

Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring IntelePeer<sup>™</sup> SIP Trunk Service with Avaya Aura® Communication Manager Evolution Server 6.0.1 and Avaya Session Border Controller for Enterprise 4.0.5 – Issue 1.0

# Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the IntelePeer<sup>™</sup> SIP Trunk Service and an Avaya SIP-enabled enterprise solution. IntelePeer<sup>™</sup> can offer the SIP Trunk Service using several different platform technologies in the IntelePeer<sup>™</sup> network. These Application Notes correspond to the SIP Trunk Service offered using a Sonus GSX9000 SBC in the network. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager Evolution Server, and various Avaya endpoints.

IntelePeer<sup>™</sup> is a member of the Avaya DevConnect 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.

#### **Table of Contents**

1.	Introduction	4
2.	General Test Approach and Test Results	4
2.1	Interoperability Compliance Testing	4
2.2.	Test Results	5
2.3.	Support	5
3.	Reference Configuration	5
4.	Equipment and Software Validated	7
5.	Configure Avaya Aura® Communication Manager	
5.1.	Licensing and Capacity	
5.2.	System Features	9
5.3.	IP Node Names	
5.4.	Codecs	
5.5.	IP Interface for procr	
5.6.	IP Network Region	
5.7.	Signaling Group	
5.8.	Trunk Group	14
5.9.	Inbound Routing	
5.10.	Calling Party Information	
5.11.	Outbound Routing	
5.12.	Saving Communication Manager Configuration Changes	
6.	Configure Avaya Session Border Controller for Enterprise	
6.1.	Global Profiles	
6.1.1.	Routing Profile	
6.1.2.	Topology Hiding Profile	
6.1.3.	Server Interworking Profile	
6.1.4.	Signaling Manipulation	
6.1.5.	Server Configuration	
6.2.	Domain Policies	
6.2.1.	Media Rules	
6.2.2.	Signaling Rules	
6.2.3.	Application Rules	
6.2.4.	Endpoint Policy Group	
6.3.	Device Specific Settings	53
	Network Management	
6.3.2.	Signaling Interface	55
6.3.3.	Media Interface	
	End Point Flows - Server Flow	
7.	SIP Trunk Service Configuration	59
8.	Verification and Troubleshooting	
8.1.	Verification	
8.2.	Troubleshooting	61

PM; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 65
SPOC 5/25/2012	©2012 Avaya Inc. All Rights Reserved.	IPeerCM601ASBCE

9.	Conclusion	63
10.	References	64

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between the IntelePeer<sup>™</sup> SIP Trunk Service and an Avaya SIP-enabled enterprise solution. IntelePeer<sup>™</sup> can offer the SIP Trunk Service using several different platform technologies in the IntelePeer<sup>™</sup> network. These Application Notes correspond to the SIP Trunk Service offered using a Sonus GSX9000 SBC in the network. The Avaya solution consists of Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager Evolution Server and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with the IntelePeer<sup>TM</sup> SIP Trunk Service are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

# 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager and the Avaya Session Border Controller for Enterprise to connect to the public Internet using a broadband connection. The enterprise site was configured to connect to the SIP Trunk Service. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising standards-based interfaces pertinent to the interoperability of the tested products and their functionality. 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.

The SIP Trunk Service passed compliance testing.

### 2.1. Interoperability Compliance Testing

To verify SIP trunking interoperability, the following features and functionality were covered during the interoperability compliance test:

- Incoming PSTN calls to various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. Phone types included H.323, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (soft client).

PM; Reviewed:	Solution & Interoperability Test Lab Application Notes	4 of 65
SPOC 5/25/2012	©2012 Avaya Inc. All Rights Reserved.	IPeerCM601ASBCE

- Avaya one-X® Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. The H.323 protocol was the only protocol tested.
- Various call types including: local, long distance, international, outbound toll-free.
- Codec G.711MU
- DTMF transmission using RFC 2833.
- G.711 Faxing.
- Caller ID presentation and Caller ID restriction.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, and conference.
- Off-net call forwarding and mobility (extension to cellular).

Items not supported or 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 SIP Trunk Service was completed with successful results for all test cases.

# 2.3. Support

For technical support with the SIP Trunk Service, contact IntelePeer<sup>TM</sup> using the Customer Care links at <u>www.IntelePeer<sup>TM</sup>.com</u>

# 3. Reference Configuration

**Figure 1** illustrates a sample Avaya SIP-enabled enterprise solution connected to the SIP Trunk Service. This is the configuration used for compliance testing.

The Avaya components used to create the simulated customer site included:

- Communication Manager
- Communication Manager Messaging
- Avaya Session Border Controller for Enterprise
- Avaya G450 Media Gateway
- Avaya 9600-Series IP telephones (H.323)
- Avaya one-X® Communicator (H.323)
- Avaya digital and analog telephones

Located at the edge of the enterprise is the Avaya Session Border Controller for Enterprise (Avaya SBCE). It has a public side that connects to the external network and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through the Avaya SBCE. In this way, the Avaya SBCE can protect the enterprise against any SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. For security reasons, any actual public IP addresses used in the configuration have been replaced with private IP addresses. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

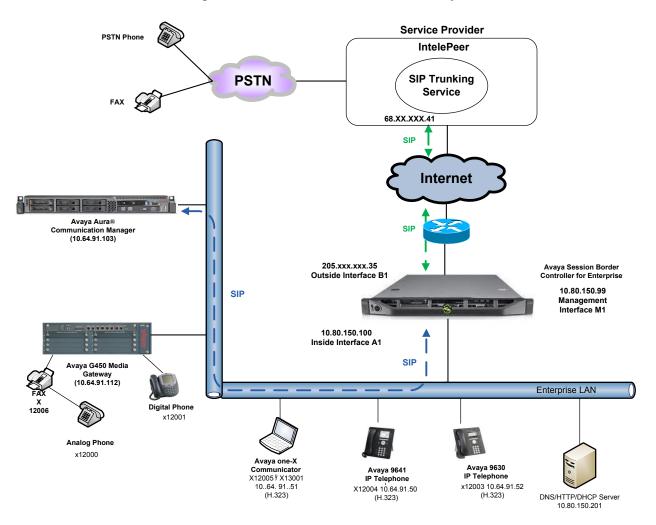


Figure 1: Avaya IP Telephony Network using the SIP Trunk Service

For inbound calls, the calls flow from the service provider to the Avaya SBCE and then to Communication Manager. Once the call arrives at Communication Manager, 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

PM; Reviewed:	Solution & Interoperability Test Lab Application Notes	6 of 65
SPOC 5/25/2012	©2012 Avaya Inc. All Rights Reserved.	IPeerCM601ASBCE

restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Avaya SBCE. From Avaya SBCE, the call is sent to the SIP Trunk Service.

IntelePeer<sup>TM</sup> allows all North American Numbering Plan (NANP) numbers to be dialed with either 10 digits or 11 digits (1 + 10).

# 4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components						
Component	Release					
Avaya Aura® Communication Manager	R016x.00.1.510.1-19350 (SP 6)					
Avaya Aura® Communication Manager	N6.0.1-8.0					
Messaging						
Avaya Session Border Controller for	4.0.5.Q02					
Enterprise						
Avaya G450 Media Gateway	31.20.1					
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.103S					
Avaya 9641 IP Telephone (H.323)	Avaya one-X® Deskphone SIP Edition 6.0.3					
Avaya one-X® Communicator (H.323)	6.1.2.06 SP2					
Avaya 2420 Digital Telephone	n/a					
Avaya 6210 Analog Telephone	n/a					
IntelePeer <sup>TM</sup> SIP Trunking Solution Components						
Component	Release					
Sonus GSX9000 SBC	V07.03.04S003					

#### Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance testing.

**Note**: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager.

# 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the SIP Trunk Service. A SIP trunk is established between Communication Manager and the Avaya SBCE for use by signaling traffic to and from IntelePeer<sup>TM</sup>. It is assumed the general installation of Communication Manager and the Avaya G450 Media Gateway 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:** IP addresses and phone numbers shown throughout these Application Notes have been edited so that the actual IP addresses of the network elements and public PSTN numbers are not revealed.

# 5.1. 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 below shows that **12000** licenses are available and **280** 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	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:					
Maximum Administered SIP Trunks:	12000	280			
Maximum Administered Ad-hoc Video Conferencing Ports:	12000	0			
Maximum Number of DS1 Boards with Echo Cancellation:	522	0			
Maximum TN2501 VAL Boards:	10	0			
Maximum Media Gateway VAL Sources:	250	1			
Maximum TN2602 Boards with 80 VoIP Channels:	128	0			
Maximum TN2602 Boards with 320 VoIP Channels:	128	0			
Maximum Number of Expanded Meet-me Conference Ports:	300	0			
(NOTE: You must logoff & login to effect the per	missio	on change	s.)		

Solution & Interoperability Test Lab Application Notes 8 of 65 ©2012 Avaya Inc. All Rights Reserved. IPeerCM601ASBCE

# 5.2. 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 featuresPage1 of19FEATURE-RELATED SYSTEM PARAMETERSSelf Station Display Enabled? yTrunk-to-Trunk Transfer: allAutomatic Callback with Called Party Queuing? nAutomatic Callback - No Answer Timeout Interval (rings): 3Call Park Timeout Interval (minutes): 10Off-Premises Tone Detect Timeout Interval (seconds): 20AAR/ARS Dial Tone Required? y
```

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 types of calls.

```
9 of 19
                                                                   Page
change system-parameters features
                        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
INTERNATIONAL CALL ROUTING PARAMETERS
               Local Country Code: 1
         International Access Code: 011
ENBLOC DIALING PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n
CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

# 5.3. IP Node Names

Use the **change node-names ip** command to verify the node name defined for the IP address of Communication Manager (**procr**) created during installation. Add a node name and IP address for the Avaya SBCE's internal interface (e.g., **ASBCE**). These node names will be needed for defining the service provider signaling group in Section 5.7.

change node-names	ip	Page	1 of	2
	IP NODE NAMES			
Name	IP Address			
ASBCE	10.80.150.100			
Messaging	10.64.91.103			
SM	10.64.91.109			
acme	10.64.91.115			
default	0.0.0			
procr	10.64.91.103			

### 5.4. 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, **ip-codec-set 2** was used for this purpose. The SIP Trunk Service supports G.729A, and G.711MU. During compliance testing only G.711MU was tested. The true order of preference is defined by the end customer. In the example below, **G.711MU** and **G.729A** was entered in the **Audio Codec** column of the table. Default values can be used for all other fields.

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

Set the Fax Mode to t.38-standard on Page 2.

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

### 5.5. 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 sample configuration. While the focus here is the use of the Processor Ethernet (Procr) for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

```
change ip-interface proc
                                                                                    2
                                                                     Page
                                                                             1 of
                                   IP INTERFACES
                  Type: PROCR
                                                        Target socket load: 1700
                                                     Allow H.323 Endpoints? y
      Enable Interface? y
                                                      Allow H.248 Gateways? y
        Network Region: 1
                                                       Gatekeeper Priority: 5
                                 IPV4 PARAMETERS
                                                   IP Address: 10.64.91.103
             Node Name: procr
           Subnet Mask: /24
```

### 5.6. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, **IP-network-region 2** was chosen for the service provider trunk. **IP network region 1** is the default IP network region and encompasses all the elements within the enterprise. Use the **change ip-network-region 2** command to configure IP network region 2 with the following parameters:

• Set the Location field to match the enterprise location for this SIP trunk.

