



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura[®] Communication Manager R6.2, Avaya Aura[®] Session Manager R6.2 and Avaya Session Border Controller Advanced for Enterprise R4.0.5 to Support IntelPeer SIP Trunk Service using TLS transport – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between IntelPeer SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager, Avaya Aura[®] Communication Manager and Avaya Session Border Controller Advanced for Enterprise. IntelPeer is a member of the DevConnect Global SIP Service Provider program.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Note: This Application Note is applicable with Avaya Aura[®] 6.2 which is currently in Controlled Introduction. Avaya Aura[®] 6.2 will be Generally Available in Summer 2012.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between IntelPeer SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager (SM), Avaya Aura[®] Communication Manager (CM) Evolution Server and Avaya Session Border Controller Advanced for Enterprise (ASBCAE). Customers using this Avaya SIP-enabled enterprise solution with the IntelPeer SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Session Manager, Communication Manager and the Avaya Session Border Controller Advanced for Enterprise. The enterprise site was configured to use the SIP Trunk Service provided by IntelPeer .

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by IntelPeer . Incoming PSTN calls were made to H.323, SIP, Digital and Analogue telephones at the enterprise.
- Outgoing calls from the enterprise site were completed via IntelPeer to the PSTN. Outgoing calls from the enterprise to the PSTN were made from H.323, SIP, Digital and Analogue telephones.
- Calls using G.729A and G.711A codec's
- Transport Layer Security (TLS) protocol is used to provide a secure channel by encrypting communications over IP networks
- DTMF transmission using RFC 2833 with successful Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media (also known as “shuffling”) with SIP and H.323 telephones was used during this test.
- Avaya one-X[®] Communicator was used to test soft client functionality
- Inbound and Outbound fax was tested using T.38 standard

- Call coverage and call forwarding for endpoints at the enterprise site.

Items supported but not tested included the following:

- Inbound toll-free, 411 and emergency calls (911) are supported but were not tested as part of the compliance test.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the IntelPeer SIP Trunk Service with the following observations:

- The calls were delivered to the ASBCAE using SIP over TLS
- All tests were completed using H.323, SIP, Digital and Analogue phone types. The Avaya one-X® Communicator was used to test soft client functionality.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Inbound and Outbound fax was tested using T.38 standard.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit

<http://support.avaya.com>

For technical support on IntelPeer products please contact an authorized IntelPeer representative at:

www.intelepeer.com or 1 877.336.9171

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the IntelPeer SIP Trunk Service. Located at the enterprise site is a Session Manager, Communication Manager, and the Avaya Session Border Controller Advanced for Enterprise. Endpoints are Avaya 9600 series IP telephones (SIP and H.323), Avaya 2400 series Digital telephone, a PC running one-X Communicator, an Analogue telephone and Fax Machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

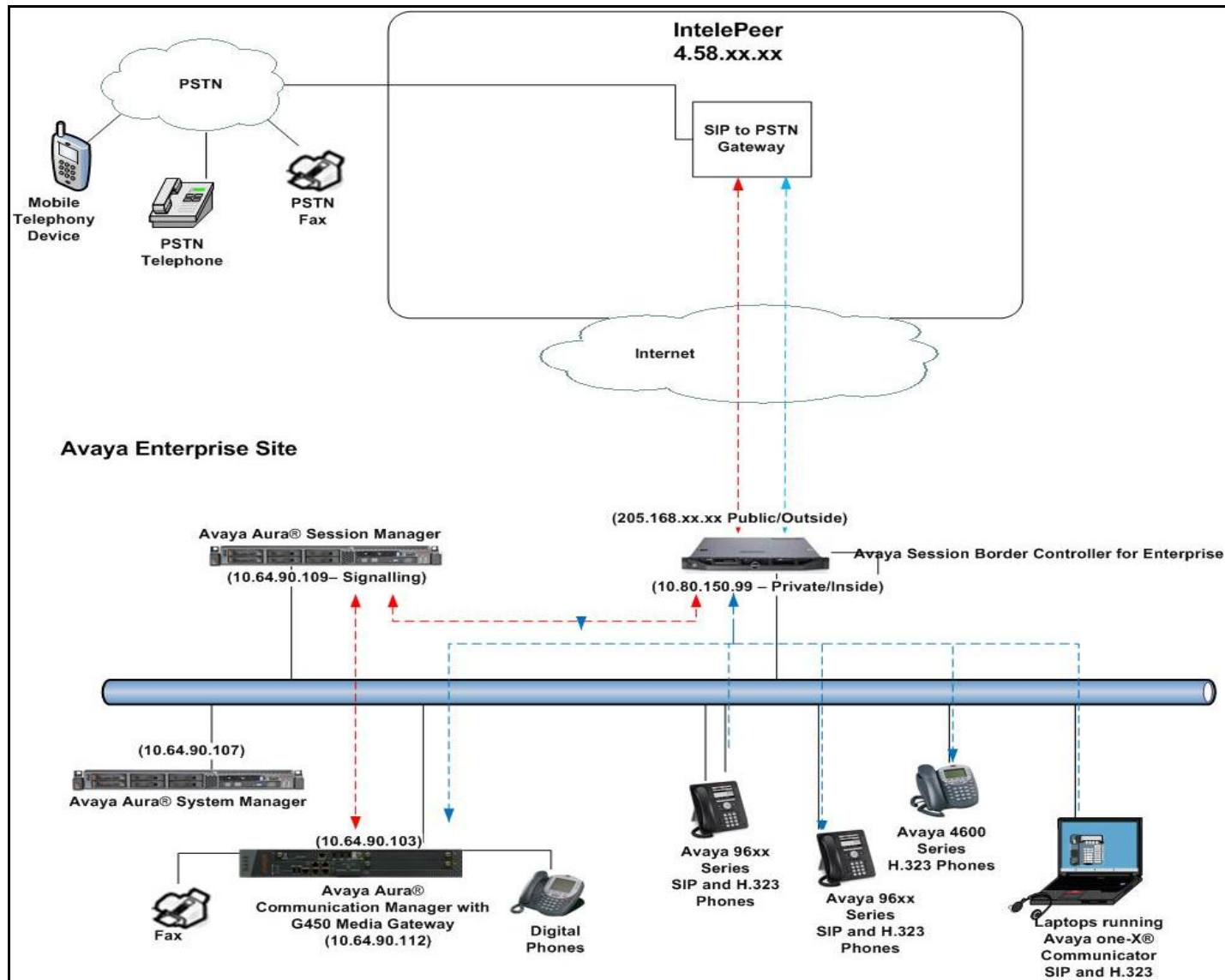


Figure 1: IntelPeer SIP Solution Topology

For inbound calls, the calls flow from the service provider to the ASBCAE and then to Session Manager. Session Manager uses the configured dial patterns and routing policies to determine the recipient (in this case Communication Manager) and on which link to send the call. Once the call arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager uses configured dial patterns to determine the route to the ASBCAE. From the ASBCAE, the call is sent to the PSTN via the IntelPeer SIP Trunk service.

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment	Software
Avaya Aura® Communication Manager	Release 6.2 load 823.0
Avaya Aura® System Manager	Release 6.2 Version 6.2.12.0
Avaya Aura® Session Manager	Release 6.2 Version 6.2.0.0.620118
G450 Gateway	3.1.20.1
Avaya Session Border Controller for Enterprise	4.0.5Q02
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.103S
Avaya 9600-Series Telephones (SIP)	96xx-IPT-SIP-R2_6_6_0-102111
Avaya 96X1- Series Telephones (SIP)	96x1-IPT-SIP-R6_0_3-120511
Avaya 9641 IP Telephone (H.323)	Avaya one-X® Deskphone SIP Edition 6.0.3
Avaya One-X Communicator (H.323)	6.1.3.08_SP3-Patch2-35791
Avaya 2400-Series and 6400-Series Digital Telephones	N/A
Intelpeer	Firmware
Sonus GSX9000 SBC	V07.03.04 S003

Table 1: Equipment and Software Used in the Sample Configuration

5. Configure Avaya Aura® Communication Manager Release 6.2

This section describes the steps for configuring Communication Manager for SIP Trunking. SIP trunks are established between Communication Manager and Session Manager. These SIP trunks will carry SIP Signaling associated with the IntelPeer SIP Trunk Service. For incoming calls, Session Manager receives SIP messages from IntelPeer and directs the incoming SIP messages to Communication Manager. Once the message arrives at Communication Manager, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed.

All outgoing calls to the PSTN are processed within Communication Manager and may be first subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects a SIP trunk, the SIP signaling is routed to Session Manager. Session Manager directs the outbound SIP messages to the ASBCAE and then to the IntelPeer network. 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. The general installation of the Avaya Servers and Avaya G450 Media Gateway is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

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. Use the **display system-parameters customer-options** command, and on **Page 2** verify that the **Maximum Administered SIP Trunks** supported by the system is sufficient for the combination of trunks to the IntelPeer network, and any other SIP trunks used.

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	2
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	128	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:	12000	275

On **Page 4**, verify that **IP Trunks** field is set to **y**.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	IP Stations? y	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	ISDN-PRI? y	
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. Administer IP Node Names

The node names defined here will be used in other configuration screens to define a SIP signaling group between Communication Manager and Session Manager. Type **change node-names ip** to make changes to the **IP Node Names**. In the **node-names-ip** form, assign the node **Name** and **IP Address** for the Session Manager. In this case, **SM** and **10.64.90.109** are the **Name** and **IP Address** for the Session Manager. Also note the **procr** IP address as this is the interface that Communication Manager will use as the SIP signaling interface to Session Manager.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM	10.64.90.109	
SiperaSBC	10.64.19.100	
default	0.0.0.0	
procr	10.64.90.103	
procr6	::	

5.3. Administer IP Network Region

Use the **change ip-network-region 1** command to set the following values:

- The **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **avayalab.com**
- By default, **IP-IP Direct Audio** (both **Intra-region** and **Inter-region**) is set to yes to allow audio traffic to be sent directly between endpoints without using gateway VoIP resources
- The **Codec Set** is set to the number of the IP codec set to be used for calls within the IP network region. In this case, codec set **1** was used

```
change ip-network-region 1                                     Page 1 of 20
                                                              IP NETWORK REGION
Region: 1
Location: Authoritative Domain: avayalab.com
Name: Region: 1
MEDIA PARAMETERS                                             Intra-region IP-IP Direct Audio: yes
Codec Set: 1                                                 Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                           IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS                                           AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y                                RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

5.4. Administer IP Codec Set

Use the **change ip-codec-set** command for the codec set specified in the **IP Network Region** form in **Section 5.3**. Enter the list of audio codec's eligible to be used in order of preference. For the compliance test, the codecs supported by IntelPeer were configured, namely **G.711MU** and **G.729A**.

