



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Windstream SIP Trunking (Metaswitch Platform) with Avaya Aura® Communication Manager Access Element 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5 – Issue 1.0

Abstract

These Application Notes describes the steps to configure Session Initiation Protocol (SIP) Trunking between Windstream and Avaya Aura® Communication Manager Access Element 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5.

Windstream SIP Trunking provides PSTN access via a SIP trunk between the enterprise and the Windstream network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

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

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	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager	9
5.1.	Licensing and Capacity	9
5.2.	System Features	10
5.3.	IP Node Names	11
5.4.	Codecs	11
5.5.	IP Interface for procr	12
5.6.	IP Network Region	13
5.7.	Signaling Group	14
5.8.	Trunk Group	16
5.9.	Inbound Routing	18
5.10.	Calling Party Information	19
5.11.	Outbound Routing	20
5.12.	Saving Communication Manager Configuration Changes	23
6.	Configure Avaya Aura® Session Manager	24
6.1.	Avaya Aura® System Manager Login and Navigation	24
6.2.	Specify SIP Domain	25
6.3.	Add Location	26
6.4.	Adaptations	30
6.5.	Add SIP Entities	32
6.6.	Add Entity Links	36
6.7.	Add Routing Policies	37
6.8.	Add Dial Patterns	38
6.9.	Verify Avaya Aura® Session Manager Instance	42
7.	Configure Avaya Session Border Controller for Enterprise	44
7.1.	Global Profiles	47
7.1.1.	Routing Profile	47
7.1.2.	Topology Hiding Profile	48
7.1.3.	Server Interworking Profile	52
7.1.4.	Signaling Manipulation	60
7.1.5.	Server Configuration	62
7.2.	Domain Policies	70
7.2.1.	Media Rules	70
7.2.2.	Signaling Rules	72
7.2.3.	Application Rules	74

7.2.4.	Endpoint Policy Group	75
7.3.	Device Specific Settings.....	77
7.3.1.	Network Management	77
7.3.2.	Signaling Interface.....	78
7.3.3.	Media Interface	79
7.3.4.	End Point Flows - Server Flow	80
8.	Windstream SIP Trunking Configuration	82
9.	Verification and Troubleshooting	83
9.1.	Verification	83
9.2.	Troubleshooting	84
10.	Conclusion.....	87
11.	References	87

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Windstream and Avaya Aura® Communication Manager Access Element 5.2.1, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5.

The Windstream SIP Trunking service referenced within these Application Notes is positioned for customers that have an IP-PBX or IP-based network equipment with SIP functionality, but need a form of IP transport and local services to complete their solution.

Windstream SIP Trunking will enable delivery of origination and termination of local, long-distance and toll-free traffic across a single broadband connection. A SIP signaling interface will be enabled to the Customer Premises Equipment (CPE).

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Communication Manager, Session 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 Trunking 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 APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

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).
- 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. H.323 was the only protocol tested.

- Various call types including: local, long distance, international, outbound toll-free, and local directory assistance (411).
- G.711MU codec.
- In-band DTMF.
- 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.
- Network Call Redirection using the SIP REFER method or a 302 response.
- Off-net call forwarding and mobility (extension to cellular).

Items not supported or not tested included the following:

- Inbound toll-free, operator assisted calls and emergency calls (911) are supported but were not tested as part of the compliance test.
- T.38 Fax not supported.

2.2. Test Results

Interoperability testing of Windstream SIP Trunking was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **T.38 Fax** – The use of T.38 Fax did not pass compliance testing. Windstream returns a “488 Not Acceptable Here” response to the SIP INVITE with T.38 parameters. Thus, the use of T.38 Fax is not recommended with this solution.
- **Outbound call to busy number** – When a call is placed to a PSTN number that is busy, the caller will hear a busy tone, but Windstream will not return a “486 Busy Here”, instead the call is answered with a “200 OK” response and a busy tone is played in the RTP stream.
- **Network Call Redirection using REFER with redirected party Busy** – In the testing environment, when an inbound call was made to the enterprise, to a vector redirecting the call to another PSTN endpoint that was busy, the caller will hear a busy tone, but Windstream will not return a “486 Busy Here”, preventing any additional processing of the call by Communication Manager, like the routing of the call to a local agent on the enterprise.
- **Network Call Redirection using REFER with transfer** – When Communication Manager is configured With the Network Call Redirection feature enabled and an extension receives a call from a PSTN number and attempts to transfer (either consultative or blind) the call to another PSTN extension, the transfer is successful but the REFER will fail. This causes the Communication Manager to stay connected to both calls for the duration of the call rather than releasing the calls back to the PSTN.
- **DTMF transmission using RFC 2833** – In the testing environment, DTMF transmission was successfully transmitted in-band using the G.711MU codec rather than in the RTP payload as specified in RFC 2833 (**Reference [19]**).

Windstream SIP Trunking passed compliance testing.

2.3. Support

For technical support on Windstream SIP Trunking, contact Windstream using the Customer Service links at www.windstream.com.

3. Reference Configuration

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

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

- Communication Manager
- Communication Manager Messaging
- Session Manager
- System Manager
- Avaya Session Border Controller for Enterprise
- Avaya G450 Media Gateway
- Avaya 9600-Series IP telephones (H.323)
- Avaya 1600-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.

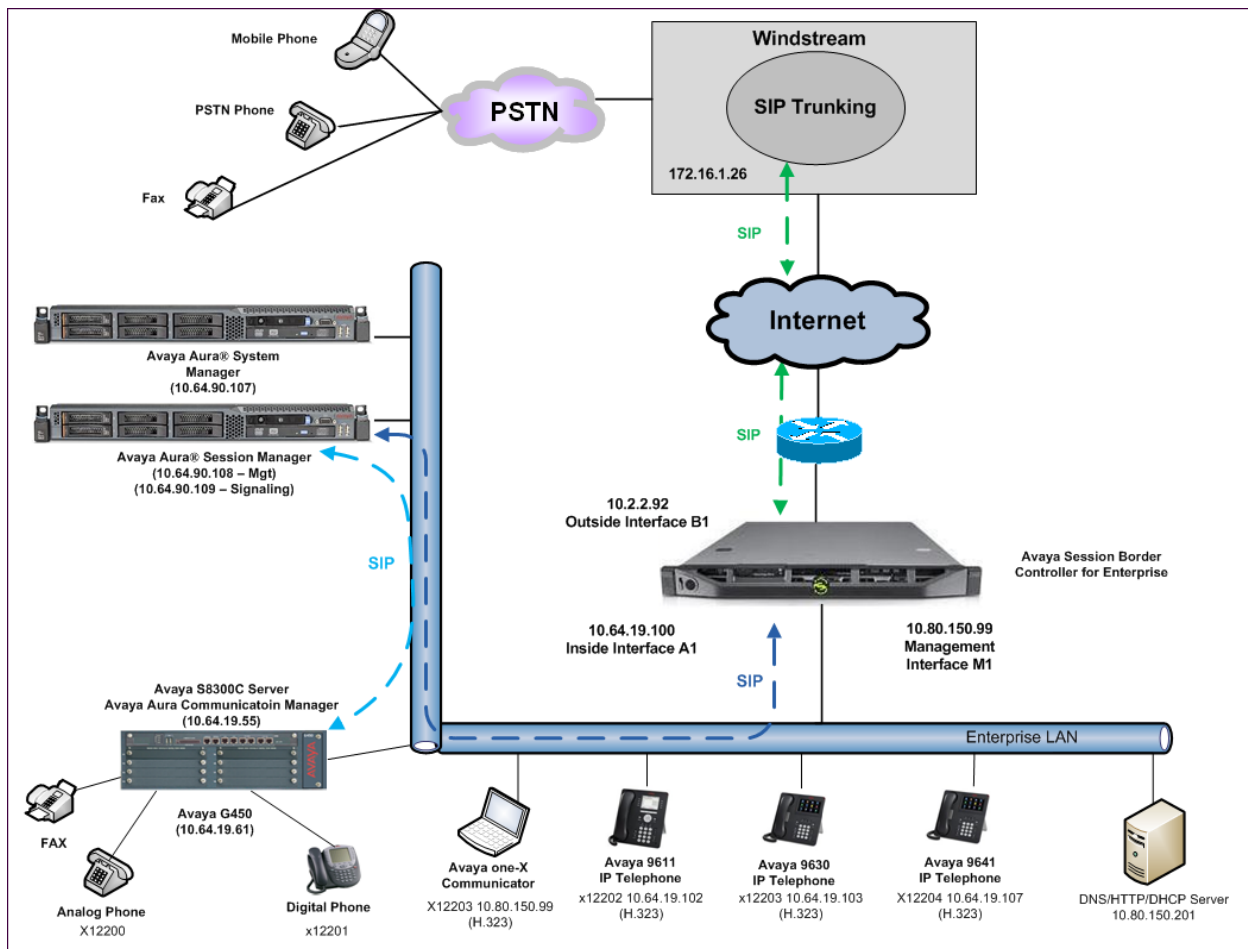


Figure 1: Avaya IP Telephony Network using the SIP Trunking service

A separate trunk was created between Communication Manager and Session Manager to carry the service provider traffic. This was done so that any trunk or codec setting required by the service provider could be applied only to this trunk and not affect other enterprise SIP traffic. In addition, this trunk carried both inbound and outbound traffic.