PM; Reviewed:	Solution & Interoperability Test Lab Application Notes	11 of 65
SPOC 5/25/2012	©2012 Avaya Inc. All Rights Reserved.	IPeerCM601ASBCE

- 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.
- 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. To enable shuffling, set both **Intra-region** and **Inter-region IP-IP Direct Audio** fields to **yes.** This is the default setting. Shuffling can be further restricted at the trunk level on the Signaling Group form.
- Set the Codec Set field to the IP codec set defined in Section 5.4.
- Default values can be used for all other fields.

```
Page
change ip-network-region 2
                                                                        1 of 20
                              IP NETWORK REGION
 Region: 2
   ation: 1
Name: SIP Trunks
Location: 1
                        Authoritative Domain: avayalab.com
MEDIA PARAMETERS
                                 Intra-region IP-IP Direct Audio: yes
    Codec Set: 2
                               Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 5000
                                         IP Audio Hairpinning? n
  UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
       Audio PHB Value: 46
       Video PHB Value: 26
802.1P/O 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
```

**On Page 4**, define the IP codec set to be used for traffic between region 2 and the rest of the enterprise (Region 1). Enter the desired IP codec set in the **codec set** column of the row with destination region (**dst rgn**) 1. Default values may be used for all other fields. The example below shows the settings used for the compliance test. It indicates that codec set 2 will be used for calls between region 2 (the service provider region) and region 1 (the rest of the enterprise).

```
Page 4 of 20
change ip-network-region 2
                                                    I
Source Region: 2 Inter Network Region Connection Management
                                                          М
                                                    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
                                                           е
1
    2 y NoLimit
                                                    n
                                                          t.
2
    2
3
4
```

PM; Reviewed: SPOC 5/25/2012

Solution & Interoperability Test Lab Application Notes 12 of 65 ©2012 Avaya Inc. All Rights Reserved. IPeerCM6

### 5.7. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the Avaya SBCE for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, **Signaling Group 2** was used for this purpose and was configured using the parameters highlighted below.

- Set the Group Type field to sip.
- Set the **IMS Enabled** field to **n**. This specifies Communication Manager will serve as an Evolution Server.
- Set the **Transport Method** to **tcp** (Transmission Control Protocol). Set the **Near-end** Listen Port and Far-end Listen Port to 5060.
- Set the **Peer Detection Enabled** field to **n**.
- Set the **Peer Server** to **Others**.
- Set the Near-end Node Name to procr. This node name maps to the IP address of Communication Manager as defined in Section 5.3.
- Set the **Far-end Node Name** to **ASBCE**. This node name maps to the IP address of the Avaya SBCE's internal interface as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**.
- Set the Far-end Domain to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to y. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Default values may be used for all other fields.

```
add signaling-group 2
                                                                        Page 1 of
                                                                                       1
                                  SIGNALING GROUP
 Group Number: 1 Group Type: sip
IMS Enabled? n Transport Method: tcp
        O-SIP? n
                                                                 SIP Enabled LSP? n
     IP Video? n
                                                       Enforce SIPS URI for SRTP? v
  Peer Detection Enabled? n Peer Server: Others
   Near-end Node Name: procr
                                                Far-end Node Name: ASBCE
 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

DTMF over IP: rtp-payload

Session Establishment Timer(min): 3
                                                         RFC 3389 Comfort Noise? n
                                               Direct IP-IP Audio Connections? y
                                                          IP Audio Hairpinning? n
        Enable Layer 3 Test? y
                                                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n
                                                     Alternate Route Timer(sec): 6
```

Solution & Interoperability Test Lab Application Notes 13 of 65 ©2012 Avaya Inc. All Rights Reserved. IPeerCM6

# 5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.7**. For the compliance test, **Trunk Group 2** 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 **Direction** to **two-way**.
- 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.

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 <b>TAC: *02</b>
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night	Service:
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member As	signment Method: auto
		Signaling Group: 2
	Nu	mber of Members: 10

On **Page 2**, 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 **600** seconds was used.

```
add trunk-group 2

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
```

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 5.2**, 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

TRUNK FEATURES

ACA Assignment? n Measured: none

Maintenance Tests? y

Numbering Format: public

UUI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. On **Page 4**, set the **Network Call Redirection** field to **y** if using the SIP REFER method. This allows inbound calls transferred back to the PSTN to use the SIP REFER method, see **Reference [15]**. Set the **Send Diversion Header** field to **y** as well. This field provides additional information to the network if the call has been re-directed. This is necessary 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 **n**. Set the **Telephone Event Payload Type** to **101**, the value preferred by IntelePeer<sup>TM</sup>.

**Note:** IntelePeer<sup>TM</sup>'s SIP Trunking Feature **does not require** the use of the Diversion header on re-directed calls. When using IntelePeer<sup>TM</sup>'s SIP Trunking Feature, set the **Send Diversion Header** and **Network Call Redirection** field to **n** but the **Support Request History** field to **y**.

add trunk-group 2 PROTOCOL VARIATIONS Mark Users as Phone? n
Prepend '+' to Calling Number? n
Send Transferring Party Information? n
Network Call Redirection? n
Send Diversion Header? n
Support Request History? y
Telephone Event Payload Type: 101 Convert 180 to 183 for Early Media? y
Always Use re-INVITE for Display Updates? y
Identity for Calling Party Display: P-Asserted-Identity

# 5.9. Inbound Routing

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. The DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. Use the **change inc-call-handling-trmt trunk-group 2** command to create an entry for each DID. As an example, the following screen illustrates the conversion of DID number **3033289130** to extension **12001** and so forth.

change inc-ca INCO		<b>ng-trmt tr</b> HANDLING	-	-		Page	1 of	30
Service/	Number	Number	Del	Insert				
Feature	Len	Digits						
public-ntwrk	10 303	3289130	10	12001				
public-ntwrk	10 303	3289131	10	12002				
public-ntwrk	10 303	3289132	10	12003				
public-ntwrk	10 303	3289133	10	12004				
public-ntwrk	10 303	3289134	10	12005				
-								

PM; Reviewed: SPOC 5/25/2012

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

# 5.10. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since public numbering was selected to define the format of this number (Section 5.8), use the change **public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID number will be one assigned by the SIP service provider. It is also used to authenticate the caller.

In the sample configuration, five DID numbers were assigned for testing. These five numbers were assigned to the five extensions **12001**, **12002**, **12003**, **12004** and **12005**. Thus, these same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these five extensions at the Enterprise.

char	change public-unknown-numbering 1 Page 1 of 2							
		NUMBE	RING - PUBLIC/UN	IKNOWN	FORMAT			
				Total				
Ext	Ext	Trk	CPN	CPN				
Len	Code	Grp(s)	Prefix	Len				
					Total Administered: 13			
			5	5	Maximum Entries: 9999			
5	5			5				
5	3			5	Note: If an entry applies to			
5	4			5	a SIP connection to Avaya			
5	5			5	Aura(tm) Session Manager,			
5	6			5	the resulting number must			
5	7			5	be a complete E.164 number.			
5	8			5				
5	12000	2	3033289130	10				
5	12001	2	3032899131	10				
5	12003	2	3033289132	10				
5	12004	2	3033289133	10				
5	12005	2	3033289134	10				

# 5.11. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. 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. Use the **change dialplan analysis** command to define a dialed string beginning with **9** of length **1** as a feature access code (**fac**).

Solution & Interoperability Test Lab Application Notes 17 ©2012 Avaya Inc. All Rights Reserved. IPed

change dial	plan analysis		Page 1 of 12
		DIAL PLAN ANALYSIS TABLE	
		Location: all	Percent Full: 2
Dialed String 0 1 2 3 4 5 6 7 8 <b>9</b>	Total Call Length Type 1 attd 5 ext 5 ext 5 ext 5 ext 5 ext 5 ext 5 ext 5 ext 5 ext 5 ext 1 fac	Dialed Total Call Diale String Length Type Strin	ed Total Call
*	3 dac		
#	3 dac		

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 CO	DDE	(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		
Call Forwarding Enhanced Status: Act:		Deactivation:			
Call Park Access Code:	*40				
Call Pickup Access Code:	*41				
CAS Remote Hold/Answer Hold-Unhold Access Code:	*42				
CDR Account Code Access Code:					
Change COR Access Code:					
Change Coverage Access Code:					
Conditional Call Extend Activation:		Deactivation:			
Contact Closure Open Code:	*80	Close Code:	#80		
-					

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9.

- **Dialed String:** enter the leading digits (e.g., **1303**) necessary to uniquely select the desired route pattern.
- **Total Min:** enter the minimum number of digits (e.g., **11**) expected for this PSTN number.
- **Total Max:** enter the maximum number of digits (e.g., 11) expected for this PSTN number.
- **Route Pattern:** enter the route pattern number (e.g., 1) to be used. The route pattern (to be defined next) will specify the trunk group(s) to be used for calls matching the dialed number.
- **Call Type:** enter **fnpa**, the call type for North American 1+10 digit calls. For local 7 or 10 digit calls enter **hnpa**. For 411 and 911 calls use **svcl** and **emer** respectively. The call type tells Communication Manager what kind of call is made to help decide how to handle the dialed string and whether or not to include a preceding 1. For more information and a complete list of Communication Manager call types, see **Reference [3]** and **[4].**

The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 1 which contains the SIP trunk to the service provider (as defined next).

change ars analysis 1						Page	1 of	2
	P	ARS DI	GIT ANALY	SIS TABI	LΕ			
			Location:	all		Percent Full:	0	
Dialed	Tot		Route	Call	Node	ANI		
String	Min	Max	Pattern	Туре	Num	Reqd		
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		
2	10	10	1	hnpa		n		
3	10	10	1	hnpa		n		
4	10	10	1	- hnpa		n		
411	3	3	1	svcl		n		
5	10	10	1	hnpa		n		
555	7	7	deny	hnpa		n		
6	10	10	1	hnpa		n		
				•				

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 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 SIP service provider. For the compliance test, trunk group 2 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**: The prefix mark (**Pfx Mrk**) of **1** will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.

chai	nge	e ro	oute	e-p	at	tern	1										Page		1	of	3
							Patte	rn		er: 1 AN? n		<b>Pattern</b> Secure	Name: SIP?	-	TRK						
Grj	p E No		NPZ			-	Toll List		l Di	2							DCS/ QSIG		С		
									Dgts	5							In	tw			
1:	2		0		1												n		us	ser	
2:																	n		us	ser	
3:																	n		us	ser	
4:																	n		us	ser	
5:																	n		us	ser	
6:																	n		us	ser	
	E	SCC	VAI	LUE	3	TSC	CA-TS	C	ITC	C BCI	ES	Service/F	eature	PAI	RM 1	Jo.	Numberin	g I	LAF	R	
	0	1 2	2 M	4	W		Reque	st							Do	gts	Format				
															Suba	dr	ess				
1:	У	У	УΥ	У	n	n			res	st								1	nor	ne	
2:	У	У	УΥ	У	n	n			res	st								1	nor	ne	
3:	У	У	УΥ	У	n	n			res	st								1	nor	ne	
4:	V	v v	v v	V	n	n			res	st								1	nor	ne	

Use the **change ars digit-conversion** command to manipulate the routing of dialed digits that match the DIDs to prevent these calls from going out the PSTN and using unnecessary SIP trunk resources. The example below shows the DID numbers assigned by IntelePeer<sup>™</sup> being converted to 5 digit extensions.

change ars digit-conv	version	0			Page	1 of	2
	ARS I			SION TABLE on: all	Perc	ent Ful	11: 0
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv 2	ANI Req
3033289130	10	10	10	12001	ext	У	n
3033289131	10	10	10	12002	ext	У	n
3033289132	10	10	10	12003	ext	У	n
3033289133	10	10	10	12004	ext	У	n
3033289134	10	10	10	12005	ext	- y	n
						-	

### 5.12. Saving Communication Manager Configuration Changes

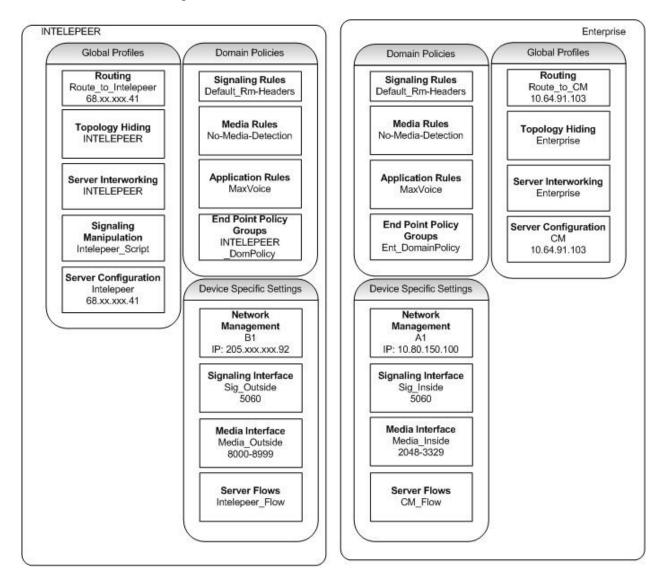
The command save translation all can be used to save the configuration.

save translation all	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

# 6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference [12]** and **[13]**.

A pictorial view of this configuration is shown below. It shows the components needed for the compliance test. Each of these components is defined in the Avaya SBCE web configuration as described in the following sections.