```
change ip-codec-set 1                                         Page 1 of 2
                                                              IP Codec Set
Codec Set: 1
Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.722-64K      2          20
2: G.711MU        n          2          20
3: G.729A        n          2          20
4:
```


Set the **Fax Mode** to **t.38-standard** on **Page 2** of the codec set form as shown below.

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

5.5. Administer SIP Signaling Groups

Add a signaling group and trunk group for inbound and outbound PSTN calls to IntelPeer SIP Trunk Service. For the compliance test, these were configured using TLS (Transport Layer Security) and a TLS port of 5071 rather than the default TLS port of 5061. Configure the **Signaling Group** using the **add signaling-group n** command, where **n** is an available signaling group, as follows:

- Set the **Group Type** field to **sip**
- The **Transport Method** field is set to **tls**
- Set the **Near-end Node Name** to the processor interface (node name **procr**). This value is taken from the **IP Node Names** form shown in **Section 5.2**
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM**), also shown in **Section 5.2**
- Ensure that the TLS port value of **5071** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields
- In the **Far-end Network Region** field, enter the IP Network Region configured in **Section 6.2**. This field logically establishes the far-end for calls using this signaling group as network region **1**
- Enter the **Far-end Domain**. For the compliance test, the **Far-end Domain** was set to **avayalab.com**.
- The **Direct IP-IP Audio Connections** field is set to **y**
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833

The default values for the other fields may be used.

Add signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5071	Far-end Listen Port: 5071	
	Far-end Network Region: 2	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

5.6. Administer SIP Trunk Group

A trunk group is associated with the signaling group described in **Section 5.5**. Configure the trunk group using the **add trunk-group n** command, where **n** is an available trunk group. On **Page 1** of this form:

- Set the **Group Type** field to **sip**
- Choose a descriptive **Group Name**
- Specify a trunk access code (**TAC**) consistent with the dial plan, i.e. ***02**
- The **Direction** is set to **two-way** to allow incoming and outgoing calls
- Set the **Service Type** field to **public-ntwrk**
- Set **Member Assignment Method** to **auto**
- Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously configured in **Section 5.5**
- Specify the **Number of Members** supported by this SIP trunk group

Add trunk-group 2		Page 1 of 21
TRUNK GROUP		
Group Number: 2	Group Type: sip	CDR Reports: y
Group Name: SIP SP 2	COR: 1	TN: 1 TAC: *02
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: 2	
	Number of Members: 10	

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed upon with IntelPeer to prevent unnecessary SIP messages during call setup. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

Add trunk-group 2	Page 2 of 21
Group Type: sip	
TRUNK PARAMETERS	
Unicode Name: auto	
Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 600	
Disconnect Supervision - In? y Out? y	
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end.

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section Error! Reference source not found.**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

Add trunk-group 2	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
Maintenance Tests? y	
Numbering Format: public	
UII Treatment: service-provider	
Replace Restricted Numbers? y	
Replace Unavailable Numbers? y	
Modify Tandem Calling Number: tandem-cpn-form	
Show ANSWERED BY on Display? y	

On **Page 4**, set the **Network Call Redirection** field to **n** since Intelepeer does not support REFER. Set the **Send Diversion Header** field to **y**. This field will add a Diversion header and 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 **Support Request History** field to **y** to allow trunk to trunk transfers. Set the **Telephone Event Payload Type** to **101**, the value preferred by Intelepeer.

Add trunk-group 2	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: 101	

5.7. Administer Calling Party Number Information

In this section the Calling Party Number sent when making a call using the SIP trunk is specified.

5.7.1.Set Private Numbering

Use the **change private-numbering 1** command to configure Communication Manager to send the calling party number. In the sample configuration, all stations with a **5**-digit extension beginning with **12** and **13** will send the calling party number **30355591xx** to IntelePeer SIP Trunk Service. This calling party number will be sent in the SIP From, Contact and PAI headers, and displayed on display-equipped PSTN telephones. Public DID numbers have been masked for security purposes.

change public-unknown-numbering 1				Page 1 of 2	
NUMBERING - PUBLIC/UNKNOWN FORMAT					
		Total			
Ext	Ext	Trk	CPN	CPN	
Len	Code	Grp(s)	Prefix	Len	
					Total Administered: 1
5	12000	2	3035559132	10	
5	12003	2	3035559131	10	
5	12004	2	3035559130	10	
5	13000	2	3035559133	10	
5	13004	2	3035559134	10	

5.8. Administer Route Selection for Outbound Calls

In these Application Notes, the Automatic Route Selection (ARS) feature will be used to route outbound calls via the SIP trunk to IntelPeer SIP Trunk Service. In the sample configuration, the single digit **9** is used as the ARS access code. Avaya telephone users will dial **9** to reach an outside line. Use the **change feature-access-codes** command to configure or observe **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:	*10	
Abbreviated Dialing List2 Access Code:	*12	
Abbreviated Dialing List3 Access Code:	*13	
Abbreviated Dial - Prgm Group List Access Code:	*14	
Announcement Access Code:	*19	
Answer Back Access Code:		
Auto Alternate Routing (AAR) Access Code:	*00	
Auto Route Selection (ARS) - Access Code 1:	9	Access Code 2:
Automatic Callback Activation:	*33	Deactivation: #33
Call Forwarding Activation Busy/DA:	*30 All: *31	Deactivation: #30

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. A small sample of dial patterns are illustrated here. Further administration of ARS is beyond the scope of these Application Notes. The example entries shown will match outgoing calls to numbers beginning with **1**. Calls are sent to **Route Pattern 1**, which contains the previously configured SIP Trunk Group. All other entries are shown only as examples.

change ars analysis 1						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 0	
	Dialed String	Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
1		11	11	1	fnpa		n
1303		11	11	1	fnpa		n
1502		11	11	1	fnpa		n
1720		11	11	1	fnpa		n
1800		11	11	1	fnpa		n
1866		11	11	1	fnpa		n
1877		11	11	1	fnpa		n
1888		11	11	1	fnpa		n
1908		11	11	1	fnpa		n

Use the **change route-pattern** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, route pattern **1** is used to route calls to trunk group **2** {Grp No).

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

5.9. Administer Incoming Digit Translation

This step configures the settings necessary to map incoming DID calls to the proper Communication Manager extension(s). The incoming digits sent in the INVITE message from IntelPeer can be manipulated as necessary to route calls to the desired extension. In the examples used in the compliance testing, the incoming DID numbers provided by IntelPeer correlate to the internal extensions assigned within Communication Manager. The entries displayed below translate incoming DID numbers **30355591xx** to a 5 digit extension by deleting all of the incoming digits and inserting an extension. Public DID numbers have been masked for security purposes.