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

Outbound calls to the PSTN are first processed by Communication Manager and may be subject to outbound features such as automatic route selection, digit manipulation and class of service restrictions. Once Communication Manager selects the proper SIP trunk, the call is routed to Session Manager. Session Manager once again uses the configured dial patterns (or regular expressions) to determine the route to Avaya SBCE. From Avaya SBCE, the call is sent to the Windstream SIP Trunking service.

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	R015x.02.1.016.4 -18942
Avaya Aura® Communication Manager Messaging	R015x.02.1.016.4 A9021rfh C1317rff
Avaya Aura® System Manager	6.2.0.0.15669-6.2.12.9
Avaya Aura® Session Manager	6.2.0.0.620118
Avaya Session Border Controller for Enterprise	4.0.5.Q09
Avaya G450 Media Gateway	31.22.0
Avaya 1616 IP Telephone (H.323)	Avaya one-X® Deskphone Value Edition 1.301S
Avaya 9641 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.2009
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.104S
Avaya 9611 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.2009
Avaya 9608 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.0.3
Avaya one-X® Communicator	6.1.3.09
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Windstream SIP Trunking Solution Components	
Component	Release
Metaswitch	7.03.00 SU 56

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing.

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for the Windstream SIP Trunking service. A SIP trunk is established between Communication Manager and Session Manager for use by signaling traffic to and from Windstream. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager 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 shows that **450** SIP trunk licenses are available and **265** 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:		450	18	
Maximum Concurrently Registered IP Stations:		450	3	
Maximum Administered Remote Office Trunks:		0	0	
Maximum Concurrently Registered Remote Office Stations:		0	0	
Maximum Concurrently Registered IP eCons:		68	0	
Max Concur Registered Unauthenticated H.323 Stations:		450	0	
Maximum Video Capable Stations:		450	0	
Maximum Video Capable IP Softphones:		450	0	
Maximum Administered SIP Trunks:		450	265	
Maximum Administered Ad-hoc Video Conferencing Ports:		450	0	
Maximum Number of DS1 Boards with Echo Cancellation:		80	0	
Maximum TN2501 VAL Boards:		0	0	
Maximum Media Gateway VAL Sources:		50	1	
Maximum TN2602 Boards with 80 VoIP Channels:		0	0	
Maximum TN2602 Boards with 320 VoIP Channels:		0	0	
Maximum Number of Expanded Meet-me Conference Ports:		300	0	

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 features                               Page 1 of 18
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

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.

```
change system-parameters features                               Page 9 of 18
      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 that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and for Session Manager (**SM62**). 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	
CMM	10.64.19.56	
SM62	10.64.90.109	
default	0.0.0.0	
procr	10.64.19.55	

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. In the example below, **G.711MU** 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 Codec	Silence Suppression	Frames Per Pkt
1: G.711MU	n	2
2:		
3:		

Since T.38 fax is not supported, set the **Fax Mode** to **off** on **Page 2**.

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

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 PE 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 procr		Page 1 of 1
IP INTERFACES		
Type: PROCR	Target socket load: 1700	
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
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 the rest of the enterprise. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

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

```
change ip-network-region 2                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 2
Location: 1           Authoritative Domain: avayalab.com
Name: SIP TRUNK
MEDIA PARAMETERS
  Codec Set: 2
  UDP Port Min: 2048
  UDP Port Max: 3329
  Intra-region IP-IP Direct Audio: yes
  Inter-region IP-IP Direct Audio: yes
  IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
  Audio 802.1p Priority: 6
  Video 802.1p Priority: 5
  AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
  RSVP Enabled? n
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and region 1 (the rest of the enterprise). 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).

change ip-network-region 2										Page	4 of	20
Source Region: 2 Inter Network Region Connection Management										I		M
										G	A	t
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c			
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e		
1	2	y	NoLimit					n		t		
2	2											
3												
4												

5.7. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager 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 1 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 Access Element Server for Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port. For ease of troubleshooting, the compliance test was conducted with the **Transport Method** set to **tcp** and the **Near-end Listen Port** and **Far-end Listen Port** set to **5060**.
- Set the **Peer Detection Enabled** field to **y**. The **Peer Server** field will initially be set to **Others** and cannot be changed via administration. The Peer Server field will automatically change to **SM** once Communication Manager detected a Session Manager peer.
- 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 **SM**. This node name maps to the IP address of Session Manager 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 **in-band**. This value sends the DTMF digits in the RTP audio stream.
- Default values may be used for all other fields.

add signaling-group 1		Page 1 of 1
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
IP Video? n		
Near-end Node Name: procr	Far-end Node Name: SM62	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 2	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: in-band	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 6	

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 1 was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an appropriate Class of Restriction (COR) designated for SIP Trunks in the **COR** field.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Service Type** field to **public-ntwrk**.
- Set 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 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1          Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SP      COR: 10      TN: 1      TAC: *101
    Direction: two-way      Outgoing Display? n
    Dial Access? n
    Queue Length: 0
  Service Type: public-ntwrk      Auth Code? n
                                     Signaling Group: 1
                                     Number 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 1                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
  SCCAN? n                                     Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 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.

add trunk-group 1		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public	UI Treatment: service-provider	
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		

On **Page 4**, set the **Network Call Redirection** field to **y**. This allows inbound calls transferred back to the PSTN to use the SIP REFER method, see **Reference [18]**. Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is 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**. Default values may be used for all other fields

```

add trunk-group 1
                                Page 4 of 21

                                PROTOCOL VARIATIONS

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

```

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. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Windstream is unchanged by Session Manager, then 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** command to create an entry for each DID. As an example, the following screen illustrates a conversion of DID number **5015551490** to extension **19000**. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were tested successfully.

```

change inc-call-handling-trmt trunk-group 1
                                Page 1 of 30

                                INCOMING CALL HANDLING TREATMENT

Service/      Number   Number   Del Insert
Feature       Len      Digits
public-ntwrk  10  5015551490    10  19000
public-ntwrk

```

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 used to authenticate the caller.

In the bolded rows shown in the example abridged output below, Communication Manager extensions are mapped to DID numbers that are known to Windstream for this SIP Trunk connection when the call uses trunk group 1.

change public-unknown-numbering 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	12200	1	5015551070	10	Total Administered: 6
5	12201	1	5015551071	10	Maximum Entries: 240
5	12202	1	5015551072	10	
5	12203	1	5015551073	10	
5	12204	1	5015551074	10	
5	12205	1	5015551075	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**).

change dialplan analysis							Page 1 of 12		
DIAL PLAN ANALYSIS TABLE									
Location: all							Percent Full: 0		
	Dialed String	Total Length	Call Type		Dialed String	Total Length	Call Type		Dialed String
	1	5	ext						
	2	5	ext						
	4	4	ext						
	5	4	ext						
	6	5	ext						
	7	4	ext						
	8	1	fac						
	9	1	fac						
	*	4	dac						
	#	4	fac						

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 9	
FEATURE ACCESS CODE (FAC)			
Abbreviated Dialing List1 Access Code: #110			
Abbreviated Dialing List2 Access Code: #111			
Abbreviated Dialing List3 Access Code: #112			
Abbreviated Dial - Prgm Group List Access Code: #113			
Announcement Access Code: #114			
Answer Back Access Code:			
Attendant Access Code:			
Auto Alternate Routing (AAR) Access Code: 8			
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:	
Automatic Callback Activation:		Deactivation:	
Call Forwarding Activation Busy/DA: #002 All:		Deactivation: #004	
Call Forwarding Enhanced Status: Act:		Deactivation:	

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** Error! Reference source not found. 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
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
12	11	11	1	fnpa		n	
13	11	11	1	fnpa		n	
14	11	11	1	fnpa		n	
15	11	11	1	fnpa		n	
16	11	11	1	fnpa		n	
17	11	11	1	fnpa		n	
18	11	11	1	fnpa		n	
19	11	11	1	fnpa		n	
303	10	10	1	hnpa		n	
411	3	3	1	svcl		n	
501	10	10	1	hnpa		n	
720	10	10	1	hnpa		n	
911	3	3	1	emer		n	

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 **1** 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: 1** 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.

