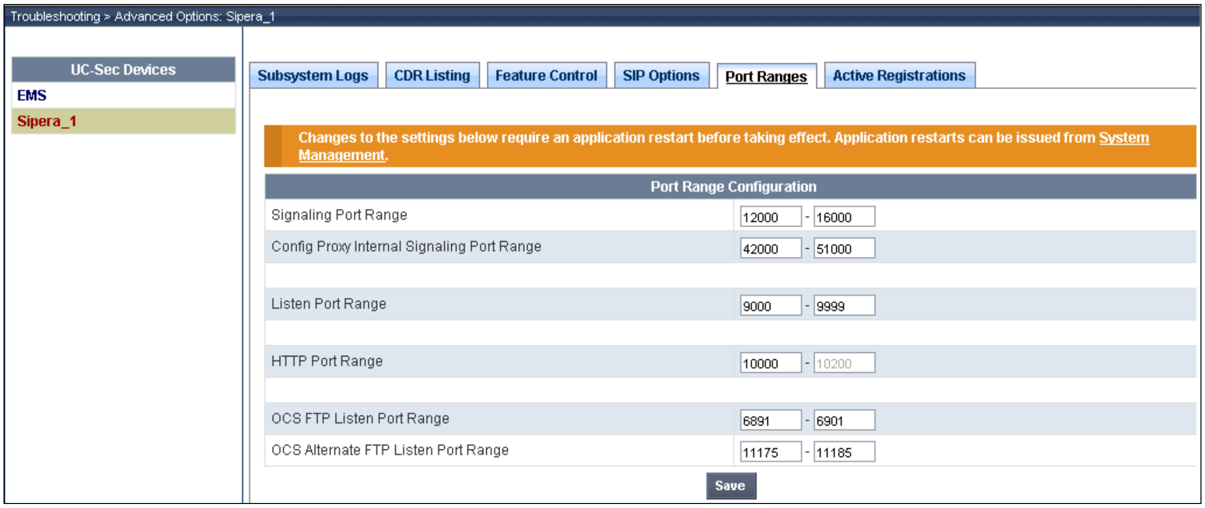
Figure 81: End Point Flow - Server Flow

7.7. Troubleshooting Section

7.7.1. Changing the Default Ports

The default ports need to be changed to follow the guidelines supplied by AT&T for the RTP port range of 16384 – 32767. After changing the default ports here, follow Section 7.5.2 to change the RTP port range towards AT&T.

1. Select **Troubleshooting** from the menu on the left-hand side
2. Select **Advanced Options**
3. Select the **Sipera_1** 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)
   c. Click **Save**



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

Figure 82: Default Port Ranges

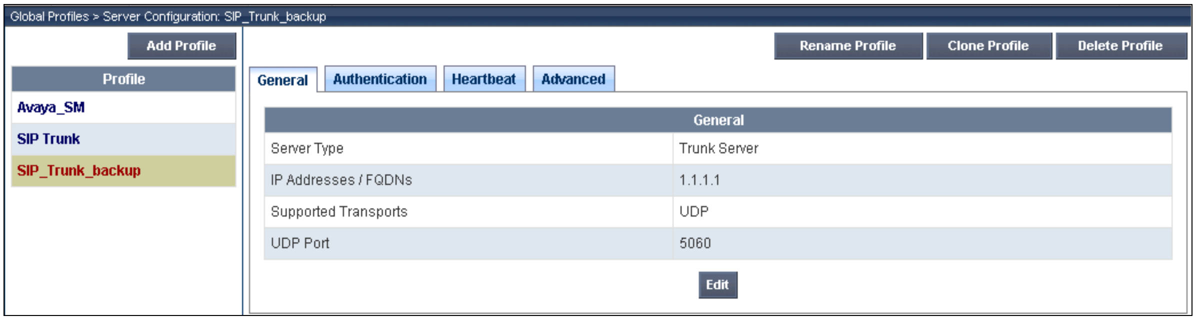
7.8. Redundancy

If the service provider offers a secondary location for back-up purposes, it is possible to configure a secondary location for the network to use in case the primary is unavailable. The heartbeat must be enabled on both server configurations for redundancy to work properly.