change inc-call-handling-trmt trunk-group 2					Page	1 of	30
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	11	13035559130	11	12000			
public-ntwrk	10	3035559130	10	12000			
public-ntwrk	10	3035559131	10	12003			
public-ntwrk	10	3035559132	10	12004			
public-ntwrk	10	3035559133	10	13000			
public-ntwrk	10	3035559134	10	13004			

Save Communication Manager changes by entering **save translation** to make them permanent.

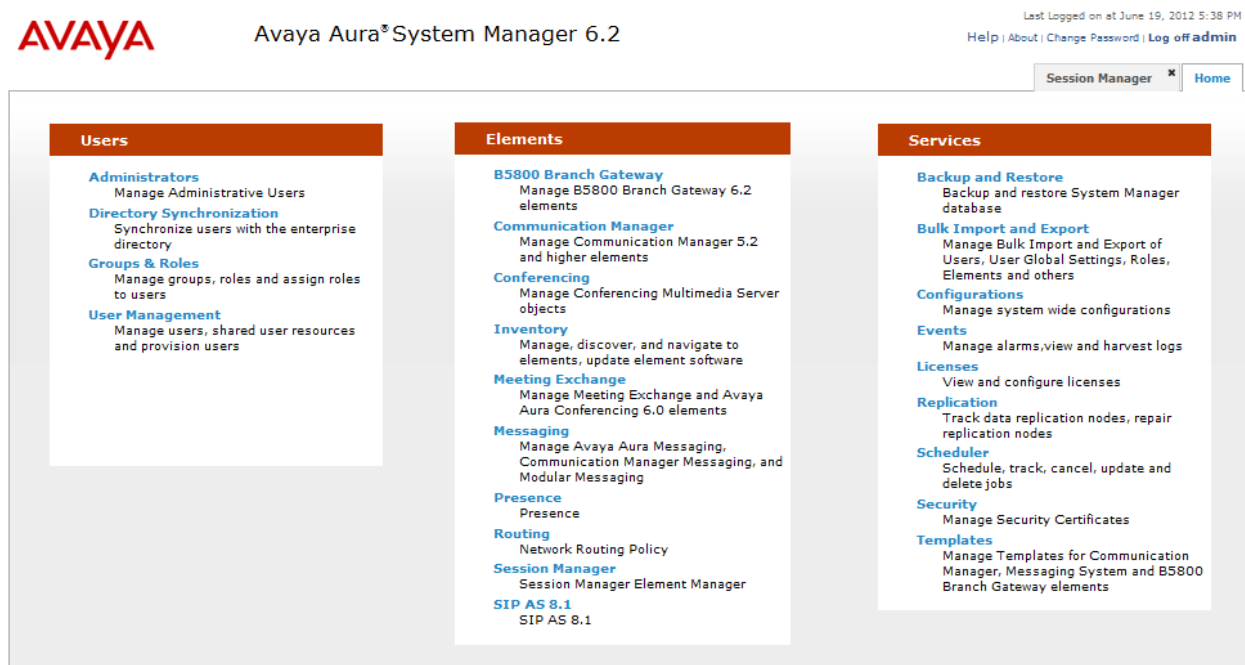
6. Configuring Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP domain
- Administer SIP Location
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Aura® Communication Manager as Managed Element
- Administer Application for Avaya Aura® Communication Manager
- Administer Application Sequence for Avaya Aura® Communication Manager
- Administer SIP Extensions

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where <FQDN> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the Home tab will be presented with menu options shown below.



6.2. Administer SIP domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu (not shown) and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avayalab.com**). Click **Commit** to save changes (not shown).

The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.2", and a user status bar indicating "Last Logged on at June 19, 2012 5:38 PM" with links for "Help", "About", "Change Password", and "Log off admin". The left sidebar contains a menu with "Routing" selected, and sub-items: "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The main content area is titled "Home / Elements / Routing / Domains" and shows "Domain Management" with buttons for "Edit", "New", "Duplicate", "Delete", and "More Actions". Below this is a table with columns "Name", "Type", "Default", and "Notes". One item is listed: "avayalab.com" with type "sip" and "Default" set to "No". A "Select: All, None" option is at the bottom left of the table.

6.3. Administer Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, * is used to specify any number of allowed characters at the end of the string. Click **Commit** to save changes. Below is the location configuration used for the simulated enterprise.

The screenshot shows the Avaya Aura System Manager 6.2 interface for the "Locations" configuration page. The top navigation bar is identical to the previous screenshot. The left sidebar shows "Routing" selected, with "Locations" highlighted in the sub-menu. The main content area is titled "Home / Elements / Routing / Locations" and shows "Location Details" with "Commit" and "Cancel" buttons. The "General" section contains fields for "Name" (set to "Location_1") and "Notes" (set to "Location 1 SM"). The "Overall Managed Bandwidth" section includes a "Managed Bandwidth Units" dropdown set to "Kbit/sec", and input fields for "Total Bandwidth" and "Multimedia Bandwidth". A checkbox "Audio Calls Can Take Multimedia Bandwidth" is checked. The "Per-Call Bandwidth Parameters" section includes input fields for "Maximum Multimedia Bandwidth (Intra-Location)" (1000 Kbit/Sec), "Maximum Multimedia Bandwidth (Inter-Location)" (1000 Kbit/Sec), "Minimum Multimedia Bandwidth" (64 Kbit/Sec), and "Default Audio Bandwidth" (80 Kbit/Sec).

6.4. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **CM** for a Communication Manager SIP entity, and **Gateway** for the SBC SIP entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Session Border Controller SIP Entity

6.4.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signaling interface.

The screenshot shows the 'SIP Entities' configuration page in the Avaya Aura interface. The left sidebar contains a menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and 'General'. It contains the following fields:

- Name:** ASM62
- FQDN or IP Address:** 10.64.90.109
- Type:** Session Manager (dropdown menu)
- Notes:** (empty text field)
- Location:** Location_1 (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/Denver (dropdown menu)
- Credential name:** (empty text field)

At the bottom, there is a 'SIP Link Monitoring' section with a dropdown menu set to 'Use Session Manager Configuration'. In the top right corner, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

Session Manager must be configured with port numbers for the protocols that will be used by the other SIP entities. To configure these, scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number (5061) on which the system listens for SIP requests
- In the **Protocol** field enter the transport protocol (TLS) to be used for SIP requests
- In the **Default Domain** field, from the drop down menu select **avayalab.com** as the default domain

Port

TCP Failover port:

TLS Failover port:

2 Items Refresh Filter: Enable

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

Select : All, None

6.4.2. Avaya Aura[®] Communication Manager SIP Entity

The following screens show the SIP entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the interface that will be providing SIP signaling for Communication Manager. The entity **Type** is set to **CM**.

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: CM62_TG3

* FQDN or IP Address: 10.64.90.103

Type: CM

Notes: SIP Phones

Adaptation:

Location: Location_1

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

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

Entity Links

6.4.3. Avaya Session Border Controller Advanced for Enterprise SIP Entity

The following screen shows the SIP entity for the Avaya Session Border Controller Advanced for Enterprise used for routing fixed and mobile calls. The **FQDN or IP Address** field is set to the IP address of the private interface administered in **Section 7** of this document.

AVAYA Avaya Aura*System Manager 6.2

Last Logged on at June 19, 2012 5:38 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: ASBCAE

FQDN or IP Address: 10.64.19.100

Type: SIP Trunk

Notes: Avaya SBC

Adaptation: [dropdown]

Location: AvayaSBC

Time Zone: America/Denver

Override Port & Transport with DNS SRV: [checkbox]

SIP Timer B/F (in seconds): 4

Credential name: [text field]

Call Detail Recording: egress [dropdown]

Commit Cancel

6.5. Administer Entity Links

A SIP trunk between Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button . Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name
- In the **SIP Entity 1** field select **SessionManager**
- In the **Port** field enter the port number to which the other system sends its SIP requests
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.4**
- In the **Port** field enter the port number to which the other system expects to receive SIP requests
- Select the **Trusted** tick box to make the other system trusted
- In the **Protocol** field enter the transport protocol to be used to send SIP requests

Click **Commit** (not shown) to save changes. The following screen shows the Entity Links used in this configuration.



Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Home / Elements / Routing / Entity Links

Entity Links

Help ?

Commit Cancel

1 Item Refresh

Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM62_cm62_tg2_50	* ASM62	TLS	* 5071	* cm62_tg2	* 5071	Trusted	

* Input Required

Commit Cancel

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Home / Elements / Routing / Entity Links

Entity Links

Help ?

Commit Cancel

1 Item Refresh

Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM62_CM62_TG3_5	* ASM62	TLS	* 5061	* CM62_TG3	* 5061	Trusted	

* Input Required

Commit Cancel