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

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 Windstream being converted to 5 digit extensions.

change ars digit-conversion 0					Page 1 of 2			
ARS DIGIT CONVERSION TABLE					Percent Full: 0			
Location: all								
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	ANI	Req
5015551071	10	10	10	12201	ext	y	n	
5015551070	10	10	10	12200	ext	y	n	
5015551072	10	10	10	12202	ext	y	n	
5015551073	10	10	10	12203	ext	y	n	
5015551074	10	10	10	12204	ext	y	n	
5015551075	10	10	10	12205	ext	y	n	
							n	
							n	
							n	
							n	
							n	
							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 Aura® Session Manager

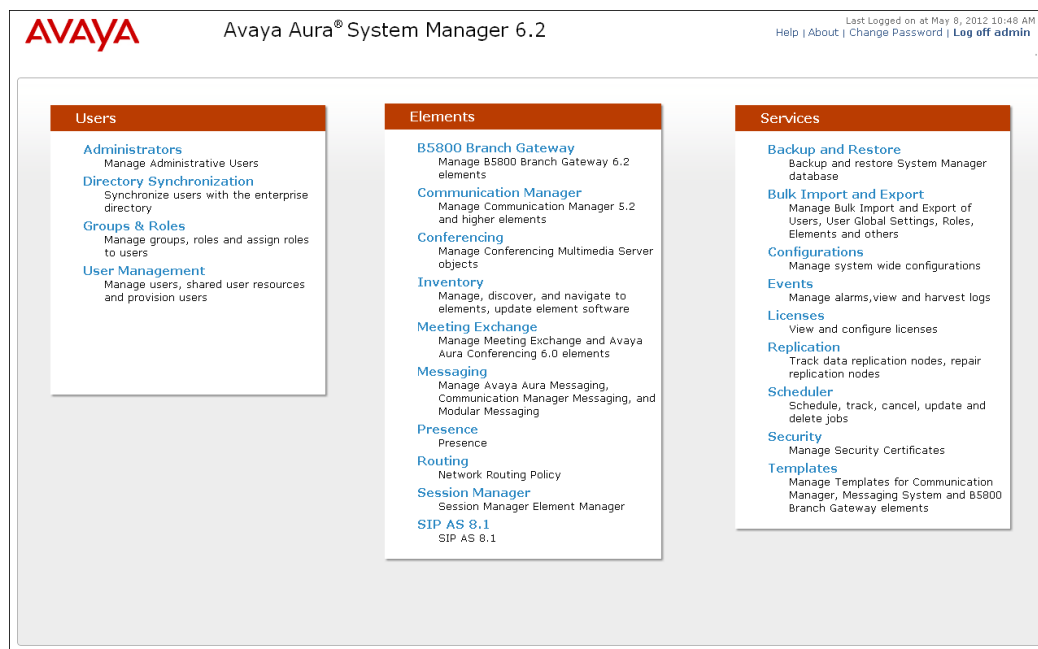
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager Instance, corresponding to the Session Manager server to be administered in System Manager.

It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL <https://<ip-address>/SMGR>, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed.



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at May 8, 2012 10:48 AM
Help | About | Change Password | Log off admin

Routing Home / Elements / Routing Help ?

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"

6.2. Specify SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain (**avayalab.com**). Navigate to **Routing → Domains** and click the **New** button in the right pane (not shown). In the new right pane that appears, fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the **avayalab.com** domain.

Home / Elements / Routing / Domains Help ?

Domain Management

Commit **Cancel**

Warning: SIP Domain name change will cause login failure for Communication Address handles with this domain. Consult release notes or Support for steps to reset login credentials.

1 Item | Refresh Filter: Enable

Name	Type	Default	Notes
* avayalab.com	sip	<input type="checkbox"/>	

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The **Location Pattern** was not populated. The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In this sample configuration Locations are added to SIP Entities (**Section 6.5**), so it was not necessary to add a pattern.

The following screen shows the addition of **Location_1**, this location will be used for Session Manager. Click **Commit** to save.

Home / Elements / Routing / Locations

Help ?

Location Details

Commit Cancel

General

* Name:

Location_1

Notes:

Location 1 SM

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

* Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Note: Call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for Communication Manager and Avaya SBCE. Displayed below is the screen for **CM521** used for Communication Manager.

[Home](#) / [Elements](#) / [Routing](#) / [Locations](#)

Location DetailsCommit

General

*

Name:

CM521

Notes:

CM 5.2.1.

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

* Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Below is the screen for **AvayaSBCE** used for Avaya SBCE.

[Home](#) / [Elements](#) / [Routing](#) / [Locations](#)

Location DetailsCommit

General

*** Name:**

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

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

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

*** Minimum Multimedia Bandwidth:** **Kbit/Sec**

*** Default Audio Bandwidth:**

6.4. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

The following screen shows the adaptation that was available in the sample configuration.

The screenshot shows the 'Adaptations' page in a web-based configuration tool. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Adaptations'. On the right, there is a 'Help ?' link. Below the title 'Adaptations', there are buttons for 'Edit', 'New', 'Duplicate', 'Delete', and a 'More Actions' dropdown menu. A table below these buttons shows a list of adaptations. The table has columns for 'Name', 'Module name', 'Egress URI Parameters', and 'Notes'. There is one item listed: 'CM521_Adaptation' with module name 'DigitConversionAdapter' and notes 'Digit Conversion to CM 5.2.1'. Above the table, it says '1 Item' and 'Refresh'. To the right of the table, it says 'Filter: Enable'. Below the table, there is a 'Select : All, None' option.

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	CM521_Adaptation	DigitConversionAdapter		Digit Conversion to CM 5.2.1

The adapter named **CM521 Adaptation** will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Windstream SIP Trunking. This adaptation uses the **DigitConversionAdapter** to convert digits between Communication Manager and Windstream.

The screenshot shows the 'Adaptation Details' page in the same configuration tool. The breadcrumb navigation is 'Home / Elements / Routing / Adaptations'. On the right, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The page title is 'Adaptation Details'. Below the title, there is a 'General' section. The form contains the following fields: 'Adaptation name' (required, with an asterisk) with the value 'CM521 Adaptation'; 'Module name' with a dropdown menu showing 'DigitConversionAdapter'; 'Module parameter' (empty); 'Egress URI Parameters' (empty); and 'Notes' with the value 'Digit Conversion to CM 5.2.1'.

Scrolling down, the following screen shows a portion of the **CM521 Adaptation** adapter that can be used to convert digits between the Communication Manager extension numbers (user extensions, VDNs) and the DID numbers assigned by Windstream.

An example portion of the settings for **Digit Conversion for Outgoing Calls from SM** (i.e., inbound to Communication Manager) is shown below.

Digit Conversion for Outgoing Calls from SM

Add
Remove

6 Items
Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern ^	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	* 5015551070	* 10	* 10		* 10	12200	both		
<input type="checkbox"/>	* 5015551071	* 10	* 10		* 10	12201	both		
<input type="checkbox"/>	* 5015551072	* 10	* 10		* 10	12002	both		
<input type="checkbox"/>	* 5015551073	* 10	* 10		* 10	12003	both		
<input type="checkbox"/>	* 5015551074	* 10	* 10		* 10	12004	both		
<input type="checkbox"/>	* 5015551075	* 10	* 10		* 10	12005	both		

Select : All, None

* Input Required
Commit
Cancel

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Communication Manager and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Enter **Session Manager** for Session Manager, **CM** for Communication Manager and **SIP Trunk** for Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** that will be applied to this entity.
- **Location:** Select one of the locations defined previously.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

Home / Elements / Routing / SIP Entities

[Help ?](#)

SIP Entity Details [Commit](#) [Cancel](#)

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. This section defines a default set of ports that Session Manager will use to listen for SIP requests, typically from registered SIP endpoints. Session Manager can also listen on additional ports defined elsewhere such as the ports specified in the SIP Entity Link definition in **Section 6.6**.