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

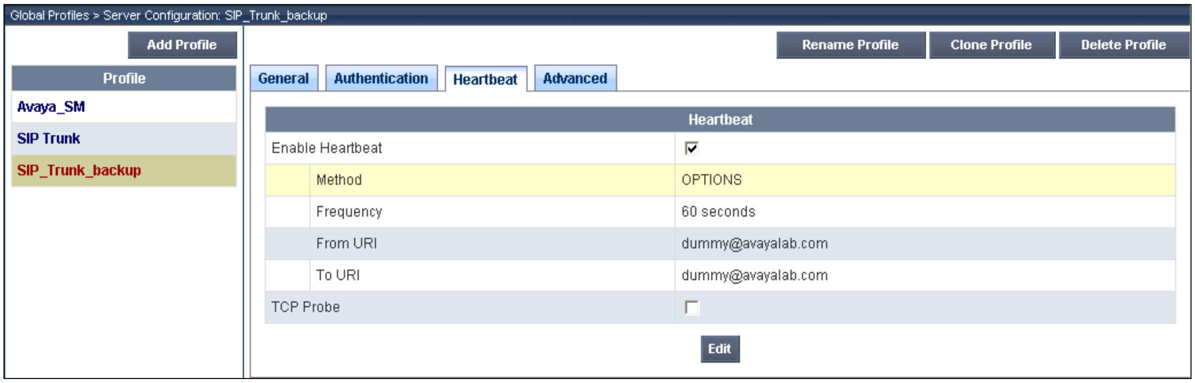
1. Select **Global Profiles** from the menu on the left-hand side
2. Select the **Server Configuration**
3. Select **Add Profile**
4. **Name: SIP_Trunk_backup**
5. On the **Add Server Configuration Profile** Tab:
   a. Select Server Type**: Call Server**
   b. **IP Address: 1.1.1.1** (Example Address for a secondary location)
   c. **Supported Transports**: Check **UDP**
   d. **UDP Port: 5060**
   e. Hit **Next**
6. At the **Authentication** tab
   a. Hit **Next**
7. At 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: dummy@avayalab.com
   e. To URI: dummy@avayalab.com
8. On the **Advanced** Tab
   a. Hit **Next**
9. Click **Finish**
10. Select the Primary Trunk created in **Section 7.3.6**: **SIP Trunk**
11. Select the **Heartbeat Tab**

12. Select **Edit**
13. **Repeat Steps 7a – 7e**
14. Click **Finish**



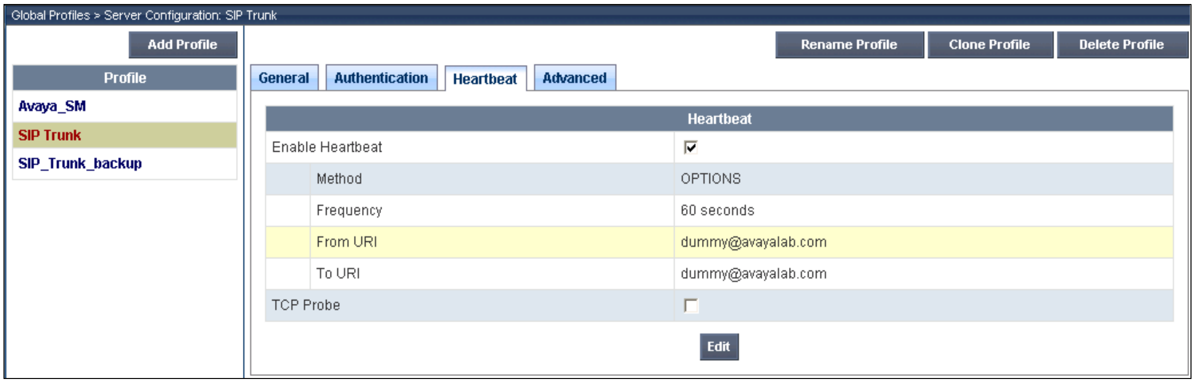
General	
Server Type	Trunk Server
IP Addresses / FQDNs	1.1.1.1
Supported Transports	UDP
UDP Port	5060