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

Use a web browser to access the Avaya SBCE UC-Sec web interface, enter https://<ipaddr>/ucsec in the address field of the web browser, where <ip-addr> is the management LAN IP address of UC-Sec.

Sipera Systems LARM-VENUY - PROTECT	Sign in Login ID ucsec Password Sign in
The UC-Sec ™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.	
Visit the Sipera Systems website to learn more.	
<b>NOTICE TO USERS:</b> This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.	
	~

Log in with the appropriate credentials. Click **Sign In**.

The main page of the Avaya SBCE UC-Sec Control Center will appear.

UC-Sec Control Ce Welcome ucsec, you signed in as Admin. (				Sipera Sipera	a
🌘 Alarms 🔲 Incidents 👫 Sta	ntistics 📄 Logs 💰 Diagnostics 🎑 L	Jsers		🗾 Logout 🕜 <u>H</u> elp	dp
<ul> <li>UC-Sec Control Center</li> <li>Welcome</li> <li>Administration</li> <li>Backup/Restore</li> <li>System Management</li> <li>Global Parameters</li> <li>Global Profiles</li> <li>SIP Cluster</li> <li>Domain Policies</li> <li>Device Specific Settings</li> <li>Troubleshooting</li> <li>TLS Management</li> <li>IM Logging</li> </ul>	suite of security, enablement and complia communications such as Voice-over-IP (vi collaboration applications. If you need support, please call our toll free <u>support@sipera.com</u> . <u>Alarms (Past 24 Hours)</u> None found. <u>Administ</u>	curity product, the Sipera UC-Sec offers a complete nce features for protecting and deploying unified oIP), instant messaging (IM), multimedia, and	Quicl Sipera Website Sipera VIPER Labs Contact Support UC-Sec Devices ASBCE	CLINKS	

PM; Reviewed: SPOC 5/25/2012 Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

To view system information that was configured during installation, navigate to UC-Sec Control Center  $\rightarrow$  System Management. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named ASBCE is shown. To view the configuration of this device, click the monitor icon (the third icon from the right).

UC-Sec Control Ce Welcome ucsec, you signed in as Admin. C		п			(	5	Sip	era Systems
🕘 Alarms 📋 Incidents 👫 Sta	ntistics 📃 Logs 📑 Diagno	ostics 📓 Users			2	Logo	urt 🧕	) <u>H</u> elp
UC-Sec Control Center Welcome Administration Backup/Restore System Management	System Management							
Global Parameters	Device Name	Serial Number	Version	Status				
<ul> <li>Global Profiles</li> <li>SIP Cluster</li> <li>Domain Policies</li> <li>Device Specific Settings</li> <li>Troubleshooting</li> <li>TLS Management</li> <li>M Logging</li> </ul>	ASBCE	IPCS31020130	4.0.5.Q02	Commissioned	※	•	<b>ب</b> ا	Ø X

The System Information screen shows the Network Settings, DNS Configuration and Management IP information provided during installation, and corresponds to Figure 1. The Box Type was set to SIP and the Deployment Mode was set to Proxy. Default values were used for all other fields.

	System	n Inform	nation: ASBCE			
	Netv	vork Ca	onfiguration			
General Settings			Device Setting	js —		
Appliance Name	ASBCE		HA Mode		NO	
Box Type	SIP		Secure Chan	nel Mode	NONE	
Deployment Mode	Proxy		Two Bypass	Mode	NO	
Network Settings						
IP	Public IP		Netmask	Ga	teway	Interface
10.80.150.100	10.80.150.100	2	55.255.255.0	10.8	0.150.1	A1
20592	20592	25	5.255.255.128	205.		B1
DNS Configuration —			Management	IP(s)		
Primary DNS	10.80.150.201		IP		10.80.150	).99
Secondary DNS						
DNS Location	DMZ					
DNS Client IP	10.80.150.100					

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

# 6.1. Global Profiles

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

#### 6.1.1. Routing Profile

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

Create the Routing Profile for Communication Manager and IntelePeer<sup>TM</sup> SIP Trunk. To add a routing profile, navigate to UC-Sec Control Center  $\rightarrow$  Global Profiles  $\rightarrow$  Routing and select Add Profile. Enter a Profile Name and click Next to continue.

UC-Sec Control Co Welcome ucsec, you signed in as Admin	. Cu	irrent server time is 5:33:08 PM	_								6	Sip	era Systems
	tat	istics 📄 Logs 🚮 Dia			Users						<u>9</u> ]	_ogout 🕜	) <u>H</u> elp
UC-Sec Control Center	1	Global Profiles > Routing: Route	_to_	CM-Lab2									
S Welcome		Add Profile							Ren		Clone Pro	ofile Delete	Profile
Administration		Dauting Destites					Clink hore f	n ndd n	de e e nin ti			_	
Backup/Restore		Routing Profiles					Click here t	o auu a	aescripu	on.			
System Management		default	R	outing Profi	ile								
Global Parameters		Route_to_											
<ul> <li>Global Profiles</li> </ul>		Route_to_SM-Lab1	2								A	dd Routing R	lule
Domain DoS		Route_to_CS1K		_								_	
Singerprint		Route to CM-Lab2											
Server Interworking													
🌑 Phone Interworking		Route_to_SP2											
Routing		Route_to_SP3		1 *	*			Routi	ng Profile				
Server Configuration		Route_to_CM-Lab1											
Subscriber Profiles		To-SM62-Lab2			Profile	Name		R	loute_to_C	M-Lab2			
		Route to SP4											_
Signaling Manipulation	-								Next				
RI Groups		To Shared-Group											
SIP Cluster													
Domain Policies	_												
~													

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

In the new window that appears, enter the following values. Use default values for all remaining fields:

URI Group: Select "\*" from the drop down box.
 Next Hop Server 1: Enter the Domain Name or IP address of the Primary Next Hop server.
 Next Hop Server 2: (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
 Routing Priority Based on Next Hop Server: Checked.
 Outgoing Transport: Checked.

Click Finish (not shown).

The following screen shows the Routing Profile to Communication Manager. The Next Hop Server 1 is the IP address of the Communication Manager Processor Ethernet as defined in Section 5.3. The Outgoing Transport is set to TCP and matches the Transport Method set in the Communication Manager Signaling Group in Section 5.7.

UC-Sec Control Center Welcome Administration Backup/Restore System Management	Global Profiles > Routing: Route_to Add Profile	
System Management	Routing Profiles	Click here to add a description.
	default	Routing Profile
Global Parameters	Route_to_SP1	
Global Profiles	Route_to_SM-Lab1	Add Routing Ru
Eingerprint	Route_to_CS1K	Next Ignore Outering
Server Interworking	Route_to_CM-Lab2	Driority UDL Group Next Hop Next Hop Hop NADTE SPV Hop in Pouto Outgoing
Phone Interworking	Route_to_SP2	Priority Ork Group Server 1 Server 2 Priority Dialog Header Transport
Media Forking	Route_to_SP3	1 * 10.64.91.103 🔽 🗖 🗖 TCP
Routing	Route_to_CM-Lab1	
Subscriber Profiles	To-SM62-Lab2	
Topology Hiding	To-SIP Trunk 3-WS	
Signaling Manipulation		
A URI Groups		
SIP Cluster		
Domain Policies		
Device Specific Settings		
TLS Management		

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. The following screen shows the Routing Profile to IntelePeer<sup>™</sup>. In the Next Hop Server 1 field enter the IP address that IntelePeer<sup>™</sup> uses to listen for SIP traffic and set the **Outgoing Transport** to **UDP**.

UC-Sec Control C Welcome ucsec, you signed in as Admi									8	Sip	Syster					
🕘 <u>A</u> larms 📃 Incidents 📭	<u>S</u> tat	istics 📄 <u>L</u> ogs	📑 Diagno	stics 👔	<u>U</u> s	ers								<b>2</b>	ogout 🥳	<u>H</u> el
DC-Sec Control Center	*	Global Profiles > Rout	ing: Route_to_	SP2												
S Welcome			Add Profile								Ren	ame l	Profile	Clone Pro	file Delete	Profi
Administration Backup/Restore		Routing Pro	files					Clic	k here to add	a descrip	tion.					
System Management		default			_											
Global Parameters		Route_to_SP1		Routin	g Proi	file										
Global Profiles     Domain DoS		Route to SM-Lat	1											A	dd Routing I	Rule
		Route_to_CS1K		_				_								
🎒 Fingerprint 😼 😼	Ξ	Route_to_CM-Lat	12	Prie	ritu	URI Group	Next Hop		Next Hop	Next Hop	NAPTR	CDV	Next Hop in	Ignore Route	Outgoing	
Phone Interworking		Route_to_SP2		PIR		OKIGIOUP	Server 1		Server 2	Priority	NAPIK	SRV	Dialog	Header	Transport	t
🐴 Media Forking		Route_to_SP3		1		*	6841								UDP	ø
Routing		Route_to_CM-Lat	01													
Server Configuration Subscriber Profiles		To-SM62-Lab2														
I Topology Hiding		To-SIP Trunk 3-W	IS													
Signaling Manipulation	_															
🝰 URI Groups																
SIP Cluster																
Domain Policies	Ŧ															

### 6.1.2. Topology Hiding Profile

The Topology Hiding profile manages how various source and destination addresses, 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.

Create a Topology Hiding Profile for the enterprise and IntelePeer<sup>TM</sup> SIP Trunk. In the sample configuration, the **Enterprise** and **IntelePeer<sup>TM</sup>** profiles were cloned from the default profile. To clone a default profile, navigate to **UC-Sec Control Center**  $\rightarrow$  **Global Profiles**  $\rightarrow$  **Topology Hiding**. Select the **default** profile and click on **Clone Profile** as shown below.