In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

Defaults can be used for the remaining fields. Click **Commit** to save.

For the compliance test, two **Port** entries were added.

Port

TCP Failover port:

TLS Failover port:

2 Items | [Refresh](#) Filter: [Enable](#)

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

Select : All, None

The following screen shows the addition of Communication Manager. The **FQDN or IP Address** field is set to the IP address defined in **Section 5.3** of the procr interface on Communication Manager. The **Adaptation** field is set to the Adaptation created in **Section 6.4** and the Location is set to the one defined for Communication Manager in **Section 6.3**.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb trail at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details'. In the top right corner, there are 'Help ?', 'Commit', and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

- Name:** CM521
- FQDN or IP Address:** 10.64.19.55
- Type:** CM
- Notes:** CM 5.2.1
- Adaptation:** CM521 Adaptation
- Location:** CM521
- Time Zone:** America/Fortaleza
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty field)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration
- Supports Call Admission Control:** ☐
- Shared Bandwidth Manager:** ☐
- Primary Session Manager Bandwidth Association:** (empty dropdown)
- Backup Session Manager Bandwidth Association:** (empty dropdown)

The following screen shows the addition of **ASBCE** SIP Entity. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). The Location is set to the one defined for Avaya SBCE in **Section 6.3**. **Link Monitoring Enabled** was selected for **SIP Link Monitoring** using the specific time settings for **Proactive Monitoring Interval (in seconds)** and **Reactive Monitoring Interval (in seconds)** for the compliance test. These time settings should be adjusted or left at their default values per customer needs and requirements.

The screenshot shows a web-based configuration interface for SIP Entities. The breadcrumb navigation at the top reads 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details', and there are 'Commit' and 'Cancel' buttons in the top right corner. The 'General' section contains the following fields: 'Name' (ASBCE), 'FQDN or IP Address' (10.64.19.100), 'Type' (SIP Trunk), 'Notes' (Avaya SBC), 'Adaptation' (empty dropdown), 'Location' (AvayaSBCE), 'Time Zone' (America/Denver), 'Override Port & Transport with DNS SRV' (checkbox), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty text field), and 'Call Detail Recording' (egress). The 'SIP Link Monitoring' section includes: 'SIP Link Monitoring' (Link Monitoring Enabled), 'Proactive Monitoring Interval (in seconds)' (900), 'Reactive Monitoring Interval (in seconds)' (120), 'Number of Retries' (3), 'Supports Call Admission Control' (checkbox), 'Shared Bandwidth Manager' (checkbox), 'Primary Session Manager Bandwidth Association' (empty dropdown), and 'Backup Session Manager Bandwidth Association' (empty dropdown).

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

General

* Name: ASBCE

* FQDN or IP Address: 10.64.19.100

Type: SIP Trunk

Notes: Avaya SBC

Adaptation:

Location: AvayaSBCE

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: egress

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 3

Supports Call Admission Control: ☐

Shared Bandwidth Manager: ☐

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described as an Entity Link. Two Entity Links were created; one to Communication Manager for use only by service provider traffic and one to Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the SIP Entity for Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic would not be encrypted.

Entity Link to Communication Manager:

Home / Elements / Routing / Entity Links

Entity Links Help ? Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM62_CM521_5060	* ASM62	TCP	* 5060	* CM521	* 5060	Trusted	

Entity Link to Avaya SBCE:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* ASM62_ASBCE_5060	* ASM62	TCP	* 5060	* ASBCE	* 5060	Trusted	

6.7. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies must be added; one for Communication Manager and one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). The screen below is displayed. Fill in the following:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP entity to which this routing policy applies and click **Select** (not shown). The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager and Avaya SBCE.

Home / Elements / Routing / Routing Policies

Routing Policy Details Help ? Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM521	10.64.19.55	CM	CM 5.2.1

Home / Elements / Routing / Routing Policies

Routing Policy Details Help ? Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

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

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Manager to Windstream and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

In the **General** section, enter the following values. Use default values for all remaining fields:

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that 11 digit dialed numbers that begin with 1 originating from **CM521** uses route policy **To-ASBCE**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

[Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

2 Items | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CM521	CM 5.2.1.	To-ASBCE	0	<input type="checkbox"/>	ASBCE	To Avaya SBC
<input type="checkbox"/>	Location_1	Location 1 SM	To-ASBCE	0	<input type="checkbox"/>	ASBCE	To Avaya SBC

Select : All, None

The second example shows that a **10** digit number starting with **501555107** to domain **avayalab.com** and originating from **AvayaSBCE** uses route policy **To-CM521**. This is a DID range 501-555-1070 through 501-555-1079 assigned to the enterprise from Windstream.

Home / Elements / Routing / Dial Patterns

[Help ?](#)

Dial Pattern Details

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	AvayaSBCE	Avaya SBC	To-CM521	0	<input type="checkbox"/>	CM521	

Select : All, None

The complete list of dial patterns defined for the compliance test is shown below.

Home / Elements / Routing / Dial Patterns								
Dial Patterns								Help ?
<a>Edit <a>New <a>Duplicate <a>Delete <a>More Actions								
10 Items <a>Refresh								Filter: <a>Enable
<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	<a>0	1	28	<input type="checkbox"/>			avayalab.com	0 + Outbound Including 011
<input type="checkbox"/>	<a>1	11	11	<input type="checkbox"/>			avayalab.com	1 + Outbound
<input type="checkbox"/>	<a>122	5	5	<input type="checkbox"/>			avayalab.com	CM 5.2.1 Extensions 12200 - 12299
<input type="checkbox"/>	<a>123	5	5	<input type="checkbox"/>			avayalab.com	CM 5.2.1 Extensions 12300 - 12399
<input type="checkbox"/>	<a>303	10	10	<input type="checkbox"/>			avayalab.com	10 Digit Dialing to area code 303
<input type="checkbox"/>	<a>411	3	3	<input type="checkbox"/>			avayalab.com	Information
<input type="checkbox"/>	<a>501	10	10	<input type="checkbox"/>			avayalab.com	10 Digit Dialing to area code 501
<input type="checkbox"/>	<a>501555107	10	10	<input type="checkbox"/>			avayalab.com	DID's to CM5.2.1
<input type="checkbox"/>	<a>501555149	10	10	<input type="checkbox"/>			avayalab.com	DID's to CM5.2.1
<input type="checkbox"/>	<a>720	10	10	<input type="checkbox"/>			avayalab.com	10 Digit Dialing to area code 720
Select : <a>All , <a>None								

6.9. Add Avaya Aura® Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager instance already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the screen below:

In the **General** section, enter the following values:

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

The screen below shows the Session Manager values used for the compliance test.

Home / Elements / Session Manager [Help ?](#)

Edit Session Manager

[Commit](#) [Cancel](#)

[General](#) | [Security Module](#) | [NIC Bonding](#) | [Monitoring](#) | [CDR](#) | [Personal Profile Manager \(PPM\)](#) - [Connection Settings](#) | [Event Server](#) | [Expand All](#) | [Collapse All](#)

[General](#) ▼

SIP Entity Name ASM62

Description

***Management Access Point Host Name/IP**

***Direct Routing to Endpoints**

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.