Figure 83: Server Configuration – SIP_trunk_backup – General Tab



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

Figure 84: Server Configuration – SIP_trunk_backup – Heartbeat Tab



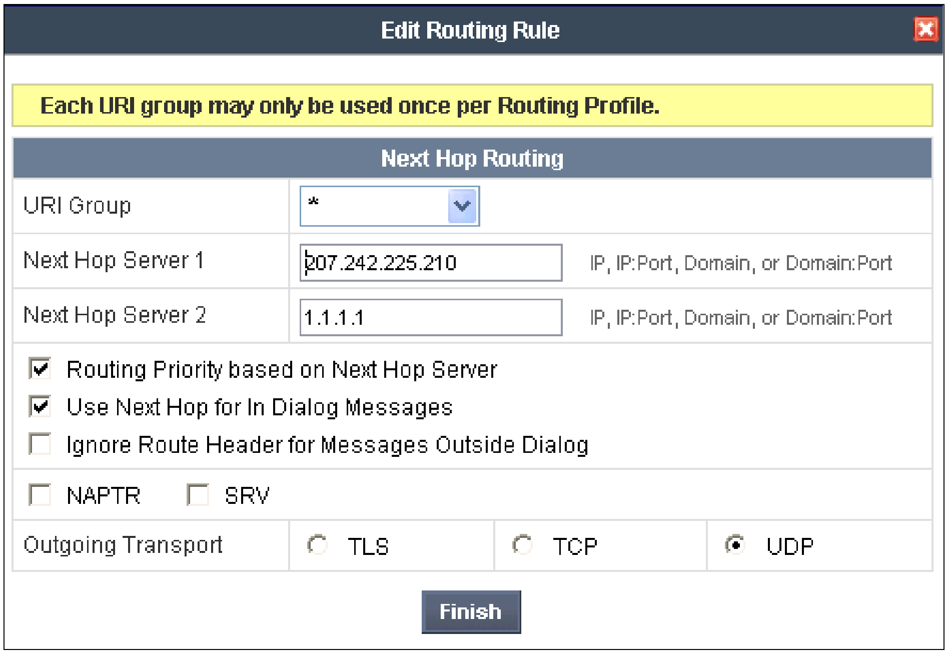
Heartbeat	
Enable Heartbeat	☑
Method	OPTIONS
Frequency	60 seconds
From URI	dummy@avayalab.com
To URI	dummy@avayalab.com
TCP Probe	☐

Figure 85: Server Configuration – SIP trunk – Heartbeat Tab

7.8.2. 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 at the end of the line to edit
5. Enter the IP Address of the secondary location in the **Next Hop Server 2: 1.1.1.1**

6. Click **Finish**



Edit Routing Rule

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

Next Hop Routing

URI Group	*	
Next Hop Server 1	207.242.225.210	IP, IP:Port, Domain, or Domain:Port
Next Hop Server 2	1.1.1.1	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