6.6. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- Enter an informative name in the **Name** field
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies

The following screen shows the routing policy for Communication Manager:

Home / Elements / Routing / Routing Policies

Routing Policy Details [Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
cm62_tg2	10.64.90.103	CM	trunk grp to SP

The following screen shows the routing policy for the Avaya Session Border Controller Advanced for Enterprise:

Home / Elements / Routing / Routing Policies

Routing Policy Details [Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
ASBCE	10.64.19.100	SIP Trunk	Avaya SBC

6.7. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select **–Avayalab.com**

Under **Originating Locations and Routing Policies**, click **Add**. In the resulting screen (not shown) under **Originating Location** select **Locations**, created in **Section 6.3**, and under **Routing Policies** select one of the routing policies defined in **Section 6.6**. Click **Select** button to save (not shown). The following screens show an example dial pattern configured for IntelPeer SIP Trunk Service.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.2", and a user status bar indicating "Last Logged on at June 19, 2012 5:38 PM" with links for "Help", "About", "Change Password", and "Log off admin". The left sidebar contains a menu with "Routing" selected, showing sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled "Home / Elements / Routing / Dial Patterns" and shows the "Dial Pattern Details" form. The "General" tab is active, displaying fields for "Pattern" (value: 1), "Min" (value: 11), "Max" (value: 11), "Emergency Call" (checkbox), "Emergency Priority" (value: 1), "Emergency Type" (text field), "SIP Domain" (dropdown menu showing "avayalab.com"), and "Notes" (value: 1 + Outbound). Below the form is the "Originating Locations and Routing Policies" section, which includes "Add" and "Remove" buttons and a table with one item. The table has columns for "Originating Location Name", "Originating Location Notes", "Routing Policy Name", "Rank", "Routing Policy Disabled", "Routing Policy Destination", and "Routing Policy Notes". The single row shows "Location_1", "Location 1 SM", "To-ASBCAE", "0", an unchecked "Routing Policy Disabled" checkbox, "ASBCE", and "To Avaya SBC". A "Filter: Enable" link is in the top right of the table area. At the bottom of the table area, it says "Select : All, None".

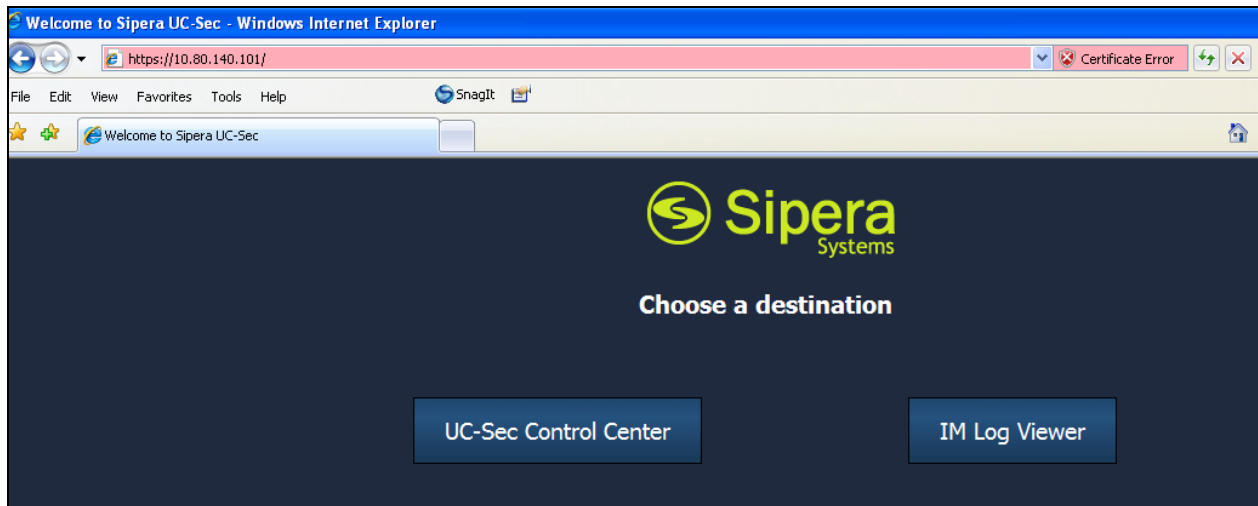
Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Location_1	Location 1 SM	To-ASBCAE	0	<input type="checkbox"/>	ASBCE	To Avaya SBC

7. Avaya Session Border Controller Advanced for Enterprise Configuration

This section provides the procedures for configuring the Avaya Session Border Controller Advanced or Enterprise.

7.1. Accessing UC-Sec Control Centre

Access the web interface by typing **https://x.x.x.x**, where x.x.x.x is the management IP of the SBC-AE.



Select **UC-Sec Control Center** and enter the **Login ID** and **Password**.



7.2. Installing TLS Certificate

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote users.

Managing TLS parameters consists of generating and installing a Certificate Signing Request (CSR), installing a Certificate Authority (CA) certificate, and installing the Certificate Revocation List (CRL). Once these procedures are completed, you must create a client profile and a server profile.

It is assumed generating of the Certificates have been previously completed and is not discussed here.

The following paragraph is an overview of the mutual certificate authentication that is being used for this application :

For the Avaya side of the SBC

- SM has certs “B” and “CAa” uploaded.
- SBC has certs “A” and “CAb” uploaded.
- During the TLS authentication process/handshake, certificate “A” is sent from the SBC to Session Manager. CA certificate “CAa” is used by Session Manager to validate certificate “A”.
- Session Manager sends certificate “B” to the SBC. CA certificate “CAb” is used by the SBC to validate certificate “B”.

For the IntelPeer side of the SBC

- IntelPeer has certs “D” and “CAc” uploaded.
- SBC has certs “C” and “CAD” uploaded.
- During the TLS authentication process/handshake, certificate “C” is sent from the SBC to IntelPeer. CA certificate “CAc” is used by IntelPeer to validate certificate “C”.
- IntelPeer sends certificate “D” to the SBC. CA certificate “CAD” is used by the SBC to validate certificate “D”.

The following procedures show how to upload the Certificate, create client and server profiles. For generating the certificates refer to **Reference [08]**

From the lefthand menu select **TLS Management → Certificates** and click on **Install** button located in the upper-right hand.

- Enter **Certificate Name**:
- Click **Browse** button to navigate to the Certificate File.
- Click **Upload**

The following screen show the installed Certificates for both Avaya and IntelPeer.



7.2.1. Managing Client profiles-Avaya

- Select the **Client Profiles** under **TLS Management**
- Select **New Profile**
- Enter the requested information into the appropriate fields
- Click **Finish**

Edit Profile

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

Profile Name

Avaya_tls_client

Certificate

Avaya_RU.crt

Certificate Info

Peer Verification

Required

Peer Certificate Authorities

Avaya_rootCA.crt

IntelePeerCA.pem

Peer Certificate Revocation Lists

Verification Depth

1

Renegotiation Parameters

Renegotiation Time (seconds)

0

Renegotiation Byte Count

0

Cipher Suite Options

Ciphers

☒ All
☐ Strong
☐ Export Only
☐ Null Only (For Debugging)
☐ Custom

Options

☐ DH
☐ ADH
☐ MD5

Value [What's this?](#)

ALL:!DH:!ADH:!MD5

Finish

7.2.2. Managing Client profiles- IntelePeer

- Select the **Client Profiles** under TLS Management
- Select **New Profile**
- Enter the requested information into the appropriate fields
- Click **Finish**

Edit Profile

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

Profile Name

IntelPeer_tls_client

Certificate

Avaya_RU.crt

Certificate Info

Peer Verification

Required

Peer Certificate Authorities

Avaya_rootCA.crt

IntelPeerCA.pem

Peer Certificate Revocation Lists

Verification Depth

1

Renegotiation Parameters

Renegotiation Time (seconds)

0

Renegotiation Byte Count

0

Cipher Suite Options

Ciphers

☒ All
☐ Strong
☐ Export Only
☐ Null Only (For Debugging)
☐ Custom

Options

☒ DH
☒ ADH
☒ MD5

Value

ALL

Finish

7.2.3. Managing Server Profiles-Avaya

- Select the **Server Profiles** under TLS Management
- Select **New Profile**
- Enter the requested information into the appropriate fields
- Click **Finish**

PM; Reviewed:
SPOC 8/23/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

27 of 58
CMSM62ASBCAEInt

Edit Profile ✕

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

Profile Name	<input style="width: 90%;" type="text" value="Avaya_tls_server"/>
Certificate	<input style="width: 90%;" type="text" value="Avaya_RU.crt"/> ▼

Certificate Info

Peer Verification	<input style="width: 90%;" type="text" value="None"/> ▼
Peer Certificate Authorities	<div style="background-color: #ccc; padding: 2px;"> Avaya_rootCA.crt IntelePeerCA.pem </div>
Peer Certificate Revocation Lists	<div style="background-color: #ccc; height: 40px;"></div>
Verification Depth	<input style="width: 90%;" type="text" value="0"/>

Renegotiation Parameters

Renegotiation Time (seconds)	<input style="width: 90%;" type="text" value="0"/>
Renegotiation Byte Count	<input style="width: 90%;" type="text" value="0"/>

Cipher Suite Options

Ciphers	<input checked="" type="radio"/> All <input type="radio"/> Strong <input type="radio"/> Export Only <input type="radio"/> Null Only (For Debugging) <input type="radio"/> Custom