Security Module ▾

SIP Entity IP Address

10.64.90.109

*Network Mask

255.255.255.0

*Default Gateway

10.64.90.1

*Call Control PHB

46

*QOS Priority

6

*Speed & Duplex

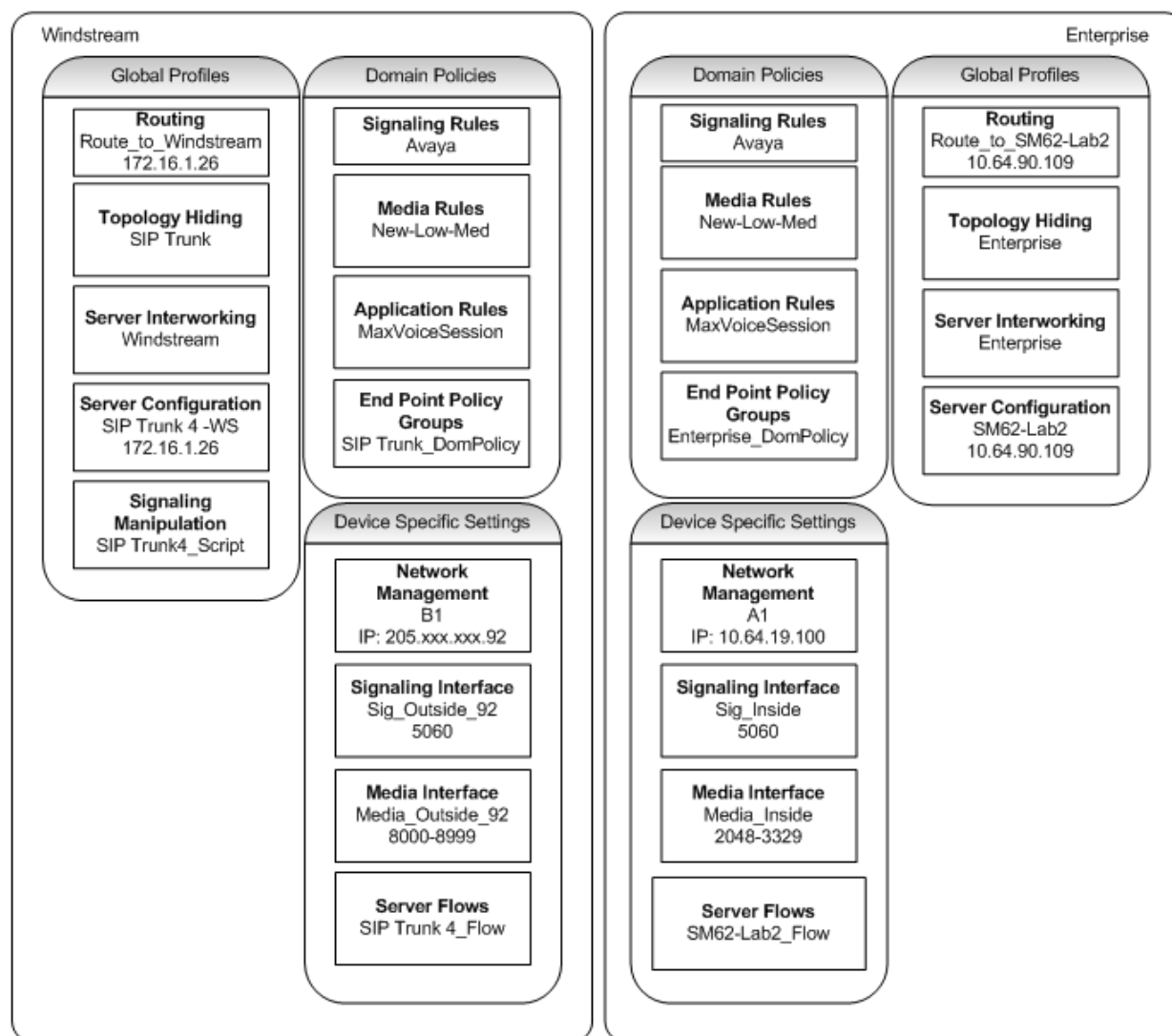
Auto ▾

VLAN ID

7. Configure Avaya Session Border Controller for Enterprise

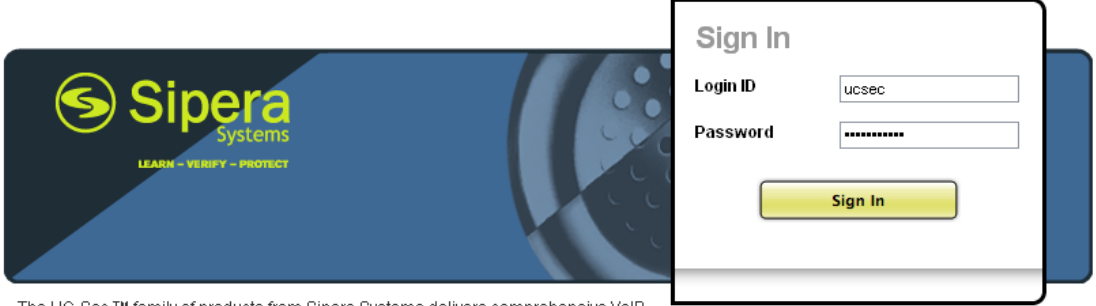
This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference** [15] and [16].

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.



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

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

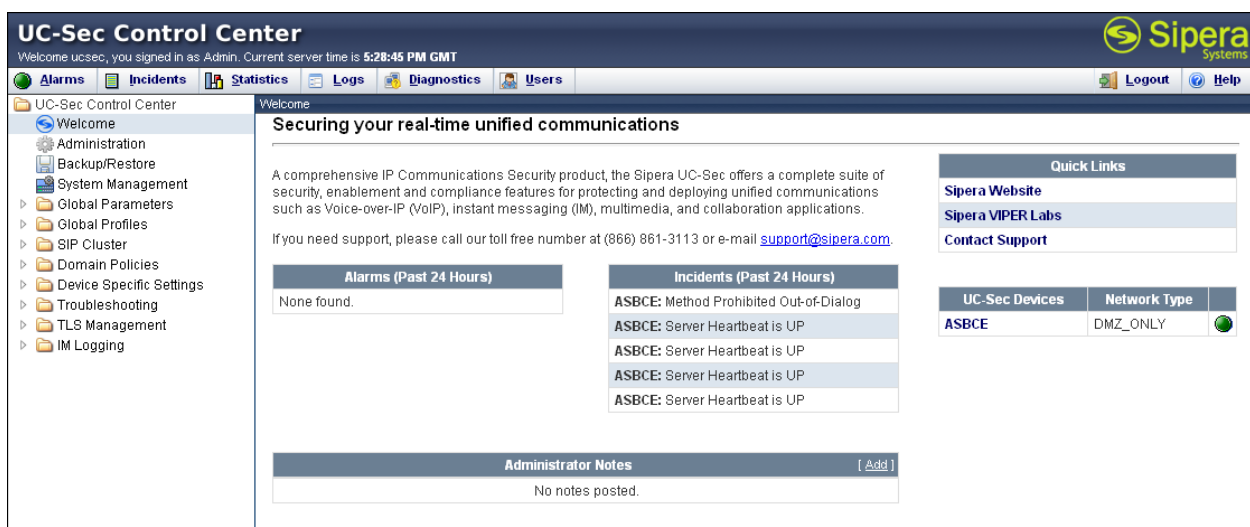


The UC-Sec™ family of products from Siper Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

[Visit the Siper Systems website to learn more.](#)

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

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



UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 5:28:45 PM GMT

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

UC-Sec Control Center

Welcome

Securing your real-time unified communications

A comprehensive IP Communications Security product, the Siper UC-Sec offers a complete suite of security, enablement and compliance features for protecting and deploying unified communications such as Voice-over-IP (VoIP), instant messaging (IM), multimedia, and collaboration applications.

If you need support, please call our toll free number at (866) 861-3113 or e-mail support@sipera.com.

Alarms (Past 24 Hours)
None found.

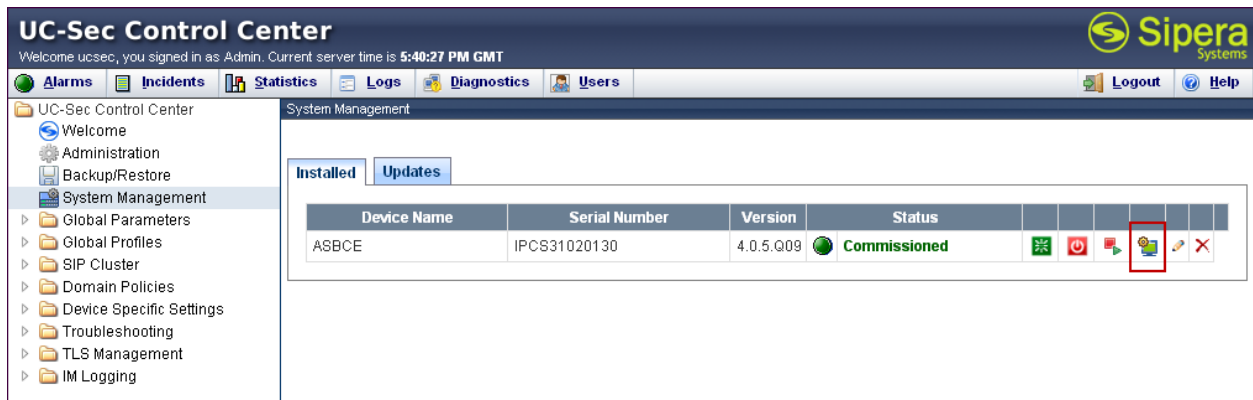
Incidents (Past 24 Hours)
ASBCE: Method Prohibited Out-of-Dialog
ASBCE: Server Heartbeat is UP
ASBCE: Server Heartbeat is UP
ASBCE: Server Heartbeat is UP
ASBCE: Server Heartbeat is UP

Administrator Notes [Add]
No notes posted.