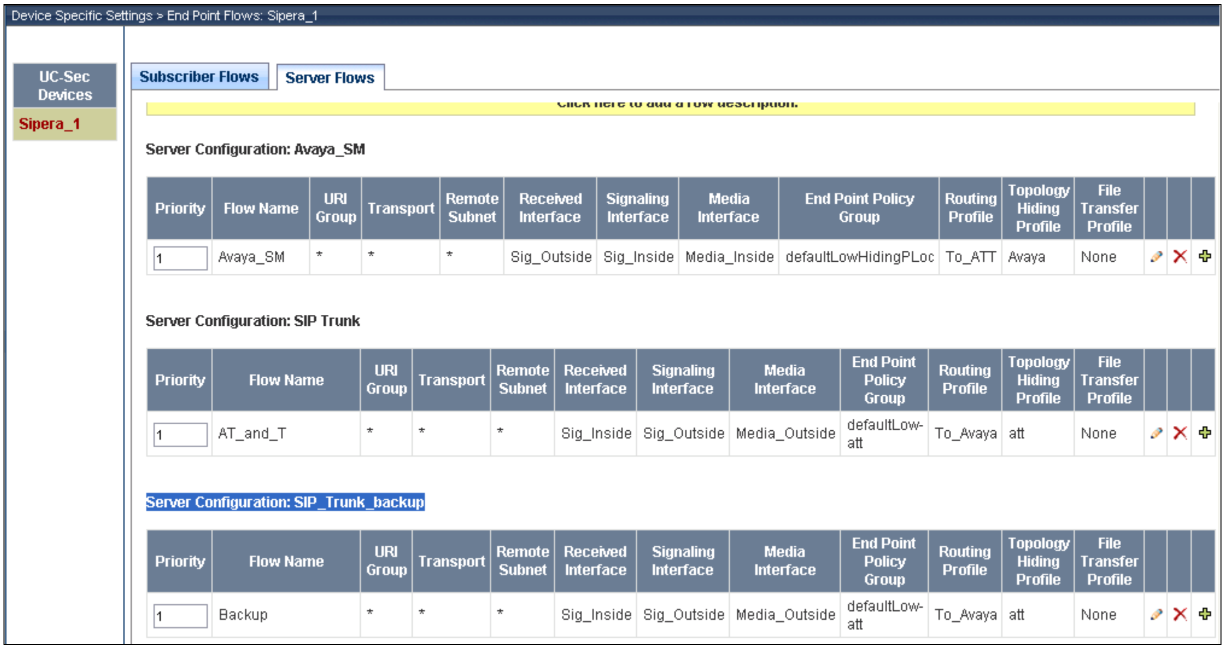
☐ NAPTR ☐ SRV

Outgoing Transport ○ TLS ○ TCP ● UDP

Figure 86: Routing – Next Hop Server 2

7.8.3. 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**
5. **Name: Backup**
    a. **Server Configuration: SIP_Trunk_backup**
    b. **URI Group: ***
    c. **Transport: ***
    d. **Remote Subnet: ***
    e. **Received Interface: Sig_Inside**
    f. **Signaling Interface: Sig_ Outside**
    g. **Media Interface: Media_ Outside**
    h. **End Point Policy Group**: **defaultLow-att**
    i. **Routing Profile: To_Avaya**
    j. **Topology Hiding Profile: att**
    k. **File Transfer Profile: None**
    l. Click **Finish**



Device Specific Settings > End Point Flows: Sipera_1
UC-Sec Devices
Sipera_1
Subscriber Flows
Server Flows
Click here to add a row description.

Server Configuration: Avaya_SM

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	✎	✗	✚

Server Configuration: SIP Trunk

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	AT_and_T	*	*	*	Sig_Inside	Sig_Outside	Media_Outside	defaultLow-att	To_Avaya	att	None	✎	✗	✚

Server Configuration: SIP_Trunk_backup

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	Backup	*	*	*	Sig_Inside	Sig_Outside	Media_Outside	defaultLow-att	To_Avaya	att	None	✎	✗	✚