Options	<input checked="" type="checkbox"/> DH <input checked="" type="checkbox"/> ADH <input checked="" type="checkbox"/> MD5
Value What's this?	<input style="width: 90%;" type="text" value="ALL"/>

7.3. Global Profiles

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

7.3.1. Server Interworking- Avaya

Server Interworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add Profile**. Enter **Profile Name** and click **Next**.

- Check **Hold Support** to **None**
- Check **T.38 Support**

All other options on the **General** tab can be left at their default values. Click on **Next** on the following screens and then **Finish** (not shown).

Editing Profile: Lab2-Interworking

General

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

Next

7.3.2. Server Interworking – IntelPeer

Server Interworking allows you to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add Profile**. Enter **Profile Name** and click on **Next**.

- Check **Hold Support** to **None**
- Check **T.38 Support**

All other options on the **General** tab can be left at their default values. Click on **Next** on the following screens and then **Finish** (not shown).

The screenshot shows a configuration window titled "Editing Profile: SIP-Trunk-2-IP" with a "General" tab. The window contains a list of settings with radio buttons or checkboxes. The "T.38 Support" option is checked. A "Next" button is at the bottom right.

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

Next

7.3.3. Routing – Avaya

The **Routing Profile** allows you to manage parameters related to routing SIP signaling messages. From the left-hand menu select **Global Profiles → Routing** and click on **Add Profile**.

- Enter **Profile Name**:
- Hit **Next** (not shown)
- Set **Next Hop Server 1** to the Session Manager IP address (**10.64.90.109**)
- Select **Routing Priority Based on Next Hop Server**
- Set **Outgoing Transport** to **TLS**
- Click **Finish** (not shown)

The screen below is a result of the details configured above:

The screenshot shows the 'Global Profiles > Routing: To-SM62-Lab2' configuration page. On the left is a sidebar with a list of routing profiles: 'default', 'Route_to_SP1_CL', 'Route_to_CS1K', 'Route_to_CM-Lab2', 'Route_to_SP2_IP', 'To-SM62-Lab2' (highlighted), 'Route_to_Windstream', and 'Route_to_SM62-Lab1'. The main area has buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. Below these is a yellow bar with the text 'Click here to add a description.' and a tab labeled 'Routing Profile'. An 'Add Routing Rule' button is in the top right of the main area. A table displays the routing rule configuration:

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	*	10.64.90.109	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS

7.3.4. Routing – IntelPeer

The **Routing Profile** allows you to manage parameters related to routing SIP signaling messages. A routing profile must be set for fixed and mobile calls. From the left-hand menu select **Global Profiles → Routing** and click on **Add Profile**.

- Enter **Profile Name** as **IntelPeer**
- Hit **Next**
- Set **Next Hop Server 1** to the IP address provided by Intelpeer (**4.58.xx.xx:5061**)
- Select **Routing Priority Based on Next Hop Server**
- Set **Outgoing Transport** to **TLS**
- Click **Finish** (not shown)

The screen below is a result of the details configured above:

Global Profiles > Routing: Route_to_SP2_IP

[Add Profile](#) [Rename Profile](#) [Clone Profile](#) [Delete Profile](#)

Click here to add a description.

Routing Profile

[Add Routing Rule](#)

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	*	4.58. :5061	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TLS

7.3.5. Server Configuration– Avaya Aura® Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles** → **Server Configuration** and click on **Add Profile**. Enter **Profile Name**. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**
- Set **IP Addresses / Supported FQDNs** to the IP address of Session Manager (10.64.90.109)
- For **Supported Transports**, check **TLS**
- **TLS Port: 5061**
- Click on **Next** (not shown) to use default values for the **Authentication** and **Heartbeat** tabs.

Edit Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.64.90.109
Supported Transports	<input type="checkbox"/> TCP <input type="checkbox"/> UDP <input checked="" type="checkbox"/> TLS
TCP Port	
UDP Port	
TLS Port	5061
<div>Finish</div>	

On the **Advanced** tab:

- Select the Name given in section 7.3.1 for **Server Interworking Profile - Avaya**
- Select the name given in section 7.2.1 for **Client Profile - Avaya**
- Click **Finish**

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Lab2-Interworking
TLS Client Profile	Avaya_tls_client
Signaling Manipulation Script	None
TLS Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
<div>Finish</div>	

7.3.6. Server Configuration– IntelPeer side

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, server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles** → **Server Configuration** and click on **Add Profile**. Enter **Profile Name**. On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**
- Set **IP Addresses / Supported FQDNs** to the Intelpeer Trunk Server IP address (4.58.xx.xx)
- **Supported Transports**: Check **TLS**
- **TLS Port**: **5061**
- Click on **Next** (not shown) to use default values for the **Authentication** and **Heartbeat** tabs.

Edit Server Configuration Profile - General	
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	4.58.1
Supported Transports	<input type="checkbox"/> TCP <input type="checkbox"/> UDP <input checked="" type="checkbox"/> TLS
TCP Port	
UDP Port	
TLS Port	5061
Finish	

On the **Advanced** tab:

- Select the server name given in section 7.3.2. for **Server Internetworking Profile – IntelPeer**
- Select the TLS Client Profile name given in section 7.2.2 for **Client Profiles - IntelPeer**
- Select **Signaling Manipulation Script** given in section 7.3.7 (**SIP Trunk2_Script**)
- Click **Finish**

Edit Server Configuration Profile - Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SIP-Trunk-2-IP
TLS Client Profile	IntelPeer_tls_client
Signaling Manipulation Script	SIP Trunk2_Script
TLS Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
Finish	

7.3.7. Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will give the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCAE. Using this language, a script can be written and tied to a given flow through the EMS GUI. The Avaya SBCAE appliance then interprets this script at the given entry point or “hook point”.

These application notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding.

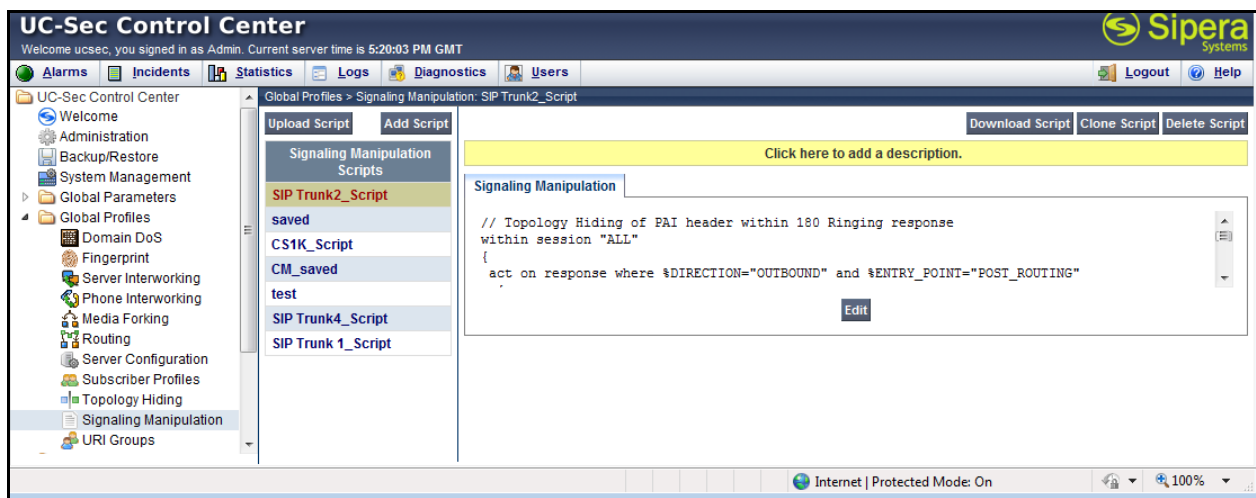
To create a new Signaling Manipulation script, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script** (not shown). A new blank SigMa Editor window will pop up. For more information on Signaling Manipulation see **Reference 0**.

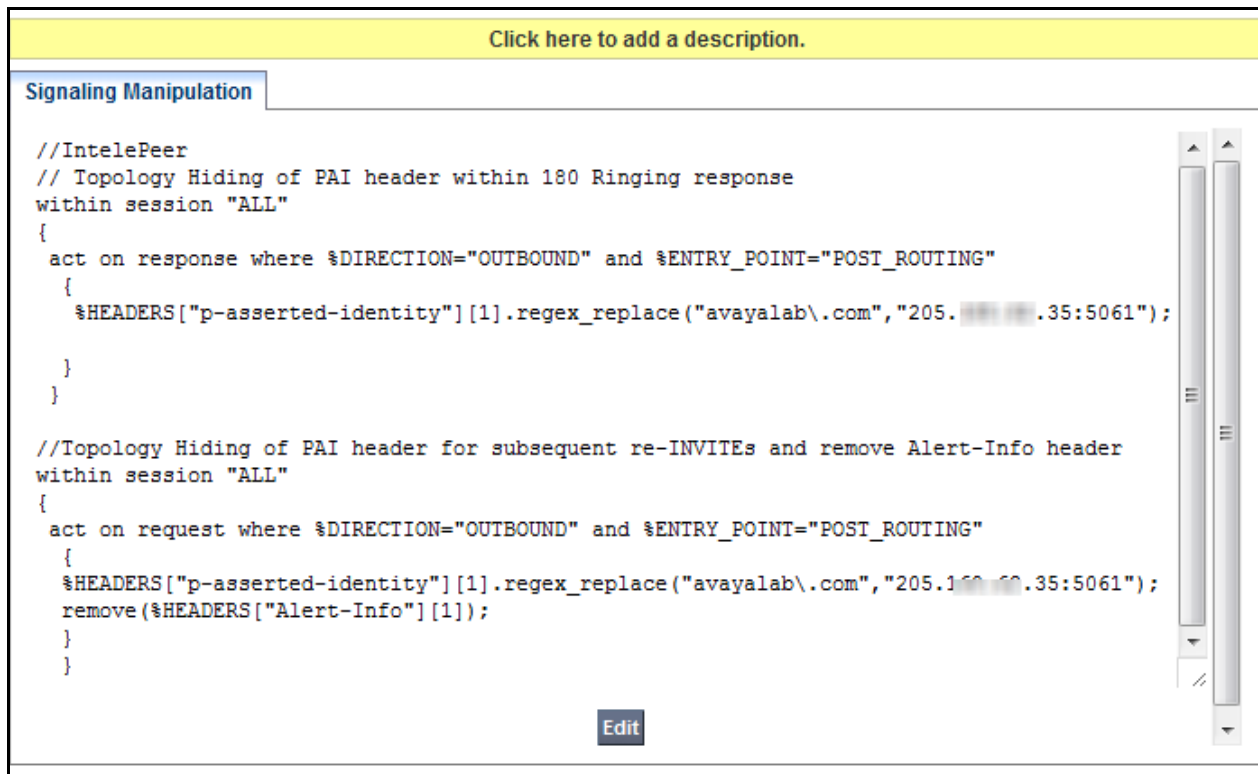
The following sample script is written in two sections. Each section begins with a comment describing what will take place in that portion of the script. The first section will act on the responses from Communication Manager to an inbound call from IntelPeer (e.g., 180 Ringing and 200 OK) while the second section acts on the requests of an outbound call to IntelPeer™ from Communication Manager (e.g., re-INVITE messages from Communication Manager for audio shuffling). The script is further broken down as follows:

- **within session “All”**
 - **act on response**
 - **%DIRECTION=“OUTBOUND”**
 - **%ENTRY_POINT=“POST_ROUTING”**
 - **%HEADERS[“p-asserted-identity”][1]**