Quick Links
[Sipera Website](#)
[Sipera VIPER Labs](#)
[Contact Support](#)

UC-Sec Devices	Network Type	
ASBCE	DMZ_ONLY	

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



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.

The screenshot displays the 'System Information: ASBCE' window. It contains several sections for configuring the device ASBCE:

- Network Configuration**
 - General Settings**

Appliance Name	ASBCE
Box Type	SIP
Deployment Mode	Proxy
 - Device Settings**

HA Mode	No
Secure Channel Mode	None
Two Bypass Mode	No
- Network Settings**

IP	Public IP	Netmask	Gateway	Interface
205.100.100.92	205.100.100.92	255.255.255.128	205.100.100.1	B1
10.64.19.100	10.64.19.100	255.255.255.0	10.64.19.1	A1
- DNS Configuration**

Primary DNS	10.80.150.201
Secondary DNS	
DNS Location	DMZ
- Management IP(s)**

IP	10.80.150.99
----	--------------

7.1. Global Profiles

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

7.1.1. 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 a Routing Profile for Session Manager and Windstream SIP Trunk. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue (not shown).

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.
- **Use Next Hop for In-Dialog Messages:** Select only if there is no secondary Next Hop server.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish** (not shown).

The following screen shows the Routing Profile to Communication Manager. The **Next Hop Server 1** IP address must match the IP address of the Session Manager Security Module in **Section 6.9**. The Outgoing Transport and port number must match the Avaya SBCE Entity Link created on Session Manager in **Section 6.6**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, Global Parameters, Global Profiles, and Routing. The 'Routing' category is selected. The main area displays the 'Routing Profiles' list on the left, with 'To-SM62-Lab2' highlighted. On the right, the 'Routing Profile' configuration page is shown. It includes buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. A yellow banner says 'Click here to add a description.' Below this is a table for 'Routing Rule' with columns: Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. The table contains one rule with Priority 1, URI Group *, Next Hop Server 1 10.64.90.109, Next Hop Server 2 ---, Next Hop Priority checked, and Outgoing Transport TCP.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.64.90.109	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The following screen shows the Routing Profile to Windstream. In the **Next Hop Server 1** field enter the IP address and port number that Windstream uses to listen for SIP traffic.

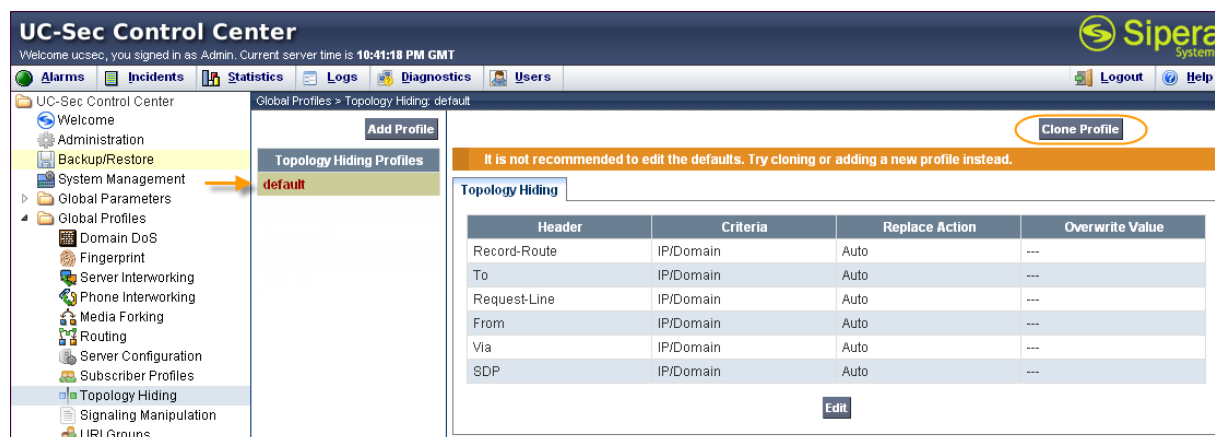
The screenshot shows the UC-Sec Control Center interface. The left sidebar is the same as the previous screenshot. The 'Routing' category is selected. The main area displays the 'Routing Profiles' list on the left, with 'Route_to_Windstream' highlighted. On the right, the 'Routing Profile' configuration page is shown. It includes buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. A yellow banner says 'Click here to add a description.' Below this is a table for 'Routing Rule' with columns: Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. The table contains one rule with Priority 1, URI Group *, Next Hop Server 1 172.16.1.26, Next Hop Server 2 ---, Next Hop Priority checked, and Outgoing Transport UDP.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	172.16.1.26	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

7.1.2. Topology Hiding Profile

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

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



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

Clone Profile

Profile Name
default

Clone Name

Finish

Edit the **Enterprise** profile to overwrite the **To**, **Request-Line** and **From** headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in Session Manager (**Section 6.2**) and the Communication Manager signaling group Far-end Domain (**Section 5.7**). Click **Finish** to save the changes.

Edit Topology Hiding Profile ✕

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

Finish

It is not necessary to modify the **SIP Trunk** profile from the default values. The following screen shows the Topology Hiding Policy created for Windstream.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 5:54:30 PM GMT

Alarms
Incidents
Statistics
Logs
Diagnostics
Users

Logout
Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
 - Domain DoS
 - Fingerprint
 - Server Interworking
 - Phone Interworking
 - Media Forking
 - Routing
 - Server Configuration
 - Subscriber Profiles
 - Topology Hiding**
 - Signaling Manipulation
 - URI Groups
- SIP Cluster
- Domain Policies
- Device Specific Settings

Global Profiles > Topology Hiding: SIP Trunk

Add Profile
Rename Profile
Clone Profile
Delete Profile

Topology Hiding Profiles

default
cisco_th_profile
SIP Trunk
Enterprise

Click here to add a description.

Topology Hiding

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

Edit

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	
Destination Headers	
To	(1) ReferTo
Request-Line	
SDP Headers	
Origin Header	

Table 2: Topology Hiding Headers

7.1.3. 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, or new profiles can be configured as described below.

In the sample configuration, separate Server Interworking Profiles were created for **Enterprise** and **Windstream**.

7.1.3.1 Server Interworking Profile – Enterprise

To create a new Server Interworking Profile for the enterprise, navigate to **UC-Sec Control Center → Global Profiles → 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

In the new window that appears, default values can be used. Click **Next** to continue.

Interworking Profile

General

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

Back

Next

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

Interworking Profile	
Privacy	
Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
Back Next	

Interworking Profile	
Configuration is not required. All fields are optional.	
SIP Timers	
Min-SE	<input type="text"/> seconds, [90 - 86400]
Init Timer	<input type="text"/> milliseconds, [50 - 1000]
Max Timer	<input type="text"/> milliseconds, [200 - 8000]
Trans Expire	<input type="text"/> seconds, [1 - 64]
Invite Expire	<input type="text"/> seconds, [180 - 300]
Transport Timers	
TCP Connection Inactive Timer	<input type="text"/> seconds, [600 - 3600]
Back Next	

On the **Advanced Settings** window uncheck the following default settings:

- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**

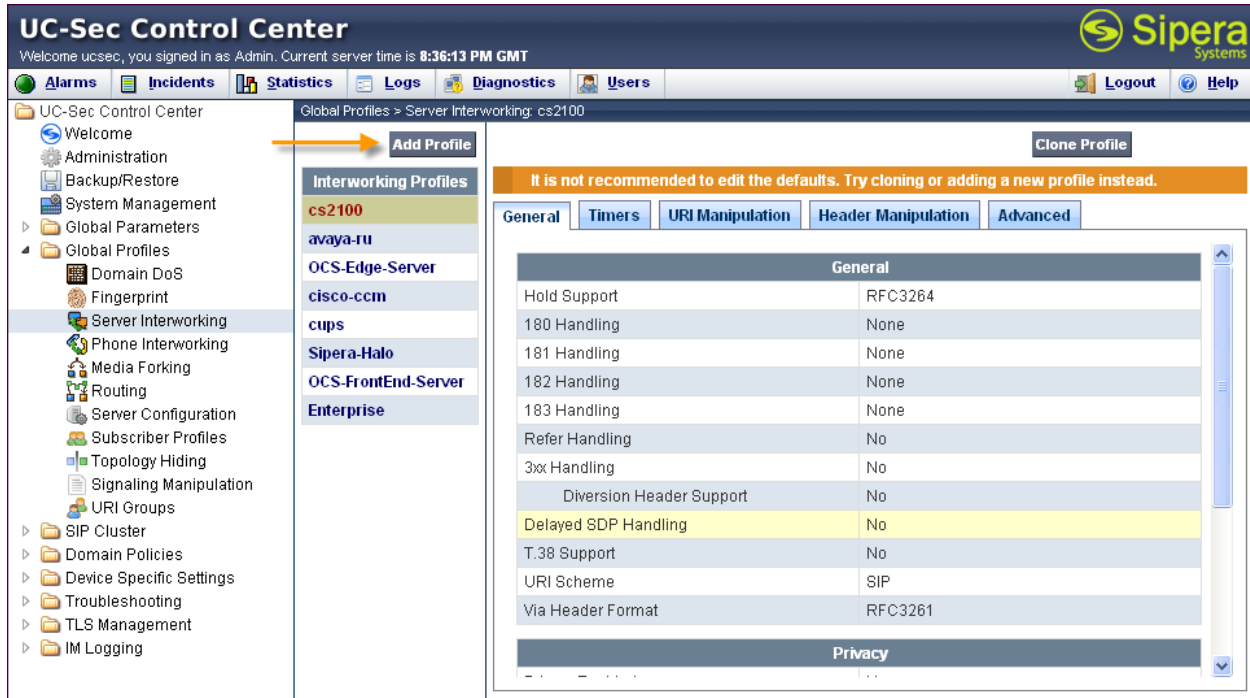
Click **Finish** to save changes.

Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLiC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Back **Finish**

7.1.3.2 Server Interworking Profile – Windstream

To create a new Server Interworking Profile for Windstream, navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Interworking** and click on **Add Profile** as shown below.



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

The screenshot shows a dialog box titled 'Interworking Profile'. It has a 'Profile Name' label and a text input field containing the text 'Windstream'. Below the input field is a 'Next' button.

In the new window that appears, default values can be used. Click **Next** to continue.

Interworking Profile

General

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

Back

Next

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

Interworking Profile

Privacy

Privacy Enabled	<input type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF

DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO
--------------	---

Back

Next

Interworking Profile

Configuration is not required. All fields are optional.

SIP Timers

Min-SE	<input type="text"/>	seconds, [90 - 86400]
Init Timer	<input type="text"/>	milliseconds, [50 - 1000]
Max Timer	<input type="text"/>	milliseconds, [200 - 8000]
Trans Expire	<input type="text"/>	seconds, [1 - 64]
Invite Expire	<input type="text"/>	seconds, [180 - 300]

Transport Timers

TCP Connection Inactive Timer	<input type="text"/>	seconds, [600 - 3600]
-------------------------------	----------------------	-----------------------

Back

Next

On the **Advanced Settings** window uncheck the following default settings:

- **Topology Hiding: Change Call-ID**
- **Change Max Forwards**

Click **Finish** to save changes.

Interworking Profile	
Advanced Settings	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
SLiC Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Back **Finish**

7.1.4. 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 add 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”.

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 and to remove unwanted headers in the SIP messages to Windstream. To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script** (not shown). A new blank SigMa Editor window will pop up. For more information on Signaling Manipulation see **Reference [16]**.

The following sample script begins with a comment describing what will take place in the script. The script will act on all outbound traffic to Windstream after the SIP message has been routed through the Avaya SBCE. The script is further broken down as follows:

- **within session “All”** Transformations applied to all SIP sessions.
- **act on message** Actions to be taken to any SIP message.
- **%DIRECTION=“OUTBOUND”** Applied to a message leaving the Avaya SBCE.
- **%ENTRY_POINT=“POST_ROUTING”** The “hook point” to apply the script after the SIP message has routed through the 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 1st instance of the header in a message.
- **.regex_replace(“avayalab\.com”, “205.xxx.xxx.92:5060”);** An action to replace a given match with the provide string (e.g., find “avayalab.com” and replace it with the external interface IP address and port). The backslash is used to escape the special meaning of “.” in a Regular Expression.

With this script, the P-Location and Alert-Info headers will be removed. The P-Asserted-Identity header will be modified by replacing the domain “avayalab.com” with the external IP address of Avaya SBCE and the SIP port of 5060.

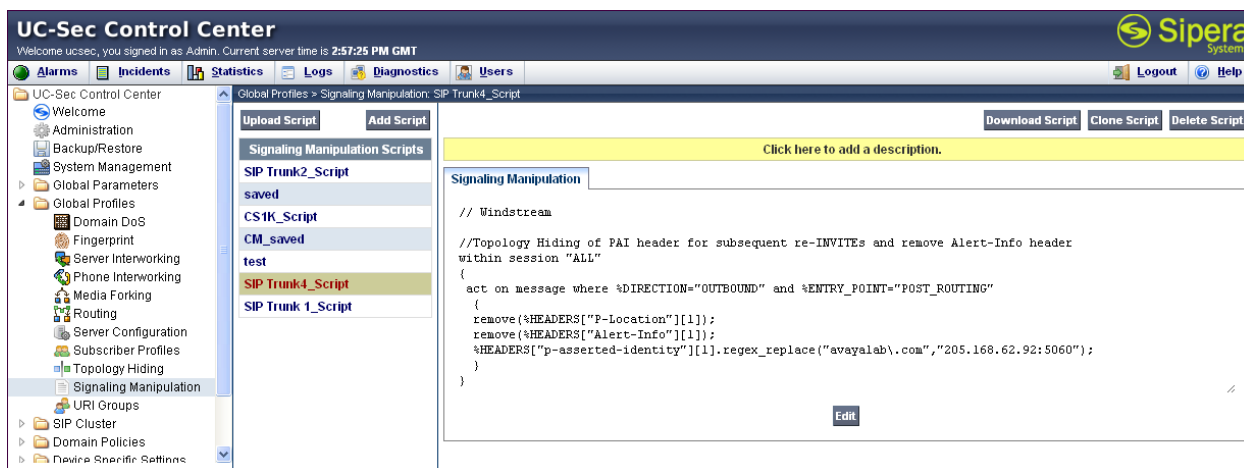


```

1 // Windstream
2
3 //Topology Hiding of PAI header for subsequent re-INVITES and remove Alert-Info header
4 within session "ALL"
5 {
6   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
7   {
8     remove(%HEADERS["P-Location"][1]);
9     remove(%HEADERS["Alert-Info"][1]);
10    %HEADERS["p-asserted-identity"][1].regex_replace("avayalab\.com","205.168.62.92:5060");
11  }
12 }
13
14

```

The following screen shows the finished Signaling Manipulation Script **SIP Trunk4_Script**.



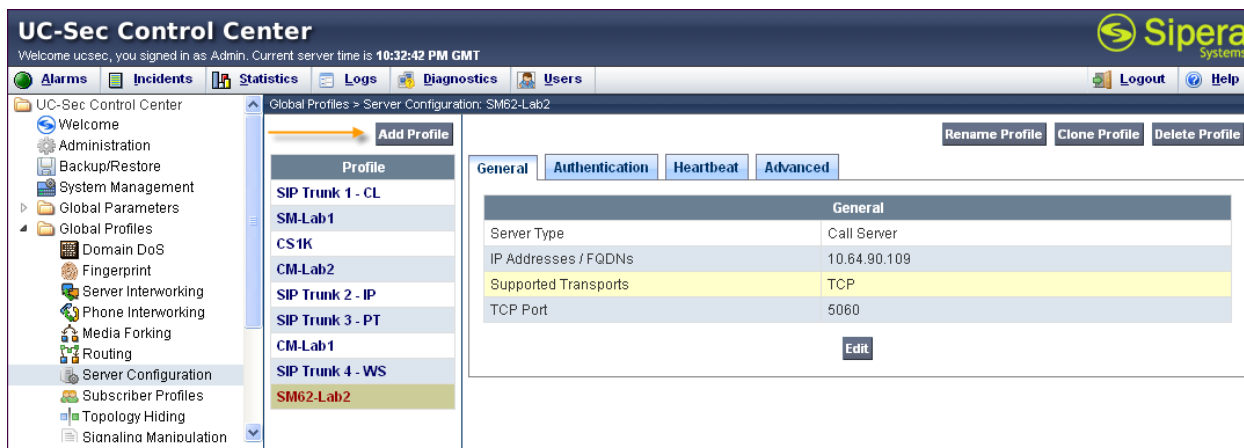
7.1.5. Server Configuration

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.