Figure 87: Server Flows – Added Backup Flow

8. Verification Steps

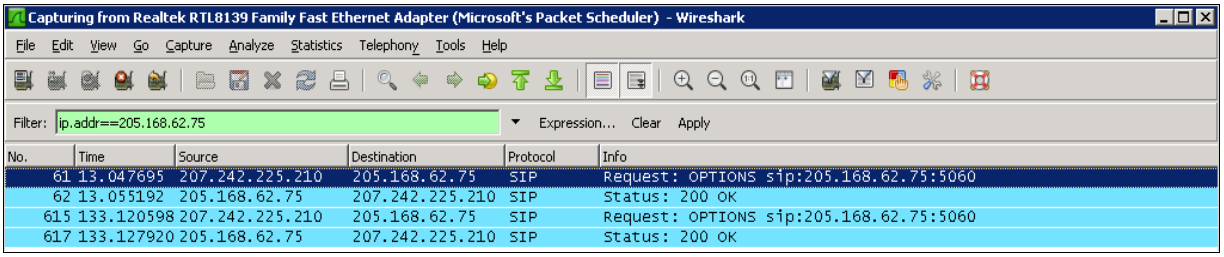
The following steps may be used to verify the configuration:

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 disconnect properly.
2. Place an inbound call to an agent or phone, but do not answer the call. Verify that the call covers to Modular Messaging voicemail. Retrieve the message from Modular Messaging. .

8.1. Sipera E-SBC Verification

8.1.1. Verify Sipera E-SBC Connectivity to AT&T IP Flexible Reach

Verify that your entity links from the E-SBC (205.168.62.75) to AT&T IP Flexible Reach Service (207.242.225.210) are up and communicating with SIP OPTION messages and a response message.



Capturing from Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler) - Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Help
Expression...
Clear
Apply

Filter: ip.addr==205.168.62.75

```
No.   Time        Source           Destination      Protocol  Info
   61 13.047695   207.242.225.210  205.168.62.75    SIP       Request: OPTIONS sip:205.168.62.75:5060
   62 13.055192   205.168.62.75    207.242.225.210  SIP       Status: 200 OK
  615 133.120598  207.242.225.210  205.168.62.75    SIP       Request: OPTIONS sip:205.168.62.75:5060
  617 133.127920  205.168.62.75    207.242.225.210  SIP       Status: 200 OK
```

Figure 88: SIP OPTIONS Messages

8.2. Communication Manager Verifications

Verify that the signaling group / trunk group between the Communication Manager and Avaya Session Manager are up by using **status signaling-group** and **status trunk-group commands.**