Velcome ucsec, you signed in as Admin. Cu Alarms 🔲 Incidents 👫 Stati					🗾 Logout 🔞 I
	Global Profiles > Topology Hiding: de	- 1000 -			Zi Eogour 😈
S Welcome	Add Profile	Iauli			Clone Profile
Backup/Restore	Topology Hiding Profiles	It is not recommend	ed to edit the defaults. Try cloni	ng or adding a new profile instea	d.
📓 System Management 🛛 🗕 🛁	default	Topology Hiding			
🛅 Global Profiles		Header	Criteria	Replace Action	Overwrite Value
🛗 Domain DoS 🎒 Fingerprint		Record-Route	IP/Domain	Auto	
Server Interworking	PARTEC	То	IP/Domain	Auto	
🚯 Phone Interworking		Request-Line	IP/Domain	Auto	
🟫 Media Forking		From	IP/Domain	Auto	
🚰 Routing		Via	IP/Domain	Auto	
Subscriber Profiles		SDP	IP/Domain	Auto	
Topology Hiding				Edit	

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

Enter a descriptive name for the new profile and click Finish.

	Clone Profile	×
Profile Name	default	
Clone Name	Enterprise	
	Finish	

Edit the **Enterprise** profile to overwrite the **To**, **Request-Line** and **From** headers with the enterprise domain as shown below. The **Overwrite Value** should match the Far-end Domain set in the Communication Manager Signaling Group (**Section 5.7**). Click **Finish** to save the changes.

Edit Topology Hiding Profile						
Header		Criteria		Replace Action	Overwrite Value	
Record-Route		P/Domain	*	Auto 💌		×
То		P/Domain	*	Overwrite 💌	avayalab.com	×
Request-Line		P/Domain	*	Overwrite 💌	avayalab.com	×
From		P/Domain	*	Overwrite 💌	avayalab.com	<b>X</b>
Via		P/Domain	*	Auto 💌		×
SDP		P/Domain	*	Auto		×
				Finish		

It is not necessary to modify the **IntelePeer<sup>TM</sup>** profile from the default values. The following screen shows the Topology Hiding Policy created for IntelePeer<sup>TM</sup>.

	Statistics 📃 Logs 🛃 Diagno	LACON			Jegout 🕢		
UC-Sec Control Center S Welcome	Global Profiles > Topology Hiding: S Add Profile	P2-Topology			ofile Clone Profile Delete Pr		
Backup/Restore	Topology Hiding Profiles		Click here	e to add a description.			
System Management	default cisco_th_profile	Topology Hiding					
Global Profiles	SIP Trunk	Header	Criteria	Replace Action	Overwrite Value		
Fingerprint	Enterprise	Request-Line	IP/Domain	Auto	1 <del>,</del> 5		
Server Interworking	SP2-Topology	From	IP/Domain	Auto			
None Interworking		SDP	IP/Domain	Auto			
Media Forking		Record-Route	IP/Domain	Auto			
Routing		Via	IP/Domain	Auto	1 <del></del>		
Server Conliguration		То	IP/Domain	Auto			
Topology Hiding				Edit			
Signaling Manipulation & URI Groups				Cont			
SIP Cluster							
Domain Policies							
🛅 Device Specific Settings 🛅 Troubleshooting							
TLS Management							
in Logging							

When creating or editing Topology Hiding Profiles, there are six types of headers available for selection in the Header drop-down list to choose from. In addition to the six headers, there are additional headers not listed that are affected when either of two types of listed headers (e.g., **To Header** and **From Header**) are selected in the **Header** drop-down list. **Table 2** lists the six headers along with all of the other affected headers in three header categories (e.g., **Source Headers, Destination Headers, and SDP Headers**).

Topology Hiding Headers						
Main Header Names	Header(s) Affected by Main Header					
Source Headers						
Record-Route						
From	(1) Referred-By					
	(2) P-Asserted Identity					
Via						
Destinatio	n Headers					
То	(1) ReferTo					
Request-Line						
SDP H	eaders					
Origin Header						

**Table 2: Topology Hiding Headers** 

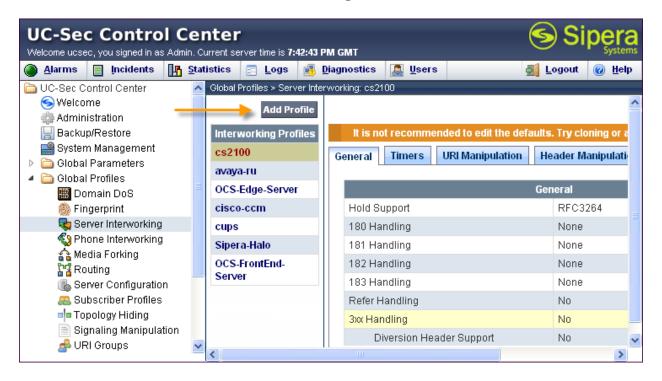
#### 6.1.3. Server Interworking Profile

The Server Interworking profile configures and manages various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters (for HA deployments), DoS security statistics, and trusted domains. Interworking Profile features are configured based on different Trunk Servers. There are default profiles available that may be used as is, or modified. New profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for the **Enterprise** and **IntelePeer<sup>TM</sup>**.

#### 6.1.3.1 Server Interworking Profile – Enterprise

To create a new Server Interworking Profile for the enterprise, navigate to UC-Sec Control Center  $\rightarrow$  Global Profiles  $\rightarrow$  Server Interworking and click on Add Profile as shown below.



Enter a descriptive name for the new profile and click Next to continue.

Interworking Profile				
Profile Name	Enterprise			
	Next			

PM; Reviewed: SPOC 5/25/2012 Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

In the new window that appears, enter the following values. Use default values for all remaining fields:

- Hold Support: Select RFC3264.
- **T.38 Support:** Checked.

Click Next to continue.

Editing Profile: Enterprise				
	General			
Hold Support	<ul> <li>None</li> <li>RFC2543 - c=0.0.0.0</li> <li>RFC3264 - a=sendonly</li> </ul>			
180 Handling	💿 None 🔘 SDP 🔘 No SDP			
181 Handling	💿 None 🔘 SDP 🔘 No SDP			
182 Handling	💿 None 🔘 SDP 🔘 No SDP			
183 Handling	💿 None 🔘 SDP 🔘 No SDP			
Refer Handling				
3xx Handling				
Diversion Header Support				
Delayed SDP Handling				
T.38 Support				
URI Scheme	💿 SIP 🔘 TEL 🔘 ANY			
Via Header Format	<ul> <li>RFC3261</li> <li>RFC2543</li> </ul>			
	Next			

Interworking Profile 🔀				
	Privacy			
Privacy Enabled				
User Name				
P-Asserted-Identity				
P-Preferred-Identity				
Privacy Header				
	DTHE			
	DTMF			
DTMF Support	💿 None 🔘 SIP NOTIFY 🔵 SIP INFO			
	Back Next			

Default values can be used for the next two windows that appear. Click Next to continue.

Interworking Profile 🔀						
Configuration is not required. All fields are optional.						
SIP Timers						
Min-SE	seconds, (90	- 86400]				
Init Timer	milliseconds	, [50 - 1000]				
Max Timer	milliseconds	, [200 - 8000]				
Trans Expire	seconds, [1 -	64]				
Invite Expire	seconds, [18	0 - 300]				
	Transport Timers					
TCP Connection Inactive Timer	seconds, [60	0 - 3600]				
	Back Next					

On the Advanced Settings window uncheck the following default settings:

- Topology Hiding: Change Call-ID
- Change Max Forwards
- Has Remote SBC

Click **Finish** to save changes.

Interworking	Profile 🛛 🔀
Advanced Se	ettings
Record Routes	<ul> <li>None</li> <li>Single Side</li> <li>Both Sides</li> </ul>
Topology Hiding: Change Call-ID	
Call-Info NAT	
Change Max Forwards	
Include End Point IP for Context Lookup	
OCS Extensions	
AVAYA Extensions	
NORTEL Extensions	
SLIC Extensions	
Diversion Manipulation	
Diversion Header URI	
Metaswitch Extensions	
Reset on Talk Spurt	
Reset SRTP Context on Session Refresh	
Has Remote SBC	
Route Response on Via Port	
Cisco Extensions	
Back Fi	nish

# 6.1.3.2 Server Interworking Profile – IntelePeer<sup>TM</sup>

To create a new Server Interworking Profile for IntelePeer<sup>TM</sup>, navigate to UC-Sec Control Center  $\rightarrow$  Global Profiles  $\rightarrow$  Server Interworking and click on Add Profile as shown below.

UC-Sec Control Cer Welcome ucsec, you signed in as Admin. Cu		1 GMT	Sipera Systems
Alarms Incidents A Stat		agnostics 🧟 Users	🛃 Logout 🔞 Help
UC-Sec Control Center  Welcome  Administration  Backup/Restore	Global Profiles > Server Interv Add Profile Interworking Profiles		Clone Profile Its. Try cloning or adding a new profile instead.
System Management     Global Parameters     Global Profiles	cs2100 avaya-ru	General Timers URI Manipulation	Header Manipulation Advanced
Domain DoS	OCS-Edge-Server		General
🎆 Fingerprint	cisco-ccm	Hold Support	RFC3264
Server Interworking	cups	180 Handling	None
Sector	Sipera-Halo	181 Handling	None
🚰 Media Forking	OCS-FrontEnd-Server	182 Handling	None
Server Configuration	Enterprise	183 Handling	None
a Subscriber Profiles	Controllate	Refer Handling	No
Topology Hiding		3xx Handling	No
📄 Signaling Manipulation 🎿 URI Groups		Diversion Header Support	No
SIP Cluster		Delayed SDP Handling	No
Domain Policies		T.38 Support	No
Device Specific Settings		URI Scheme	SIP
Troubleshooting		Via Header Format	RFC3261
<ul> <li>Canagement</li> <li>Canagement</li> <li>Canagement</li> </ul>			Privacy

Enter a descriptive name for the new profile and click **Next** to continue.

	Interworking Profile	×
Profile Name	Intelepeer	
	Next	

In the new window that appears, keep the default **Hold Support** value of **None**. IntelePeer<sup>TM</sup> SIP Trunk Service is not capable of supporting calls placed on hold by either the RFC 3264 method using the *a=sendonly* SDP attribute, or the RFC 2543 method of setting the address in the *c*= SDP line to 0.0.0.0. With the Hold Support set to None, it is necessary to create a Signaling Manipulation (**Section 6.1.4**) to remove the *sendonly* media attribute sent by Communication Manager.

Click Next to continue.

Interworking Profile		
	General	
Hold Support	<ul> <li>None</li> <li>RFC2543 - c=0.0.0.0</li> <li>RFC3264 - a=sendonly</li> </ul>	
180 Handling	💿 None 🔘 SDP 🔘 No SDP	
181 Handling	💿 None 🔘 SDP 🔘 No SDP	
182 Handling	💿 None 🔘 SDP 🔘 No SDP	
183 Handling	💿 None 🔘 SDP 🔘 No SDP	
Refer Handling		
3xx Handling		
Diversion Header Support		
Delayed SDP Handling		
T.38 Support		
URI Scheme	⊙ SIP ◯ TEL ◯ ANY	
Via Header Format	<ul> <li>● RFC3261</li> <li>● RFC2543</li> </ul>	
	Back Next	

Interworking Profile		
Privacy		
Privacy Enabled		
User Name		
P-Asserted-Identity		
P-Preferred-Identity		
Privacy Header		
DTMF		
DTMF Support	💿 None 🔘 SIP NOTIFY 🔵 SIP INFO	
Back Next		

Default values can be used for the next two windows that appear. Click Next to continue.

1	nterworking Profile 🛛 🔀		
Configuration is not required. All fields are optional.			
SIP Timers			
Min-SE	seconds, [90 - 86400]		
Init Timer	milliseconds, [50 - 1000]		
Max Timer	milliseconds, [200 - 8000]		
Trans Expire	seconds, [1 - 64]		
Invite Expire	seconds, [180 - 300]		
Transport Timers			
TCP Connection Inactive Timer	seconds, [600 - 3600]		
	Back Next		

On the **Advanced Settings** window the default values can be used. Click **Finish** to save changes.