 - **.regex_replace**
 (“avayalab\.com”, “205.xxx.xxx.35:5061”)
- Transformations applied to all SIP sessions.
 Actions to be taken to the response of an INVITE (e.g., 180 Ringing and 200 OK).
 Applied to messages leaving the Avaya SBCAE.
 The “hook point” to apply the script after the SIP message has routed through Avaya SBCAE.
 Used to retrieve an entire header. The first dimension denotes which header while the second dimension denotes the 1st instance of the header in a message.
 An action to replace a given match with the provided string (e.g., find “avayalab.com” and replace it with “205.xxx.xxx.35:5061”).

The P-Asserted-Identity header will be modified by replacing the domain “avayalab.com” with the external IP address of the Avaya SBCAE and the TLS SIP port of 5061 in both the response and request sessions.

The following screens show the **Signaling Manipulation** section with the script **SIP Trunk2_Script** already created, and the complete **SIP Trunk2_Script**:





The screen above shows the finished Signaling Manipulation Script **IntelPeer Script** (SIP Trunk2_Script).

7.3.8. 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. From the left-hand menu select **Global Profiles → Topology Hiding**.

- Click **default** profile and select **Clone Profile**
- Enter **Profile Name**. For the compliance test, **Enterprise** was chosen as the name of the **Topology Hiding Profile** for the enterprise.
- For the **Request-Line, To** and **From** headers, select **IP/Domain** under **Criteria**, **Overwrite** for **Replace Action**, and **avayalab.com** for **Overwrite Value**
- Remove all other entries
- Click **Finish**

The screen below is a result of the details configured above.

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

Finish

7.3.9. Topology Hiding – IntelPeer 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. From the left-hand menu select **Global Profiles → Topology Hiding**.

- Click **default** profile and select **Clone Profile**
- Enter **Profile Name**. For the compliance test, **SIP Trunk** was chosen as the name of the **Topology Hiding Profile** for the Service Provider.
- For the **Request-Line** header (and other headers) leave the default values of **IP/Domain** under **Criteria** and **Auto** under **Replace Action**
- Leave **Overwrite Value** as blank
- Click **Finish**

The screen below is a result of the details configured above:

Edit Topology Hiding Profile ✕

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

Finish

7.4. Domain Policies

The Domain policies maintain control over call flows entering or leaving the enterprise based upon wide range of conditions and parameters.

7.4.1. Domain Policies-Application-Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, you can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Create an Application Rule to set the number of concurrent voice traffic. The sample configuration cloned and modified the default application rule to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**. To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.

UC-Sec Control Center
 Welcome ucsec, you signed in as Admin. Current server time is 7:52:18 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
 - Application Rules
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules
 - Time of Day Rules
 - End Point Policy Groups
 - Session Policies
 - Device Specific Settings
 - Troubleshooting
 - TLS Management
 - IM Logging

Domain Policies > Application Rules: default

Add Rule

Filter By Device... **Clone Rule**

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	10
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None		
IM Logging	No		
RTCP Keep-Alive	No		

Edit

Enter a descriptive name for the new rule and click **Finish**.

Clone Rule

Rule Name	default
Clone Name	MaxVoice

Finish

Modify the rule by clicking the **Edit** button. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. Keep in mind Avaya SBCE takes 30 seconds for sessions to be cleared after disconnect. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. In the sample configuration, Communication Manager was programmed to control the concurrent sessions by setting the number of members in the trunk group (**Section Error! Reference source not found.**) to the allotted amount. Therefore, the values in the Application Rule **MaxVoice** were set high enough to be considered non-blocking.

The screenshot shows the UC-Sec Control Center interface. The left-hand navigation menu includes options like Welcome, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Time of Day Rules, End Point Policy Groups, Session Policies, Device Specific Settings, Troubleshooting, TLS Management, and IM Logging. The main area displays the configuration for the 'MaxVoice' Application Rule. The rule is set to 'Voice' with 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint' both set to 2000. The 'Miscellaneous' section shows 'CDR Support' as 'None', 'IM Logging' as 'No', and 'RTCP Keep-Alive' as 'No'. An 'Edit' button is visible at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

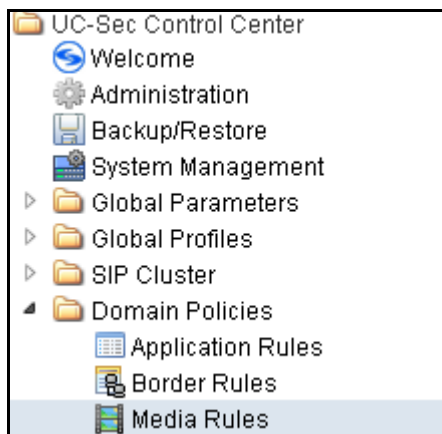
Miscellaneous			
CDR Support	None		
IM Logging	No		
RTCP Keep-Alive	No		

7.4.2. Domain Policies-Media Rules

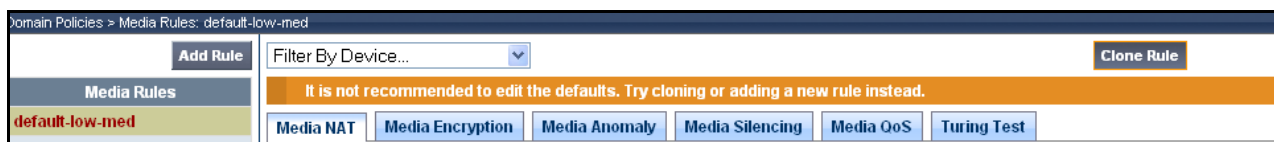
Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the UC-Sec security product.

Create a custom Media Rule to set the Quality of Service and Media Anomaly Detection. The sample configuration shows a custom Media Rule **No-Media-Detection** created for the enterprise and IntelPeer

Select **Domain Policies → Media Rules** from the left-side menu as shown below.



In the sample configuration, a single media rule was created by cloning the default rule called “default-low-med”. Select the default-low-med rule and click the **Clone Rule** button.



Enter a name in the **Clone Name** field, such as “New-Avaya-Enc” as shown below. Click **Finish**.



Select the newly created rule, select the **Media QoS** tab, and click the **Edit** button (not shown). In the resulting screen, check the **Media QoS Marking Enabled** checkbox. Select **DSCP** and select “EF” for expedited forwarding as shown below. Click **Finish**.

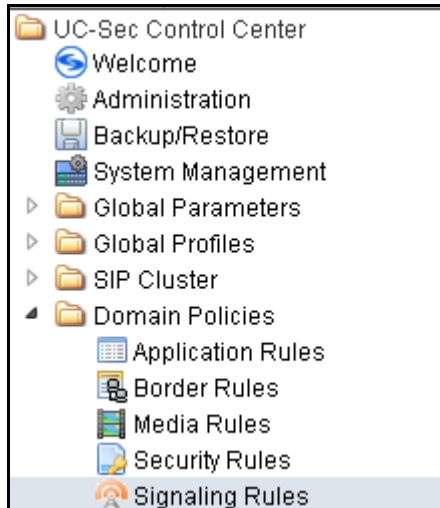
Media QoS			
Media QoS Reporting			
RTCP Enabled	<input type="checkbox"/>		
Media QoS Marking			
Enabled	<input checked="" type="checkbox"/>		
<input type="radio"/> ToS			
Audio Precedence	Routine		000
Audio ToS	Minimize Delay		1000
Video Precedence	Routine		000
Video ToS	Minimize Delay		1000
<input checked="" type="radio"/> DSCP			
Audio	EF		101110
Video	EF		101110
<input type="button" value="Finish"/>			

When configuration is complete, the “New-Avaya-Enc Media QoS” media rule **Media QoS** tab appears as follows.

Filter By Device...		Rename Rule	Clone Rule	Delete Rule						
Click here to add a description.										
Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS						
<table border="1"> <thead> <tr> <th colspan="2">Media QoS Reporting</th> </tr> </thead> <tbody> <tr> <td>RTCP Enabled</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>					Media QoS Reporting		RTCP Enabled	<input type="checkbox"/>		
Media QoS Reporting										
RTCP Enabled	<input type="checkbox"/>									
<table border="1"> <thead> <tr> <th colspan="2">Media QoS Marking</th> </tr> </thead> <tbody> <tr> <td>Enabled</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>QoS Type</td> <td>DSCP</td> </tr> </tbody> </table>					Media QoS Marking		Enabled	<input checked="" type="checkbox"/>	QoS Type	DSCP
Media QoS Marking										
Enabled	<input checked="" type="checkbox"/>									
QoS Type	DSCP									