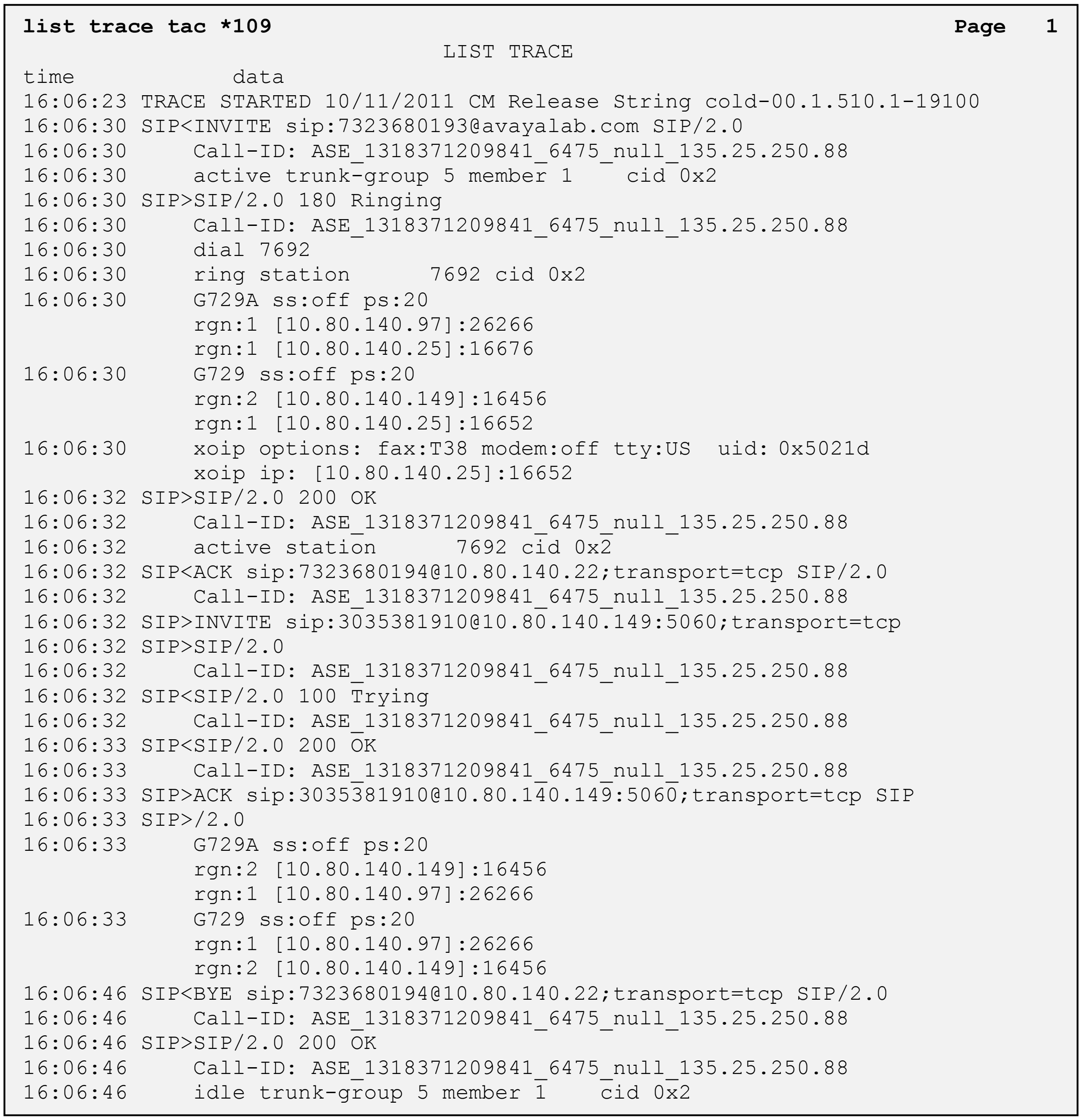
```
status signaling-group 5
                         STATUS SIGNALING GROUP
        Group ID: 1
      Group Type: sip
     Group State: in-service
```

Figure 89: Signaling Group Status

```
status trunk 5                                                      Page   1
                             TRUNK GROUP STATUS
Member   Port     Service State      Mtce Connected Ports
                                     Busy
0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00013   in-service/idle    no
0001/004 T00014   in-service/idle    no
```