Interworking	j Profile 🔀			
Advanced Settings				
Record Routes	<ul> <li>None</li> <li>Single Side</li> <li>Both Sides</li> </ul>			
Topology Hiding: Change Call-ID				
Call-Info NAT				
Change Max Forwards				
Include End Point IP for Context Lookup				
OCS Extensions				
AVAYA Extensions				
NORTEL Extensions				
SLIC Extensions				
Diversion Manipulation				
Diversion Header URI				
Metaswitch Extensions				
Reset on Talk Spurt				
Reset SRTP Context on Session Refresh				
Has Remote SBC				
Route Response on Via Port				
Cisco Extensions				
Back	inish			

## 6.1.4. 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 SBCE. Using this language, a script can be written and tied to a given flow through the EMS GUI. The Avaya SBCE appliance then interprets this script at the given entry point or "hook point".

PM; Reviewed:	Solution & Interoperability Test Lab Application Notes	37 of 65
SPOC 5/25/2012	©2012 Avaya Inc. All Rights Reserved.	IPeerCM601ASBCE

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, navigate to UC-Sec Control Center  $\rightarrow$  Global Profiles  $\rightarrow$  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 [13].

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 response from Communication Manager to an inbound call from IntelePeer<sup>™</sup> (e.g., 180 Ringing and 200 OK) while the second acts on the request of an outbound call to IntelePeer<sup>™</sup> 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"	Transformations applied to all SIP sessions.
•	act on response	Actions to be taken to the response of an
•	%DIRECTION="OUTBOUND"	INVITE (e.g., 180 Ringing and 200 OK). Applied to a messages leaving the Avaya
		SBCE.
٠	%ENTRY_POINT="POST_ROUTING"	The "hook point" to apply the script after the
		SIP message has routed through Avaya SBCE.
•	%HEADERS["p-asserted-identity"][1]	Used to retrieve an entire header. The first dimension denotes which header while the second dimension denotes the 1 <sup>st</sup> instance of the header in a message.
•	.regex_replace	
	("avayalab\.com","205.xxx.xxx.35:5060")	An action to replace a given match with the provide string (e.g., find "avayalab.com" and replace it with "205.xxx.xxx.35:5060".

The P-Asserted-Identity header will be modified by replacing the domain "avayalab.com" with the external IP address of the Avaya SBCE and the SIP port of 5060 in both the response and request sessions.

UC-Sec Control C Welcome ucsec, you signed in as Admin			т		S ⊗	ipera Systems
Alarms Incidents	<u>S</u> tat	istics 📄 Logs 🛃 Diagno	stics	Sers Users	Jegout	🕜 <u>H</u> elp
C-Sec Control Center	*	Global Profiles > Signaling Manipula	tion: SI	P Trunk2_Script		
S Welcome		Upload Script Add Script		Download Script	lone Script	elete Script
Backup/Restore		Signaling Manipulation		Click here to add a description.		
System Management		Scripts				
Global Parameters		SIP Trunk2_Script	Sig	naling Manipulation		
Global Profiles	=	saved	1	/ Topology Hiding of PAI header within 180 Ringing response		*
Domain DoS	-	CS1K_Script	W:	ithin session "ALL"		(≡)
🎆 Fingerprint 😼 👦 Server Interworking		CM_saved	<sup>1</sup>	act on response where %DIRECTION="OUTBOUND" and %ENTRY POINT="POST ROUTING"		-
Phone Interworking		test				
🚰 Media Forking		SIP Trunk4_Script		Edit		
🚰 Routing		SIP Trunk 1_Script				
Server Configuration						
Subscriber Profiles						
Signaling Manipulation						
🛃 URI Groups	Ŧ					
				😜 Internet   Protected Mode: On	🖓 🕶 🔍	100% 👻 🔐



The screen above shows the finished Signaling Manipulation Script IntelePeer<sup>™</sup> Script (SIP Trunk2\_Script).

Solution & Interoperability Test Lab Application Notes 3 ©2012 Avaya Inc. All Rights Reserved.

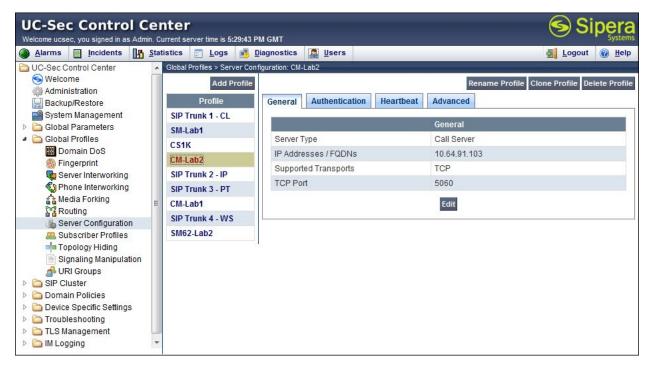
### 6.1.5. Server Configuration

The Server Configuration screen contains four tabs: General, Authentication, Heartbeat, and Advanced. Together, these tabs configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

In the sample configuration, separate Server Configurations were created for Communication \_Manager and IntelePeer<sup>TM</sup>.

#### 6.1.5.1 Server Configuration – Communication Manager

To add a Server Configuration Profile for Communication Manager, navigate to UC-Sec Control Center  $\rightarrow$  Global Profiles  $\rightarrow$  Server Configuration and click on Add Profile as shown below.



Enter a descriptive name for the new profile and click Next.

	Add Server Configuration Profile	×
Profile Name	CM-Lab2	
	Next	
	Conver Type	Trupk Conjor

PM; Reviewed: SPOC 5/25/2012

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

In the new window that appears, enter the following values. Use default values for all remaining fields:

- Server Type:
- Select Call Server from the drop-down box.
- IP Addresses / Supported FQDNs:
- Supported Transports:
- TCP Port:

Enter the IP address of the Communication Manager Processor Ethernet as defined in **Section 5.3**. Select **TCP**.

Port number on which to send SIP requests to
Communication Manager. This should match the port number used in the Far-end Listen Port in the
Communication Manager Signaling Group as defined
Section 5.7.

Click Next to continue.

Add Server Co	nfiguration Profile - General 🛛 🔀
Server Type	Call Server 🔹
IP Addresses / Supported FQDNs Comma seperated list	10.64.91.103
Supported Transports	TCP UDP TLS
TCP Port	5060
UDP Port	
TLS Port	
I	Back Next

Verify **Enable Authentication** is unchecked as Communication Manager does not require authentication. Click **Next** to continue.

Add Server Configuration Profile - Authentication 🛛 🔀				
Enable Authentication				
User Name				
Realm				
Password				
Confirm Password				
Back Next				

In the new window that appears, enter the following values. Use default values for all remaining fields:

<ul> <li>Enable Heat</li> <li>Method:</li> <li>Frequency:</li> </ul>	Select <b>OPTIONS</b> from the drop-down box. Choose the desired frequency in seconds the Avaya
	SBCE will send SIP OPTIONS. For compliance testing <b>60</b> seconds was chosen.
• From URI:	Enter the URI to be sent in the FROM header for SIP OPTIONS.
• To URI:	Enter the URI to be sent in the TO header for SIP OPTIONS.

Click Next to continue.

ve	General Authentication Heartbeat Advanced				
			Heartbeat		
	Ena	ble Heartbeat			
		Method	OPTIONS		
		Frequency	60 seconds		
		From URI	ping@avayalab.com		
		To URI	ping@avayalab.com		
	TCP	Probe			
	Edit				

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

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 6.1.3.1**. Use default values for all remaining fields. Click **Finish** to save the configuration (not shown).

	Advanced	
Enable DoS Protection		
Enable Grooming		
Interworking Profile	COMPACT NUMBER	
Signaling Manipulation Script	SIP Trunk2_Script	
UDP Connection Type	SUBID	
	Edit	

### 6.1.5.2 Server Configuration - IntelePeer™

To add a Server Configuration Profile for IntelePeer<sup>TM</sup> navigate to UC-Sec Control Center  $\rightarrow$  Global Profiles  $\rightarrow$  Server Configuration and click on Add Profile (not shown). Enter a descriptive name for the new profile and click Next.

	Add Server Configuration Profile	×
Profile Name	Intelepeer	
	Next	

In the new window that appears, enter the following values. Use default values for all remaining fields:

	er Type: ddresses /	Select <b>Trunk Server</b> from the drop-down box.
	oorted FQDNs:	Enter the IP address(es) of the SIP proxy(ies) of the service provider. In the case of the compliance test, this is the IntelePeer <sup>TM</sup> SIP Trunk IP address. This will associate the inbound SIP messages from IntelePeer <sup>TM</sup> to this Sever Configuration.
• Supp	oorted Transports:	Select the transport protocol to be used for SIP traffic between Avaya SBCE and IntelePeer <sup>TM</sup> .
• UDP	Port:	Enter the port number that IntelePeer <sup>TM</sup> uses to send SIP traffic.

Click Next to continue.

Edit Server Conf	iguration Profile - General 🛛 🔀
Server Type	Trunk Server 💌
IP Addresses / Supported FQDNs Comma seperated list	68.XX. XXX.41
Supported Transports	□ TCP ■ UDP □ TLS
TCP Port	
UDP Port	5060
TLS Port	
	Finish

Verify **Enable Authentication** is unchecked as IntelePeer<sup>™</sup> does not require authentication. Click **Next** to continue.

Add Server C	onfiguration Profile - Authentication	×
Enable Authentication		
User Name		
Realm		
Password		
Confirm Password		
	Back Next	

In the new window that appears, enter the following values. Use default values for all remaining fields:

Enable Heartbeat: Checked.
 Method: Select OPTIONS from the drop-down box.
 Frequency: Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS. For compliance testing 60 seconds was chosen.

PM; Reviewed:	Solution & Interoperability Test Lab Application Notes	44 of 65
SPOC 5/25/2012	©2012 Avaya Inc. All Rights Reserved.	IPeerCM601ASBCE

•	From URI:	Enter the URI to be sent in the FROM header for SIP OPTIONS.
•	To URI:	Enter the URI to be sent in the TO header for SIP OPTIONS.

Click Next to continue.

The SIP OPTIONS are sent to the SIP proxy(ies) entered in the **IP Addresses /Supported FQDNs** in the **Server Configuration Profile.** The URI of PING@ IntelePeer.com was used in the sample configuration to better identify the SIP OPTIONS in the call traces. IntelePeer<sup>TM</sup> does not look at the From and To headers when replying to SIP OPTIONS so any URI can be used as long as it is in the proper format (USER@DOMAIN).

Heartbeat		
Enable Heartbeat		
Method	OPTIONS	
Frequency	60 seconds	
From URI	PING@Intelepeer.com	
To URI	PING@Intelepeer.com	
TCP Probe		

In the new window that appears, select the **Interworking Profile** created for IntelePeer<sup>TM</sup> in **Section 6.1.3.2**. Select the **Signaling Manipulation Script** created in **Section 6.1.4**. Use default values for all remaining fields. Click **Finish** to save the configuration (not shown).