<table border="1"> <thead> <tr> <th colspan="2">Audio QoS</th> </tr> </thead> <tbody> <tr> <td>Audio DSCP</td> <td>EF</td> </tr> </tbody> </table>					Audio QoS		Audio DSCP	EF		
Audio QoS										
Audio DSCP	EF									
<table border="1"> <thead> <tr> <th colspan="2">Video QoS</th> </tr> </thead> <tbody> <tr> <td>Video DSCP</td> <td>EF</td> </tr> </tbody> </table>					Video QoS		Video DSCP	EF		
Video QoS										
Video DSCP	EF									
<input type="button" value="Edit"/>										

7.4.3. Domain Policies – Signaling Rules

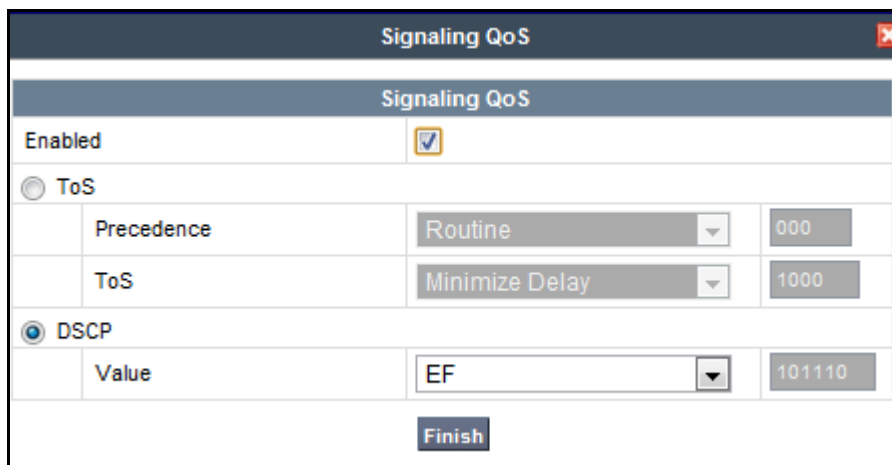
Select **Domain Policies** → **Signaling Rules** from the left-side menu as shown below:



Click the Add Rule button to add a new signaling rule. In the Rule Name field, enter an appropriate name, such as “Avaya”.



In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen, select **DSCP** and select the desired **Value** for Signaling QoS from the drop-down menu. In the sample configuration, “EF” was selected. Click **Finish** (not shown).



After this configuration, the new “Avaya” will appear as follows:

Filter By Device... Rename Rule Clone Rule Delete Rule

Click here to add a description.

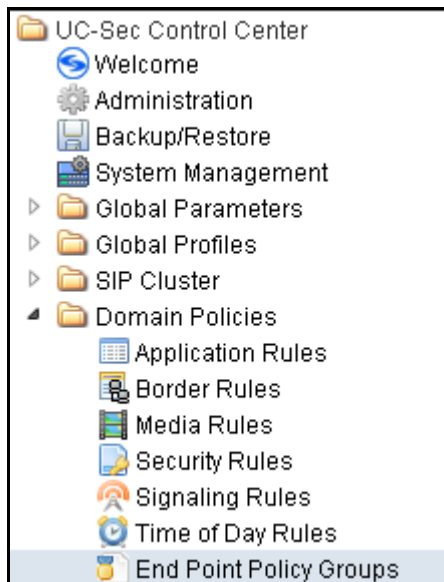
General Requests Responses Request Headers Response Headers Signaling QoS

Signaling QoS	QoS Type	DSCP
<input checked="" type="checkbox"/>	DSCP	EF

Edit

7.4.4. Domain Policies – End Point Policy Groups

Select **Domain Policies** → **End Point Policy Groups** from the left-side menu as shown below:



Select the **Add Group** button.

Enter a name in the **Group Name** field, such as “SIPPolicies_IP” as shown below. Click **Next**.

In the sample configuration, defaults were selected for all fields, with the exception of the **Application Rule** which was set to “MaxVoiceSession”, **Media Rule** which was set to “New-Low_Med”, and the **Signaling Rule**, which was set to “Avaya” as shown below. The selected non-default media rule and signaling rule chosen were created in previous sections. Click **Finish**.

Once configuration is completed, the “default-low-remark” policy group will appear as follows:

Order	Application	Border	Media	Security	Signaling	Time of Day
1	MaxVoiceSession	default	New-Low-Med	default-low	Avaya	default

7.5. Device Specific Settings

7.5.1. Network Management

The **Network Management** feature allows the public and private interface addresses and state to be set. From the left-hand menu select **Device Specific Settings → Network Management**.

Enter the **IP Address** and **Gateway** for both the Inside and the Outside interfaces.

Select the physical interface used from the drop-down menu in the **Interface** column.

IP Address	Public IP	Gateway	Interface
205.100.02.92		205.100.02.1	B1
205.100.02.35		205.100.02.1	B1
10.64.19.100		10.64.19.1	A1

Select the **Interface Configuration** tab and use the **Toggle State** button to enable the interfaces. See screen below:

Network Configuration		Interface Configuration
Name		Administrative Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

7.5.2. Media Interfaces

The **Media Interfaces** feature allows the IP Address and ports to be set for transporting Media over the SIP trunk. From the left-hand menu select **Device Specific Settings → Media Interface**.

For the inside **Media Interface**:

- Select **Add Media Interface**
- **Name:** **Media_Inside**
- **Media IP:** **10.64.90.109** (Internal Address for calls toward Session Manager)

- **Port Range: 2048-5059**
- Click **Finish**

For the outside **Media Interface**:

- Select **Add Media Interface**
- **Name: Media_Outside_35**
- **Media IP: 205.xx.xx.35** (External Address for calls toward IntelPeer trunk)
- **Port Range: 8000-8999**
- Click **Finish**
- Select **Add Media Interface**

The screen below is a result of the details configured above.

Media Interface				
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management .				
			Add Media Interface	
Name	Media IP	Port Range		
Media_Inside	10.64.19.100	2048 - 5059		
Media_Outside_92	205.1...92	8000 - 8999		
Media_Outside_35	205.1...35	8000 - 8999		

7.5.3. The Signalling Interfaces

The **Signalling Interfaces** feature allows the IP Address and ports to be set for transporting SIP Signaling over the SIP trunk. From the left-hand menu select **Device Specific Settings → Signalling Interface**. The following steps show the signaling interfaces created in the sample configuration, with TLS port 5061 used for both the inside and outside IP interfaces.

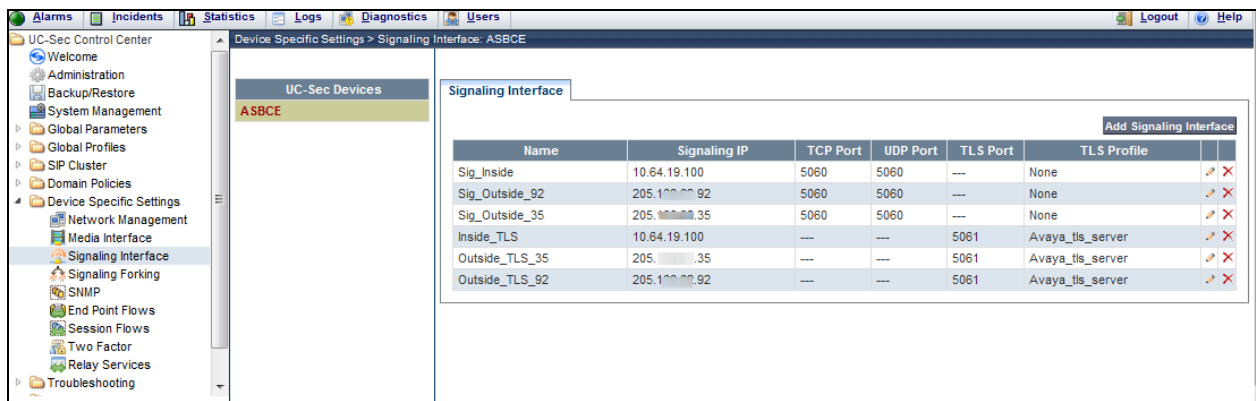
For the inside **Signaling Interface**:

- Select **Add Signaling Interface**
- **Name:** **Inside_TLS**
- **Media IP:** **10.64.19.100** (Internal Address for calls toward Session Manager)
- **TLS Port:** **5061**
- Click **Finish**

For the outside **Signaling Interface**:

- Select **Add Signaling Interface**
- **Name:** **Outside_TLS_35**
- **Media IP:** **205.xx.xx.35** (External Address for calls toward IntelPeer)
- **TLS Port:** **5061**
- Click **Finish**

The screen below is a result of the details configured above.



The screenshot shows the UC-Sec Control Center interface. The left-hand menu is expanded to 'Device Specific Settings' > 'Signaling Interface'. The main area displays a table of configured signaling interfaces. The table has columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. There are two tabs: 'Signaling Interface' (selected) and 'Add Signaling Interface'.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
Sig_Inside	10.64.19.100	5060	5060	---	None
Sig_Outside_92	205.100.00.92	5060	5060	---	None
Sig_Outside_35	205.100.00.35	5060	5060	---	None
Inside_TLS	10.64.19.100	---	---	5061	Avaya_tls_server
Outside_TLS_35	205.100.00.35	---	---	5061	Avaya_tls_server
Outside_TLS_92	205.100.00.92	---	---	5061	Avaya_tls_server

7.5.4. The End Point Flows

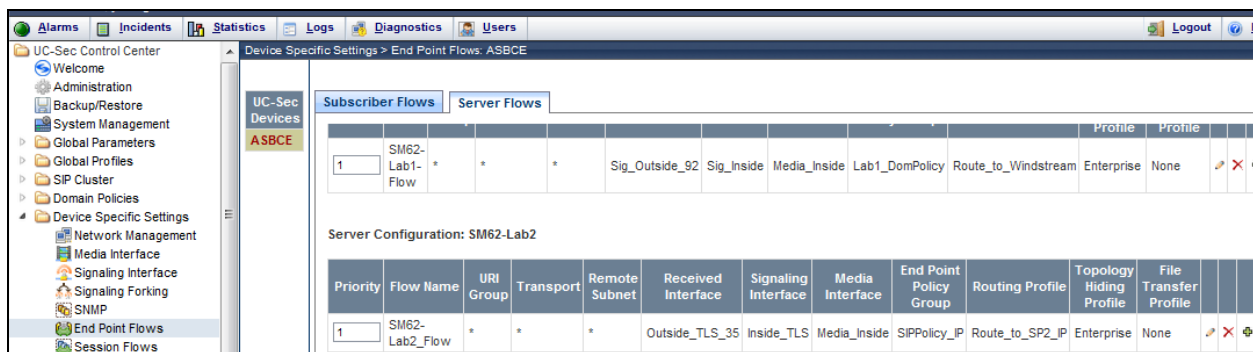
The **End Point Flows** allow the Interfaces, Policies and Profiles administered to be used to transport the SIP traffic. From the left-hand menu select **Device Specific Settings** → **Endpoint Flows**.

- Select the **Server Flows** tab

To add the settings for fixed call flow to Session Manager click on **Add Flow**.

- **Name:** SM62-Lab2_Flow
- **Server Configuration:** SM62-Lab2
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Outside_TLS_35
- **Signaling Interface:** Inside_TLS
- **Media Interface:** Media_Inside
- **End Point Policy Group:** SIPPolicy_IP
- **Routing Profile:** Route_to_SP2_IP
- **Topology Hiding Profile:** Enterprise
- **File Transfer Profile:** None
- Click **Finish**

The second entry in the screen below is a result of the details configured above:

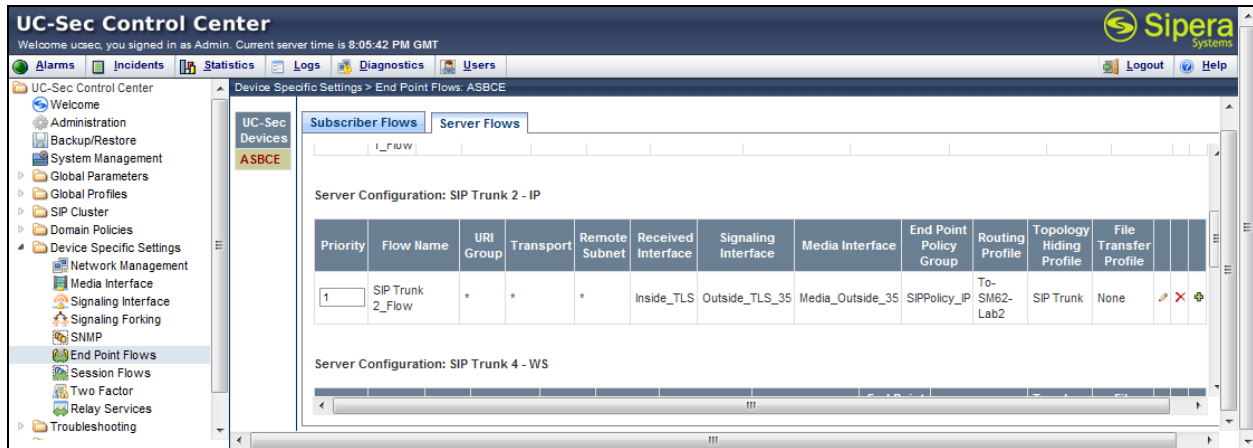


To add the settings for Fixed call flow to IntelPeer, select **Add Flow**.

- **Name:** SIP Trunk 2_Flow
- **Server Configuration:** SIP Trunk 2-IP
- **URI Group:** *
- **Transport:** *
- **Remote Subnet:** *
- **Received Interface:** Inside_TLS
- **Signaling Interface:** Outside_TLS_35

- **Media Interface: Media_Outside_35**
- **End Point Policy Group: SIPPolicy_IP**
- **Routing Profile: To-SM62-Lab2**
- **Topology Hiding Profile: SIP Trunk**
- **File Transfer Profile: None**
- Click **Finish**

The entry in the screen below is a result of the details configured above.



8. IntelPeer Configuration

The configuration required by IntelPeer to allow the tests to be carried out is not covered in this document and any further information required should be obtained through the local IntelPeer representative.

9. Verification and Troubleshooting

9.1. Verification

This section provides steps that may be performed to verify that the solution is configured correctly.

- From System Manager Home tab, click on Session Manager and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are shown as **up**.