Figure 90: Trunk Status

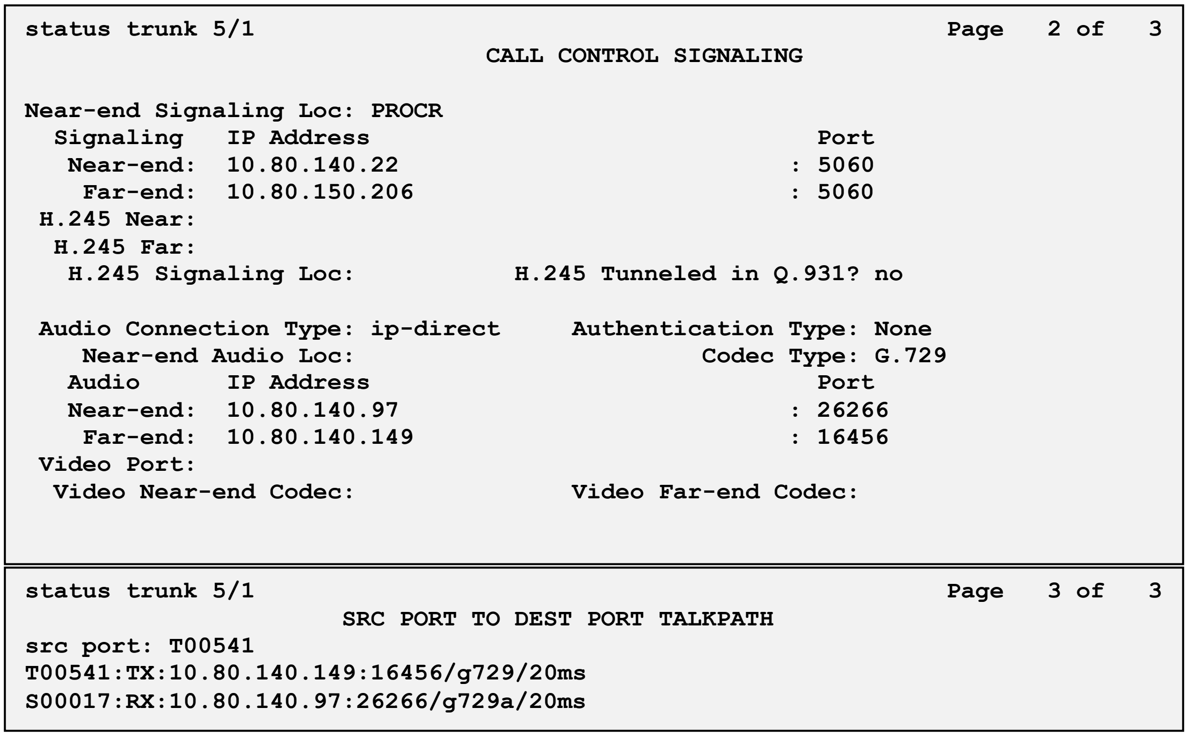
.



```
list trace tac *109                                                    Page   1
                                LIST TRACE
time            data
16:06:23 TRACE STARTED 10/11/2011 CM Release String cold-00.1.510.1-19100
16:06:30 SIP<INVITE sip:7323680193@avayalab.com SIP/2.0
16:06:30     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:30     active trunk-group 5 member 1    cid 0x2
16:06:30 SIP>SIP/2.0 180 Ringing
16:06:30     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:30     dial 7692
16:06:30     ring station      7692 cid 0x2
16:06:30     G729A ss:off ps:20
             rgn:1 [10.80.140.97]:26266
             rgn:1 [10.80.140.25]:16676
16:06:30     G729 ss:off ps:20
             rgn:2 [10.80.140.149]:16456
             rgn:1 [10.80.140.25]:16652
16:06:30     xoip options: fax:T38 modem:off tty:US  uid: 0x5021d
             xoip ip: [10.80.140.25]:16652
16:06:32 SIP>SIP/2.0 200 OK
16:06:32     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:32     active station      7692 cid 0x2
16:06:32 SIP<ACK sip:7323680194@10.80.140.22;transport=tcp SIP/2.0
16:06:32     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:32 SIP>INVITE sip:3035381910@10.80.140.149:5060;transport=tcp
16:06:32 SIP>SIP/2.0
16:06:32     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:32 SIP<SIP/2.0 100 Trying
16:06:32     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:33 SIP<SIP/2.0 200 OK
16:06:33     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:33 SIP>ACK sip:3035381910@10.80.140.149:5060;transport=tcp SIP
16:06:33 SIP>/2.0
16:06:33     G729A ss:off ps:20
             rgn:2 [10.80.140.149]:16456
             rgn:1 [10.80.140.97]:26266
16:06:33     G729 ss:off ps:20
             rgn:1 [10.80.140.97]:26266
             rgn:2 [10.80.140.149]:16456
16:06:46 SIP<BYE sip:7323680194@10.80.140.22;transport=tcp SIP/2.0
16:06:46     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:46 SIP>SIP/2.0 200 OK
16:06:46     Call-ID: ASE_1318371209841_6475_null_135.25.250.88
16:06:46     idle trunk-group 5 member 1    cid 0x2
```