Advanced		
Enable DoS Protection		
Enable Grooming		
Interworking Profile	State Constant and The	
Signaling Manipulation Script	SIP Trunk2_Script	
UDP Connection Type	SUBID	

## 6.2. Domain Policies

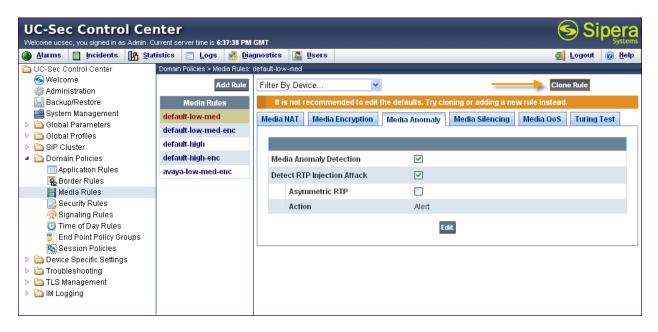
The Domain Policies feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating to the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control, and normalize call flows. There are default policies available to use, or a custom domain policy can be created.

#### 6.2.1. Media Rules

Media Rules define RTP media packet parameters such as packet encryption techniques and prioritizing 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 IntelePeer<sup>TM</sup>.

To create a custom Media Rule, navigate to UC-Sec Control Center  $\rightarrow$  Domain Policies  $\rightarrow$  Media Rules. With default-low-med selected, click Clone Rule as shown below.



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

	Clone Rule	×
Rule Name	default-low-med	
Clone Name	No-Media-Detection	
	Finish	

When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, the Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being

created during an audio shuffle. To modify the rule, select the **Media Anomaly** tab and click **Edit**. Uncheck **Media Anomaly Detection** and click **Finish** (not shown).

UC-Sec Control Cer Welcome ucsec, you signed in as Admin. C		GMT	Sipera Systems
Alarms Incidents A State	tistics 🔄 Logs 📑 Dia	gnostics 🔝 Users	<u> L</u> ogout 🕜 <u>H</u> elp
🛅 UC-Sec Control Center	Domain Policies > Media Rules:	No-Media-Detection	
S Welcome	Add Rule	Filter By Device	Rename Rule Clone Rule Delete Rule
Administration			
Backup/Restore	Media Rules	Click here to add a	lescription.
System Management	default-low-med	Media NAT Media Encryption Media Anomaly M	edia Silencing Media QoS Turing Test
Image: Comparison of the second se	default-low-med-enc		
<ul> <li>Global Profiles</li> <li>GIP Cluster</li> </ul>	default-high		
	default-high-enc	Madia Anomaly Detection	
		Media Anomaly Detection	
	-	Edit	
	No-Media-Detection		
Security Rules			
🧖 Signaling Rules			
🔯 Time of Day Rules			
🏐 End Point Policy Groups			
🌇 Session Policies			
Device Specific Settings			
Troubleshooting			
TLS Management			
IM Logging			
<ul> <li>Signaling Rules</li> <li>Time of Day Rules</li> <li>End Point Policy Groups</li> <li>Session Policies</li> <li>Device Specific Settings</li> <li>Troubleshooting</li> <li>TLS Management</li> </ul>	default-high-enc avaya-low-med-enc No-Media-Detection	Media Anomaly Detection	

The following screen shows the **No-Media-Detection** rule with **Media Anomaly Detection** disabled.

On the **Media QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for compliance testing.

UC-Sec Control Center Signature Sign			
Alarms Incidents A Stat	istics 📄 Logs 🛃 Dia	ignostics 🎑 <u>U</u> sers	🛃 Logout 🔞 <u>H</u> elp
C-Sec Control Center	Domain Policies > Media Rules:	No-Media-Detection	
S Welcome	Add Rule	Filter By Device 💌	Rename Rule Clone Rule Delete Rule
Administration			
🔚 Backup/Restore	Media Rules		Click here to add a description.
System Management Global Parameters	default-low-med	Media NAT Media Encryption	Media Anomaly Media Silencing Media QoS Turing Test
<ul> <li>Global Profiles</li> </ul>	default-low-med-enc		
<ul> <li>Clobal Fibries</li> <li>Clobal Fibries</li> <li>SIP Cluster</li> </ul>	default-high		Media QoS Reporting
Domain Policies	default-high-enc	RTCP Enabled	
Application Rules	avaya-low-med-enc		
🛃 Border Rules	No-Media-Detection		Media QoS Marking
🧮 Media Rules		Enabled	
Security Rules		QoS Type	DSCP
👰 Signaling Rules 🔯 Time of Day Rules		003 1990	5001
End Point Policy Groups			Audio QoS
Session Policies		Audio DSCP	EF
Device Specific Settings		And Dool	
Troubleshooting			Video QoS
TLS Management		Video DSCP	EF
IM Logging			
			Edit

PM; Reviewed: SPOC 5/25/2012 Solution & Interoperability Test Lab Application Notes47 of 65©2012 Avaya Inc. All Rights Reserved.IPeerCM6

#### 6.2.2. Signaling Rules

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the UC-Sec, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

Clone and modify the **default** signaling rule to strip the Alert Info header from the SIP message to hide the topology of the enterprise network from the external network before it is sent to IntelePeer<sup>TM</sup>. To clone a signaling rule, navigate to UC-Sec Control Center  $\rightarrow$  Domain Policies  $\rightarrow$  Signaling Rules. With the default rule chosen, click on Clone Rule as shown below.

UC-Sec Contro Welcome ucsec, you signed in as			N GMT	(Si∣	
Alarms Incidents	🖪 Stati	istics 📄 Logs 📑 Dia	gnostics 🎑 Users	🚮 Logout	🕜 Help
🛅 UC-Sec Control Center	~	Domain Policies > Signaling Rul	es: default		
S Welcome		Add Rule	Filter By Device 💌	Clone Rule	
📓 Backup/Restore		Signaling Rules	It is not recommended to edit the d	lefaults. Try cloning or adding a new rule instead.	
System Management	=	default	General Requests Responses	Request Headers Response Headers Signaling	QoS
<ul> <li>Global Parameters</li> <li>Global Profiles</li> <li>OD Objective</li> </ul>		No-Content-Type- Checks		Inbound	
SIP Cluster Image: A state of the		default_Rm-P-Loc	Requests	Allow	Ξ
Application Rules			Non-2XX Final Responses	Allow	
📕 Border Rules			Optional Request Headers	Allow	
📕 Media Rules 📄 Security Rules			Optional Response Headers	Allow	
Signaling Rules	~				<b>~</b>

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

	Clone Rule 🛛 🕅
Rule Name	default
Clone Name	default_Rm-Headers
	Finish

Select the **Request Headers tab** and click **Add In Header Control** (not shown). In the new window that appears, enter the following values. Use default values for all remaining fields:

- Header Name:
- Method Name:
- Header Criteria:
- Presence Action:

Enter Alert-Info. Select INVITE from the drop-down box. Select Forbidden. Select Remove header from the drop-down box.

Click **Finish** to save the configuration

Add Header Control		
Proprietary Request Header?		
Header Name	Alert-Info	
Method Name	INVITE -	
Header Criteria	<ul> <li>Forbidden</li> <li>Mandatory</li> <li>Optional</li> </ul>	
Presence Action	Remove header  486 Busy Here	
Finish		

Repeat these steps for any other headers that should be removed. The following screens show the **default\_Rm-Headers** rule used in the sample configuration with the **Alert-Info** header configured to be removed.

UC-Sec Control C Welcome ucsec, you signed in as Admin			GM	т						(	s Si	p		a
🅘 Alarms 📄 Incidents 📭	<u>S</u> tat	istics 📄 Logs 🛃 Diag	nos	tics	🧸 Users					2	Logout	0	<u>H</u> e	əlp
C-Sec Control Center	~	Domain Policies > Signaling Rules	:: de	fault_R	m-Headers									
S Welcome		Add Rule	F	ilter B	/ Device	*			Rena	ame Rule Clo	ne Rule	)ele	te Ru	ule
📄 Backup/Restore		Signaling Rules					CI	lick here to add a (	lescription.					
System Management Global Parameters		default	G	ienera	Requests	Responses	R	Request Headers	Response He	aders Sigr	aling QoS	1		
👂 🫅 Global Profiles		No-Content-Type- Checks												
SIP Cluster	Ξ	default_Rm-Headers	Add In Header Control Add Out Header Con											
Image: A constraint of the second						Met	hod	Header						
Application Rules				Row	Header Name	Na		Criteria	Action	Proprietary	Direction			
i Border Rules III Media Rules IIII Security Rules				1	Alert-Info	INVITE		Forbidden	Remove Header	No	IN	ø	×	
Signaling Rules														
🔯 Time of Day Rules														
🏐 End Point Policy Groups														
🐚 Session Policies	~													

On the **Signaling QoS** tab select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS values used for compliance testing.

	UC-Sec Control Center Signed in as Admin. Current server time is 10:03:51 PM GMT									
🅘 Alarms 📋 Incidents 👫 S	tati	istics 📃 Logs 💰 Diag	nos	tics 🏼 🌆	<u>U</u> sers					🛃 Logout 🕜 Help
	^	Domain Policies > Signaling Rules	s: de	fault_Rm-l	Headers					
S Welcome		Add Rule	F	ilter By D	)evice	*			Rename Rule	e Cione Ruie Delete Ruie
🔚 Backup/Restore		Signaling Rules					Click	here to add a d	lescription.	
System Management Global Parameters		default	G	ieneral	Requests	Responses	Requ	est Headers	Response Headers	Signaling QoS
Global Profiles		No-Content-Type- Checks								
SIP Cluster	Ξ									
🔺 🚞 Domain Policies		default_Rm-Headers		Signali	ng QoS			<b>~</b>		
Application Rules				QoS	Type			DSCP		
🔒 Border Rules				DSCF				EF		
📔 Media Rules				DSCR	,			Er		
Security Rules								Edit		
Signaling Rules	-									
🕑 Time of Day Rules										
Session Policies										
	~									

#### 6.2.3. 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 sessions allowed. 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  $\rightarrow$  Domain Policies  $\rightarrow$  Application Rules. With the **default** rule chosen, click on Clone Rule as shown below.

🖹 Alarms 🔲 Incidents 📭 Sta		GMT gnostics 🔝 Users		SI Logout 🕢 H
UC-Sec Control Center	Domain Policies > Application R	ules: default		
S Welcome	Add Rule	Filter By Device	*	Clone Rule
Backup/Restore	Application Rules	It is not recommended to	edit the defaults. Try clon	ing or adding a new rule instead.
🧱 System Management	default	Application Rule		
🕞 🛅 Global Parameters		Application Rule		
> Calobal Profiles > Calobal Profiles > Calobal Profiles		Application Type	In Out Maximu	m Concurrent Maximum Sessions Per
Domain Policies		Аррисации туре	St	essions Endpoint
Application Rules		Voice	🗹 🗹 200	10
🝓 Border Rules		Video		
🧮 Media Rules 🗔 Security Rules		IM		
Signaling Rules				
ime of Day Rules			Miscella	neous
🛐 End Point Policy Groups		CDR Support	None	
No Session Policies		IM Logging	No	
Device Specific Settings Troubleshooting		RTCP Keep-Alive	No	
<ul> <li>TLS Management</li> </ul>			Edit	1
IM Logging			Edit	

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

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

Loga an Diagnostica An Dacia	Clone Rule 🔀
Rule Name	default
Clone Name	MaxVoiceSession
	Finish

Modify the rule by clicking the **Edit** button. Set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. Keep in mind the 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 Sessions 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 5.8**) to the allotted amount. Therefore, the values in the Application Rule **MaxVoice** were set high enough to be considered non-blocking.