This is the SIP Entity link to Communication Manager utilizing TLS port 5061:

All Entity Links to SIP Entity: cm62_tg2

Summary View							
1 Item Refresh							Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	ASM62	10.64.90.103	5061	TLS	Up	200 OK	Up

This is the second SIP Entity link to Communication Manager utilizing a different port for TLS, port 5071:

All Entity Links to SIP Entity: CM62_TG3

Summary View							
1 Item Refresh							Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	ASM62	10.64.90.103	5071	TLS	Up	200 OK	Up

From the Communication Manager SAT interface run the command **status trunk n** where **n** is a previously configured SIP trunk. Observe if all channels on the trunk group display **in service/idle**.

Status trunk 2			TRUNK GROUP STATUS
Member	Port	Service State	Mtce Connected Ports Busy
0002/001	T00011	in-service/idle	no
0002/002	T00012	in-service/idle	no
0002/003	T00013	in-service/idle	no
0002/004	T00014	in-service/idle	no
0002/005	T00015	in-service/idle	no
0002/006	T00016	in-service/idle	no
0002/007	T00017	in-service/idle	no
0002/008	T00018	in-service/idle	no
0002/009	T00019	in-service/idle	no
0002/010	T00020	in-service/idle	no

- Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
- Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
- Verify that the user on the PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. 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.

2. Avaya SBCE:

- **Incidents** - Displays alerts captured by the UC-Sec appliance.

Incident Viewer

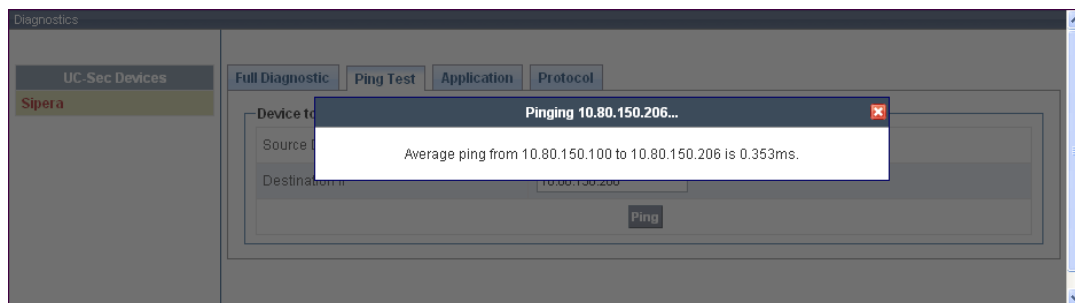
Device: All Category: All Clear Filters Refresh Show Chart Generate Report

Displaying results 1 to 15 out of 102.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
Message Dropped	662168149391824	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168147389246	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168146388212	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145887753	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145636658	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168142392101	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168140391726	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168138390782	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168136390456	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168134389013	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168132388591	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168131388258	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130886109	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130635815	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Server Heartbeat	66216530683634	12/19/11	9:38 PM	Policy	Sipera	Server Heartbeat is UP

<< < 1 2 3 4 5 > >>

- **Diagnostics** - Allows for PING tests and displays application and protocol use.



- **Troubleshooting → Trace Settings** - Configure and display call traces and packet captures for the UC-Sec appliance.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 10:31:55 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
SNMP
End Point Flows
Session Flows
Two Factor
Relay Services
Troubleshooting
Advanced Options
DoS Learning
Syslog Management
Trace Settings
TLS Management
IM Logging

Troubleshooting > Trace Settings: ASBCE

UC-Sec Devices
ASBCE

Packet Trace Call Trace Packet Capture Captures

Packet Capture Configuration

Currently capturing No

Interface A1

Local Address (ip:port) All :

Remote Address (*, *.port, ip, ip:port)

Protocol All

Maximum Number of Packets to Capture 1200

Capture Filename Intelepeer trace
Existing captures with the same name will be overwritten

Start Capture Clear

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 10:33:34 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center
Welcome
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
SIP Cluster
Domain Policies
Device Specific Settings
Network Management
Media Interface
Signaling Interface
Signaling Forking
SNMP
End Point Flows
Session Flows
Two Factor
Relay Services
Troubleshooting
Advanced Options
DoS Learning
Syslog Management
Trace Settings
TLS Management
IM Logging

Troubleshooting > Trace Settings: ASBCE

UC-Sec Devices
ASBCE

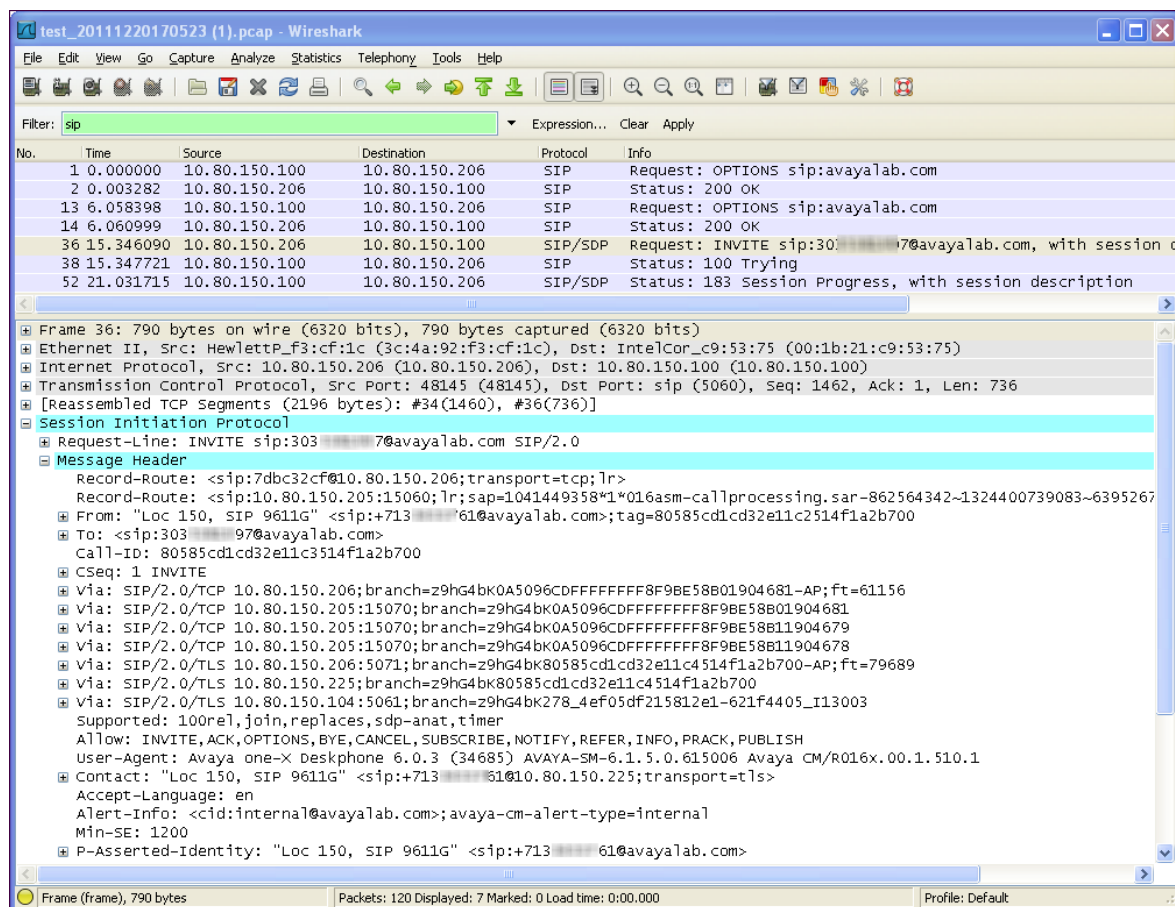
Packet Trace Call Trace Packet Capture Captures

Refresh

File Name	File Size (bytes)	Last Modified
test_20111220170523.pcap	18,178	December 20, 2011 5:05:45 PM GMT
trace.pcap	20,273	March 2, 2012 3:39:06 PM GMT

About
Admin Guide
Reset Password

The packet capture file can be downloaded and viewed using a Network Protocol Analyzer such as Wireshark for TCP/UDP protocols only.



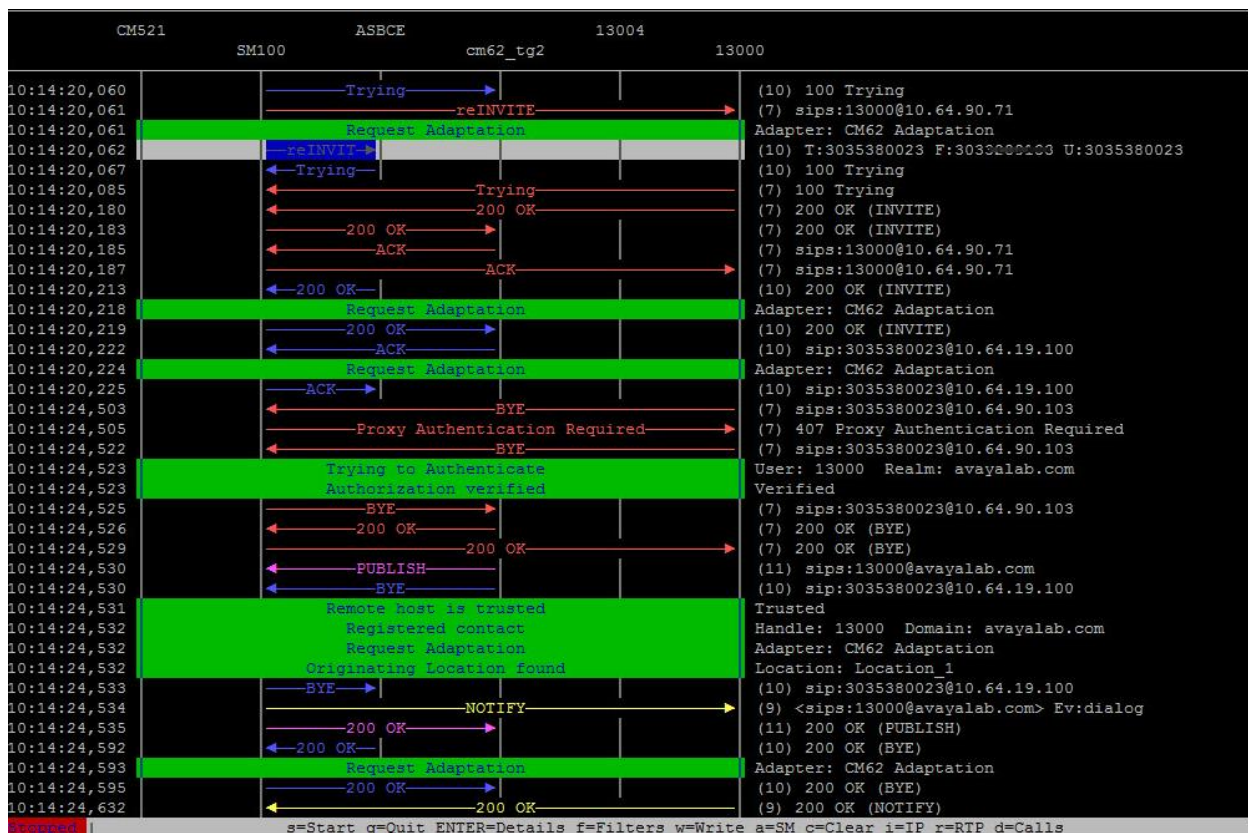
For the TLS protocol use Session Manager's traceSM utility to capture encrypted traces.

3. Session Manager: Encrypted Traces

Login to Session Manager using PuTTY SSH Client and become the Root user. Enter the command: **tracesm -x -uni**

- Capture the un-crypted packets
- Print the trace as txt file.

The screens below show the copy of captured trace and the sample of txt file.



Txt File

2012-06-12 13:10:26,412 CallLogs INFO - : Incoming Message
 Transport: TCP : ip=10.64.90.109, port=43248,

INVITE sip:18002422121@avayalab.com SIP/2.0
 Route: <sip:10.64.90.108:15061;transport=TLS;lr;phase=terminating>
 From: "12004 Softphone"
 <sip:+3033289132@avayalab.com>;tag=0be321890bfe1145484ff0883300
 To: <sip:18002422121@avayalab.com>
 Call-ID: 0be321890bfe1146484ff0883300
 CSeq: 1 INVITE
 Max-Forwards: 70
 P-Av-Transport: AP;fe=10.64.90.103:10020;ne=10.64.90.109:5071;tt=TLS;th
 Via: SIP/2.0/TLS 10.64.90.109:5071;branch=z9hG4bK0be321890bfe1147484ff0883300-
 AP;ft=855
 Via: SIP/2.0/TLS 10.64.90.103:5071;branch=z9hG4bK0be321890bfe1147484ff0883300
 Via: SIP/2.0/TCP 10.64.90.74;branch=z9hG4bK0be321890bfe1147484ff0883300
 Supported: 100rel,histinfo,join,replaces,sdp-anat,timer
 Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,INFO,PRACK,PUBLISH,UPDATE
 User-Agent: Avaya CM/R016x.02.0.823.0
 Contact: "12004 Softphone" <sip:+3035559132@10.64.90.103:5071;transport=tls>
 Accept-Language: en
 Alert-Info: <cid:internal@avayalab.com>;avaya-cm-alert-type=internal
 History-Info: <sip:18002422121@avayalab.com>;index=1
 History-Info: "18002422121" <sip:18002422121@avayalab.com>;index=1.1
 Min-SE: 1200
 P-Asserted-Identity: "12004 Softphone" <sip:+3033289132@avayalab.com>
 Record-Route: <sip:7762aaaf@10.64.90.109:5071;transport=tls;lr>
 Record-Route: sip:10.64.90.103:5071;transport=tls;lr

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and the Avaya Session Border Controller Advanced for Enterprise to IntelPeer SIP Trunk Service. The testing was successfully performed with IntelPeer, refer to **Section 2.2** for more details.

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform, Release 6.03*, February 2011.
- [2] *Administering Avaya Aura® System Platform, Release 6.03*, February 2011.
- [3] *Administering Avaya Aura® Communication Manager 6.2*, February 2012, Document Number 03-300509, Issue 7.0.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation 6.2*, February 2012, Document Number 555-245-205, Issue 9.0.
- [5] *Administering Avaya Aura® System Manager*, Release 6.2, May 2012.
- [6] *Implementing Avaya Aura® Session Manager 6.2*, February 2012, Document Number 03-603473
- [7] *Administering Avaya Aura® Session Manager 6.2*, February 2012, Document Number 03-603324.
- [8] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [9] *UC-Sec Administration Guide (010-5423-400v106)*
- [10] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2012 Avaya Inc. All Rights Reserved.

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

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