Figure 91: Output for List Trace on the TAC for the Trunk Group

Figure 88 shows **Page 2 and 3** of the output of the **status trunk 5/1** command pertaining to the same call. Note the signaling using port 5060 between Communication Manager and the Session Manager. Note the media is "ip-direct" from the IP Telephone (10.80.140.97) to the inside IP Address of the Sipera E-SBC(10.80.140.149) using G.729, 20ms.



```
status trunk 5/1                                              Page   2 of   3
                                CALL CONTROL SIGNALING

Near-end Signaling Loc: PROCR
  Signaling   IP Address                                Port
   Near-end:  10.80.140.22                            : 5060
    Far-end:  10.80.150.206                           : 5060
 H.245 Near:
  H.245 Far:
   H.245 Signaling Loc:          H.245 Tunneled in Q.931? no

 Audio Connection Type: ip-direct     Authentication Type: None
    Near-end Audio Loc:                        Codec Type: G.729
   Audio      IP Address                                Port
   Near-end:  10.80.140.97                            : 26266
    Far-end:  10.80.140.149                           : 16456
 Video Port:
  Video Near-end Codec:              Video Far-end Codec:
```

```
status trunk 5/1                                              Page   3 of   3
                      SRC PORT TO DEST PORT TALKPATH
src port: T00541
T00541:TX:10.80.140.149:16456/g729/20ms
S00017:RX:10.80.140.97:26266/g729a/20ms
```

Figure 92: Status Trunk during an active call

8.3. Troubleshooting:

1. Communication Manager:
   - **list trace station** <extension number> - Traces calls to and from a specific station.
   - **list trace tac** <trunk access code number> - Traces calls over a specific trunk group.
   - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
   - **status trunk** <trunk access code number> - Displays trunk group information.
   - **status trunk** <trunk access code number/channel number> - Displays signaling and media information for an active trunk channel.
2. Sipera E-SBC
   - **check alarms** – click on the **Alarms** button in the UC-SEC Control Center
   - **incidents** – click on **Incidents** in the UC-SEC Control Center to view a complete descriptive list of all system incidents which have occurred since the last viewing period.
   - **diagnostics** – Click on **Diagnostics** in the UC-SEC Control Center, The **Diagnostics** screen provides a variety of tools to aid in troubleshooting UC-Sec operation. Available tools include a full diagnostic test suite, as well as individual tabs to monitor certain functional aspects of the UC-Sec, such as TCP and TLS activity.

- **statistics -** provides a snap-shot display of certain cumulative, system-wide generic and SIP-specific operational information. The various **Statistics** tabs (**Calls**, **Policy**, and **Protocol**) can be displayed whenever up-to-date statistical information is required.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Session Manager, Avaya Communication Manager and the Sipera E-SBC to AT&T IP Flexible Reach Service. AT&T IP Flexible Reach Service with Sipera passed compliance testing. Please refer to **Section 2.2** for any exceptions or workarounds.

10. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager*, (Aug 2010), Document Number 03-300509.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 6.0, 555-245-205, Issue 8.0, June 2010

[3] *Installing and Configuring Avaya Aura® Session Manager,* Doc ID 03-603473 Release 6.

[4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Release 6.0, June 2010

[5] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.2.x,* February 2010, Document Number 16-601443.

[6] *4600 Series IP Telephone LAN Administrator Guide,* October 2007, Document Number 555-233-507.

[7] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide,* November 2009, Document Number 16-300698.

[8] *Avaya one-X® Communicator Getting Started, November 2009.*

[9] *Modular Messaging Multi-Site Guide Release 5.1*, June 2009

[10] *Modular Messaging for Microsoft Exchange Release 5.1 Installation and Upgrades*, June 2009

[11] *Modular Messaging for the Avaya Message Storage Server (MSS) Configuration Release 5.1 Installation and Upgrades*, June 2009

[12] *Modular Messaging for IBM Lotus Domino 5.1 Installation and Upgrades*, June 2009

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

[14] RFC 3261 *SIP: Session Initiation Protocol,* http://www.ietf.org/

[15] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, http://www.ietf.org/

[16] RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, http://www.ietf.org/

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.