Alarms Incidents	<u>S</u> tatistic:	s 📄 Logs 🛃 Diag	gno	stics 🔝 Users				🗾 Logout	0 L
UC-Sec Control Center	🔺 Dom	ain Policies > Application Ru	ules	: MaxVoiceSession					
S Welcome		Add Rule	Fi	ilter By Device	•			Rename Rule Clone Rule De	lete
Administration     Image: Backup/Restore		Application Rules				CI	lick here to add a descriptio	n.	
System Management Global Parameters		fault IxVoiceSession	A	pplication Rule					
<ul> <li>Clobal Profiles</li> <li>Cluster</li> <li>Domain Policies</li> </ul>				Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint	
Application Rules	-			Voice		✓	2000	2000	
Border Rules	=			Video		Г			
📕 Media Rules 📄 Security Rules				IM					
🧖 Signaling Rules							Miscellaneous		
🔯 Time of Day Rules				CDR Support	No	ne			
End Point Policy Groups Session Policies				IM Logging	No				
Device Specific Settings				RTCP Keep-Alive	No				
Troubleshooting			Edit						

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

#### 6.2.4. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 6.3.4.** Create a separate Endpoint Policy Group for both the enterprise and the IntelePeer<sup>™</sup> SIP Trunk Service.

To create a new policy group, navigate to UC-Sec Control Center  $\rightarrow$  Domain Policies  $\rightarrow$  Endpoint Policy Groups and click on Add Group as shown below.

UC-Sec Control Cer Welcome ucsec, you signed in as Admin. Co		бМТ						Sipe	era <sub>/stems</sub>			
Alarms Incidents Alarms	tistics 📄 Logs 🛃 Dia	jnostics 🛛	Users					🛃 Logout 🕜 !	<u>H</u> elp			
C-Sec Control Center	Domain Policies > End Point Polic	cy Groups: det	ault-low									
S Welcome	Add Group	Filter By D	)evice	*								
🔚 Backup/Restore	Policy Groups	blicy Groups It is not recommended to edit the defaults. Try adding a new group instead.										
🔛 System Management	default-low	t-low										
Global Parameters	default-low-enc	Click here to add a row description.										
Global Profiles	default-med	Policy Gro	up									
SIP Cluster												
Domain Policies	default-med-enc						View Sum	mary Add Policy Se	et			
Application Rules	default-high											
🕵 Border Rules 🗮 Media Rules	default-high-enc	Order	Application	Border	Media	Security	Signaling	Time of Day				
Security Rules	OCS-default-high	1	default	default	default-low-	default-low	default	default 🥒 🛚	ф			
Signaling Rules	avaya-def-low-enc			dondan	med	doladinon	donadit		-			
讨 Time of Day Rules	Enternine Demiliation											
🐻 End Point Policy Groups												
Soccion Policion												

The following screen shows the Enterprise\_DomPolicy created for the enterprise. Set the Application, Media and Signaling rules to the ones previously created. Set the Border and Time of Day rules to default and set the Security rule to default-low.

UC-Sec Control C Welcome ucsec, you signed in as Admir			CM	Ŧ						Si 🔊	p	
				stics	<u>U</u> sers					<u> L</u> ogout	0	<u>H</u> elp
DC-Sec Control Center	*	Domain Policies > End Point Polici	cy C	Groups: Ente	rprise_DomPolicy						-	
S Welcome		Add Group	F	ilter By De	vice	-			Rena	me Group De	elete	Group
Backup/Restore		Policy Groups				Click	here to add a	a description.				
🚔 System Management		default-low							· · · ·			
Global Parameters		default-low-enc				Hover ov	er a row to se	e its descript	lion.			
<ul> <li>Global Profiles</li> <li>Global Profiles</li> </ul>		default-med	F	Policy Grou	р							
<ul> <li>Image: Cluster</li> <li>Image: Cluster<td></td><td>default-med-enc</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>_ 1</td></li></ul>		default-med-enc										_ 1
Application Rules	-	default-high							View Sum	mary Add Po	olicy	Set
Border Rules	=	default-high-enc		Order	Application	Border	Media	Security	Signaling	Time of		
Media Rules		OCS-default-high		01401	Approduction	Bordon	linounu	coounty	orginaling	Day		
Security Rules Signaling Rules		avaya-def-low-enc		1	MaxVoiceSession	default	New-Low- Med	default-low	Avaya	default	ø	÷
ime of Day Rules		Enterprise_DomPolicy					mod					
🐻 End Point Policy Groups		SIP Trunk_DomPolicy										
Session Policies		Enterprise_enc										
Device Specific Settings												
Troubleshooting												
TLS Management	-											
						😜 Inter	net   Protected	l Mode: On			100%	• • "

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. The following screen shows the **SIP Trunk\_DomPolicy** created for the IntelePeer<sup>TM</sup> SIP Trunk Service. Set the **Application**, **Media** and **Signaling** (Avaya) rules to the ones previously created. Set the **Border** and **Time of Day** rules to **default** and set the **Security** rule to **defaulthigh**.

UC-Sec Control Ce Welcome ucsec, you signed in as Admin.			50:59 PI	M GMT							si) Si	pę				
Alarms Incidents A S	tatistics	📃 Logs	📑 Di	agnostics	🔝 <u>U</u> ser	s				2	<u>L</u> ogout	0	<u>H</u> elp			
C-Sec Control Center	<ul> <li>Domain</li> </ul>	1 Policies > End	Point Po	licy Groups:	SIP Trunk_D	omPolicy										
S Welcome Administration Backup/Restore		Policy Groups			Filter By Device     Rename Group     Det       Click here to add a description.											
<ul> <li>System Management</li> <li>Global Parameters</li> <li>Global Profiles</li> </ul>	defa	lefault-low lefault-low-enc		Policy Gr	oup	Но	Hover over a row to see its description.									
<ul> <li>D Cluster</li> <li>Domain Policies</li> <li>Application Rules</li> </ul>	defa	ult-med-enc ult-high							v	iew Summa	ry Add Po	licy	Set			
🚭 Border Rules 📕 Media Rules		ult-high-enc -default-high		Orde	r App	olication	Border	Media	Security	Signaling	Time of Day					
Becurity Rules	-	a-def-low-end rprise_DomP		1	MaxVoi	iceSession	default	New-Low -Med	default- high	Avaya	default	Ø	÷			
<ul> <li>End Point Policy Groups</li> <li>Session Policies</li> <li>Device Specific Settings</li> <li>Network Management</li> <li>Media Interface</li> <li>Signaling Interface</li> <li>Signaling Forking</li> <li>ShMP</li> <li>End Point Flows</li> <li>Session Flows</li> <li>Two Factor</li> <li>Relay Services</li> <li>Troubleshooting</li> <li>TLS Management</li> </ul>	_	DomPolicy Trunk_DomPo	Diicy													

## 6.3. Device Specific Settings

The Device Specific Settings feature allows aggregate system information to be viewed, and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

## 6.3.1. Network Management

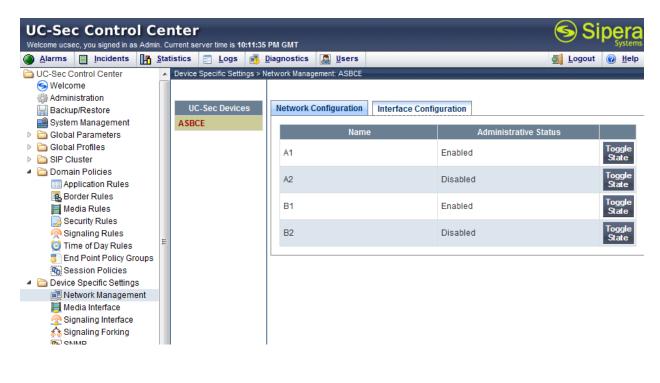
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

PM; Reviewed:	Solution & Interoperability Test Lab Application Notes	53 of 65
SPOC 5/25/2012	©2012 Avaya Inc. All Rights Reserved.	IPeerCM601ASBCE

Navigate to UC-Sec Control Center  $\rightarrow$  Device Specific Settings  $\rightarrow$  Network Management and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to A1 and the external interface is assigned to B1.

UC-Sec Control C Welcome ucsec, you signed in as Adm				5:37:21 PM GN	т							6	Si	pę	era
		istics	📃 Logs			Users						<u>si</u> 1	ogout	0	Help
🛅 UC-Sec Control Center	*	Device	Specific Set	tings > Networ	k Manag	ement: ASBCE									
S Welcome															
🌼 Administration		_													
🔚 Backup/Restore			UC-Sec D	evices	Net	work Configu	ration Inter	face	Configuration						
📫 System Management		ASBC	E												
Global Parameters									an IP address or its assoc			ation restart be	efore ta	king	
Global Profiles						effect. App	lication restar	ts ca	in be issued from <u>System</u>	Manager	<u>nent</u> .				
SIP Cluster															
Domain Policies						A1 Netr			A2 Netmask		31 Netmask	B2 N	etmasi	C	
Device Specific Settings						255.255.255.0	)			255.25	55.255.128				
Retwork Management	=														
🧮 Media Interface					A	dd IP						Save Changes	Clear	Chang	jes
🛜 Signaling Interface						IP A	ddress		Public IP		Gatew	/ay	Inter	face	
signaling Forking 💫						40.00.450.400					10.80.150.1	-	A1		~
C SNMP						10.80.150.100					10.80.150.1		AI	•	×
🞒 End Point Flows						20592					205.100.02.1		B1	-	$\mathbf{x}$
Session Flows											0.05 (000000) 4		DI		~
🚜 Two Factor						205. 100 35					205.1		B1	•	×
a Relay Services															
Troubleshooting															
TLS Management	-														
_															

Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows that the interfaces A1 and B1 are Enabled. To enable an interface click it's **Toggle State** button.



PM; Reviewed: SPOC 5/25/2012 Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

### 6.3.2. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. The Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to UC-Sec Control Center  $\rightarrow$  Device Specific Settings  $\rightarrow$  Signaling Interface and click Add Signaling Interface.

The following screen shows the signaling interfaces created in the sample configuration with TCP and UDP ports 5060 used for the inside and outside IP interfaces respectively.

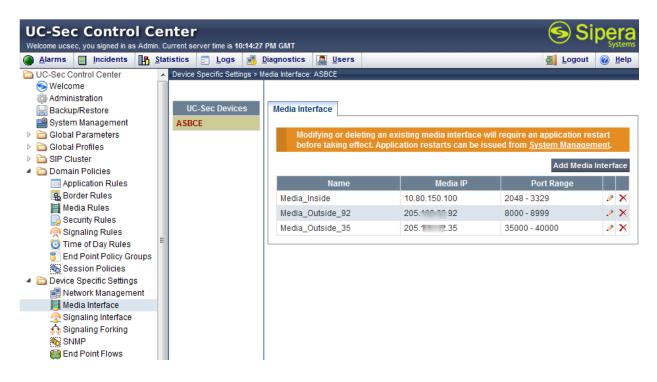


#### 6.3.3. Media Interface

The Media Interface screen is where the media ports are defined. The Avaya SBCE will listen for RTP media on the defined ports. Create a Media Interface for both the inside and outside IP interfaces. The inside port range needs to match the **UDP Port Min** and **UDP Port Max** fields in the Communication Manager IP Network Region form created in **Section 5.6.** The outside port range should match the RTP port range provided by IntelePeer<sup>TM</sup>.

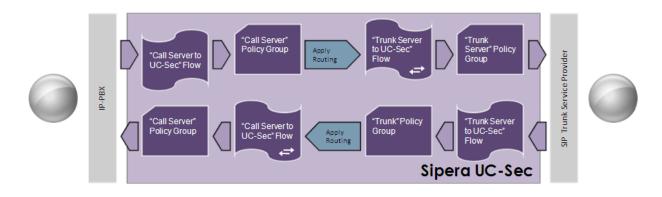
To create a new Media Interface, navigate to UC-Sec Control Center  $\rightarrow$  Device Specific Settings  $\rightarrow$  Media Interface and click Add Media Interface.

The following screen shows the media interfaces created in the sample configuration for the inside and outside IP interfaces. After the media interfaces are created, an application restart is necessary before the changes will take effect.



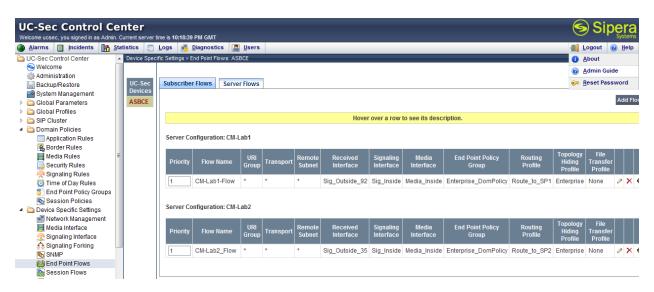
## 6.3.4. End Point Flows - Server Flow

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



PM; Reviewed: SPOC 5/25/2012 Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

Create a Server Flow for Communication Manager and the IntelePeer<sup>TM</sup> SIP Trunk Service. To create a Server Flow, navigate to UC-Sec Control Center  $\rightarrow$  Device Specific Settings  $\rightarrow$  End Point Flows. Select the Server Flows tab and click Add Flow as shown below.



In the new window that appears, enter the following values. Use default values for all remaining fields:

Flow Name: Enter a descriptive name. • Server Configuration: Select a Server Configuration created in Section 6.1.5 to • assign to the Flow. **Received Interface:** Select the Signaling Interface the Server Configuration is • allowed to receive SIP messages from. **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration. **Media Interface:** Select the Media Interface used to communicate with the • Server Configuration. **End Point Policy Group:** Select the policy assigned to the Server Configuration. ٠ **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to. **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration. •

Click Finish to save and exit.

The following screen shows the Sever Flow for IntelePeer<sup>™</sup>:

	Edit Flow: SP2_Flow	×
	Criteria	
Flow Name	\$P2_Flow	
Server Configuration	SIP Trunk 2 - IP 💌	
URI Group	*	
Transport	*	
Remote Subnet	*	
Received Interface	Sig_Inside 💌	
Signaling Interface	Sig_Outside_35 💌	
Media Interface	Media_Outside_35 -	
End Point Policy Group	SIP Trunk_DomPolicy	
Routing Profile	Route_to_CM-Lab2 -	
Topology Hiding Profile	SP2-Topology	
File Transfer Profile	None 💌	
	Finish	

The following screen shows the Sever Flow for Communication Manager:

Edit Flov	w: CM-Lab2_Flow 🔀
	Criteria
Flow Name	CM-Lab2_Flow
Server Configuration	CM-Lab2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_35 -
Signaling Interface	Sig_Inside •
Media Interface	Media_Inside
End Point Policy Group	Enterprise_DomPolicy -
Routing Profile	Route_to_SP2
Topology Hiding Profile	Enterprise 💌
File Transfer Profile	None 💌
	Finish

# 7. IP SIP Trunk Service Configuration

To use the SIP Trunk Service, a customer must request the service from IntelePeer<sup>TM</sup> using their sales process. This process can be initiated by contacting IntelePeer<sup>TM</sup> via the corporate web site at <u>www.IntelePeer.com</u> and requesting information via the online sales links or telephone numbers.

## 8. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

### 8.1. Verification

The following steps may be used to verify the configuration:

- 1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active for more than 35 seconds. This time period is included to verify that proper routing of the SIP messaging has satisfied SIP protocol timers.
- 2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active for more than 35 seconds.
- 3. Verify that the user on the PSTN can end an active call by hanging up.
- 4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

Use the SAT interface on Communication Manager to verify status of SIP trunks. Specifically use the **status trunk n** command to verify the active call has ended. Where **n** is the trunk group number used for IntelePeer<sup>™</sup> SIP Trunk Service defined in **Section 5.8**.

Below is an example of an active call.

status trui	nk 2						
		TRUNK GROUP STATUS					
Member	Port	Service State	Mtce Connected Ports Busy				
<b>0001/001</b> 0001/002 0001/003 0001/004	T00002 T00003	<pre>in-service/active in-service/idle in-service/idle in-service/idle</pre>	<b>no S00000</b> no no no				

Verify the port returns to **in-service/idle** after the call has ended.

status trunk 2							
		TRUNK GROUP STATUS					
Member	Port	Service State	Mtce Connected Ports Busy				
0001/001	T00001	in-service/idle	no				
0001/002	т00002	in-service/idle	no				
0001/003	T00003	in-service/idle	no				
0001/004	T00004	in-service/idle	no				

## 8.2. 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:
  - Incidences Displays alerts captured by the UC-Sec appliance.

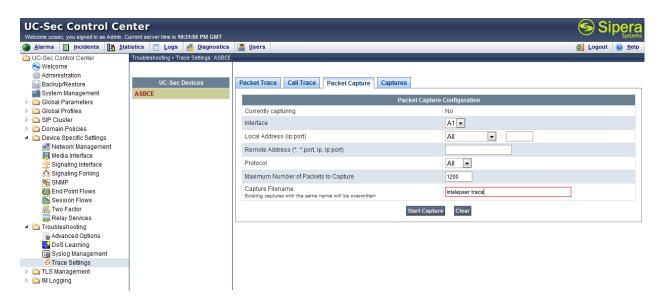
Incident Type	Incident ID	Date	Time	Category	Device	Cause
Message Dropped	662168149391824	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168147389246	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168146388212	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	662165350683634	12/19/11	9:38 PM	Policy	Sipera	Server Heartbeat is UP

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

Diagnostics		^
UC-Sec Devices	Full Diagnostic         Ping Test         Application         Protocol	
Sipera	Device to Pinging 10.80.150.206	
	Source Average ping from 10.80.150.100 to 10.80.150.206 is 0.353ms.	
	Destination	
	Ping	
		-

PM; Reviewed: SPOC 5/25/2012 Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved.

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





The packet capture file can be downloaded and viewed using a Network Protocol Analyzer such as Wireshark:

7 test 20111220170523 (1).pcap - Wires	hark				
File Edit View Go Capture Analyze Statisti					
			0,0,0,10   🖬 🗹 🖪 💥   💢		
	- ~ ~ ~ V 👱				
Filter: sip	•	Expression	Clear Apply		
No. Time Source	Destination	Protocol	Info		
1 0.000000 10.80.150.100	10.80.150.206	SIP	Request: OPTIONS sip:avayalab.c	om	
2 0.003282 10.80.150.206 13 6.058398 10.80.150.100	10.80.150.100 10.80.150.206	SIP SIP	Status: 200 OK Request: OPTIONS sip:avavalab.c		
14 6.060999 10.80.150.206	10.80.150.208	SIP	Status: 200 OK	Um	
36 15.346090 10.80.150.206	10.80.150.100	SIP/SDP		avaval	ab.com. with session (
38 15.347721 10.80.150.100	10.80.150.206	SIP	Status: 100 Trving	avayar	ab.com, wren session (
52 21.031715 10.80.150.100	10.80.150.206		Status: 183 Session Progress, w	ith se	ssion description
<					>
■ Frame 36: 790 bytes on wire (63)	20 hits). 790 hytes ca	ntured (6	320 hits)		
⊞ Ethernet II, Src: HewlettP_f3:c				3:75)	
∃ Internet Protocol, Src: 10.80.1					
■ Transmission Control Protocol, :				L, Len:	: 736
■ [Reassembled TCP Segments (2196)	bytes): #34(1460), #3	6(736)]			
Session Initiation Protocol					
Request-Line: INVITE sip:303	7@avayalab.com SI	P/2.0			
🗆 Message Header					
Record-Route: <sip:7dbc32cfc< td=""><td></td><td></td><th>&gt; *016asm-callprocessing.sar-86256</th><td></td><td></td></sip:7dbc32cfc<>			> *016asm-callprocessing.sar-86256		
			tag=80585cd1cd32e11c2514f1a2b700	+342~L:	324400/39083~639526/
I To: <sip:303 97@avayala<="" p=""></sip:303>		Tab. Com>,	ag=80383Curcuszerrcz31411azb/00		
Call-ID: 80585cd1cd32e11c35					
	206;branch=z9hG4bK0A50	96CDFFFFF	FF8F9BE58B01904681-AP;ft=61156		
■ Via: SIP/2.0/TCP 10.80.150.3					
⊞ Via: SIP/2.0/TCP 10.80.150.3					
■ Via: SIP/2.0/TCP 10.80.150.3					
			cd32e11c4514f1a2b700-AP;ft=79689		
☑ Via: SIP/2.0/TLS 10.80.150.3					
■ Via: SIP/2.0/TLS 10.80.150.3 Supported: 100rel,join,repl		KZ78_4et0	bar215812e1-62174405_I13003		
Allow: INVITE,ACK,OPTIONS,B		דדבע מברה	TNEO BRACK DUBLITSH		
			.1.5.0.615006 Avaya CM/R016x.00.3	1 510 1	
■ Contact: "Loc 150, SIP 9611					-
Accept-Language: en	State				
Alert-Info: <cid:internal@av< td=""><td>vayalab.com&gt;;avaya-cm-</td><td>alert-typ</td><th>e=internal</th><td></td><td></td></cid:internal@av<>	vayalab.com>;avaya-cm-	alert-typ	e=internal		
Min-SE: 1200	· · · ·	21-			
🗆 D. Accontod. Idoptitur. 🗥 1	50, SIP 9611G" <sip:+7< td=""><td>13 61</td><th>Bawawalah coma</th><td></td><td></td></sip:+7<>	13 61	Bawawalah coma		
■ P-Asserieu-Iuentity: LOC I			wavayaTab.Com>		~
P-Assenced-identity: LOC I	· · ·		savayalab.com>		>

# 9. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Session Border Controller for Enterprise and Avaya Aura® Communication Manager Evolution Server to the IntelePeer<sup>TM</sup> SIP Trunk Service. The IntelePeer<sup>TM</sup> SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The IntelePeer<sup>TM</sup> SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

Solution & Interoperability Test Lab Application Notes ©2012 Avaya Inc. All Rights Reserved. 63 of 65 IPeerCMe

## 10. References

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

- [1] Installing and Configuring Avaya Aura® System Platform, Release 6.0.3, Issue 2.1, March 2012.
- [2] Administering Avaya Aura® System Platform, Release 6.0.3, February 2011.
- [3] Administering Avaya Aura® Communication Manager, Release 6.0, Document Number 03-300509, Issue 6.0, June 2010
- [4] Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.0, Document Number 555-245-205, Issue 8.0, June 2010
- [5] Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x, Document Number 16-601443.
- [6] 4600 Series IP Telephone LAN Administrator Guide, Document Number 555-233-507.
- [7] Avaya one-X Deskphone H.323 Administrator Guide, May 2011, Document Number 16-300698.
- [8] Avaya one-X Deskphone SIP Administrator Guide Release 6.1, Document Number 16-603838
- [9] Administering Avaya one-X Communicator, July 2011
- [10] Administrator Guide for Avaya Communication Manager, Document Number 03-300509.
- [11] Feature Description and Implementation for Avaya Communication Manager, Document Number 555-245-205
- [12] UC-Sec Install Guide (102-5224-400v1.01)
- [13] UC-Sec Administration Guide (010-5423-400v106)
- [14] RFC 3261 SIP: Session Initiation Protocol, <u>http://www.ietf.org/</u>
- [15] RFC 3515, The Session Initiation Protocol (SIP) Refer Method, http://www.ietf.org/
- [16] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,* <u>http://www.ietf.org/</u>
- [17] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information, <u>http://www.ietf.org/</u>*

#### ©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and <sup>TM</sup> 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 <u>devconnect@avaya.com</u>.