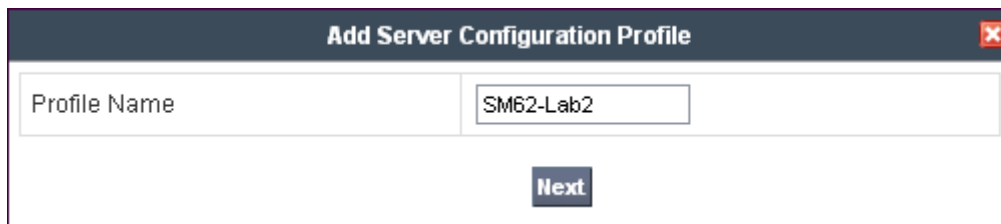
In the sample configuration, separate Server Configurations were created for Session Manager and Windstream.

7.1.5.1 Server Configuration – Session Manager

To add a Server Configuration Profile for Session Manager navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Configuration** and click on **Add Profile** as shown below.



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

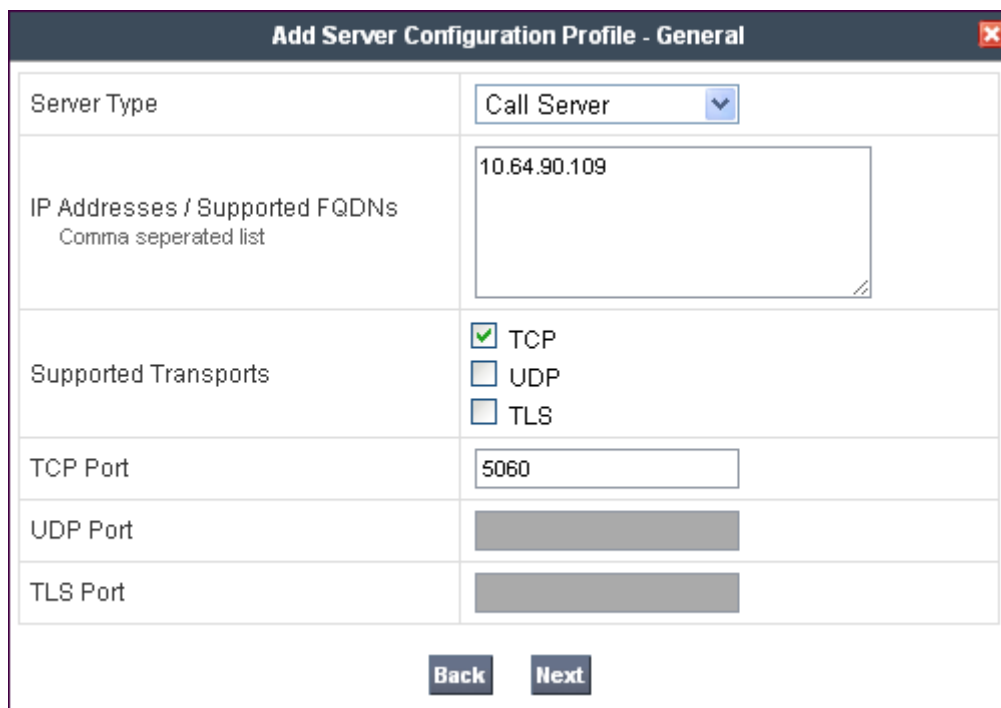


The image shows a dialog box titled "Add Server Configuration Profile". It has a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" with the value "SM62-Lab2" entered. Below the input field is a blue button labeled "Next".

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:** Enter the IP address of the Session Manager signaling interface. This should match the IP address of the Session Manager Security Module in **Section 6.9**.
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Entity Link on Session Manager in **Section 6.6**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link on Session Manager in **Section 6.6**.

Click **Next** to continue.

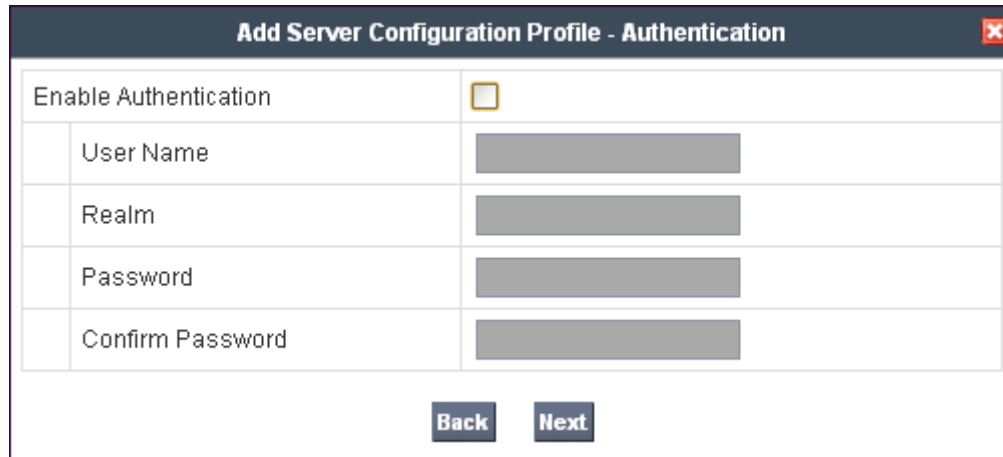


The image shows a dialog box titled "Add Server Configuration Profile - General". It has a close button (X) in the top right corner. The dialog contains several fields:

- Server Type:** A drop-down menu with "Call Server" selected.
- IP Addresses / Supported FQDNs:** A text area with the value "10.64.90.109". Below the text area is the label "Comma seperated list".
- Supported Transports:** Three checkboxes: "TCP" (checked), "UDP" (unchecked), and "TLS" (unchecked).
- TCP Port:** A text input field with the value "5060".
- UDP Port:** A disabled text input field.
- TLS Port:** A disabled text input field.

At the bottom of the dialog are two buttons: "Back" and "Next".

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



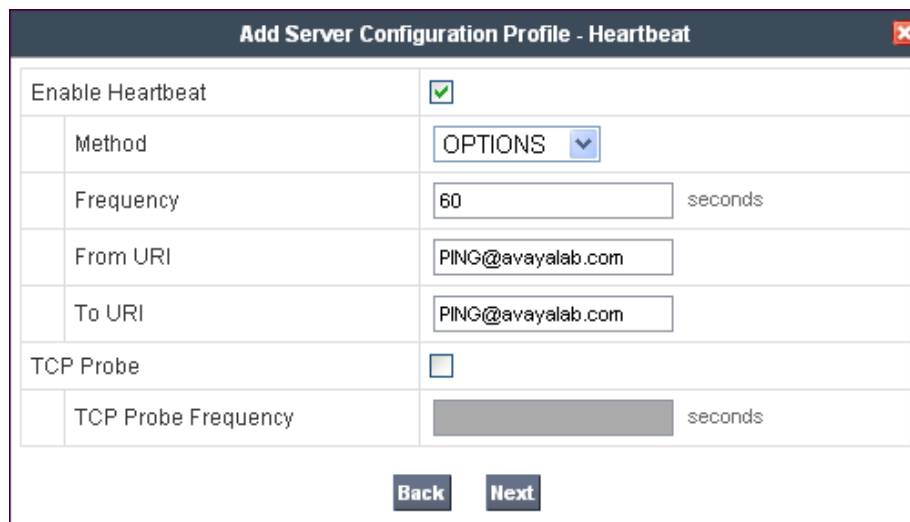
Add Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

Back **Next**

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

- **Enabled 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.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

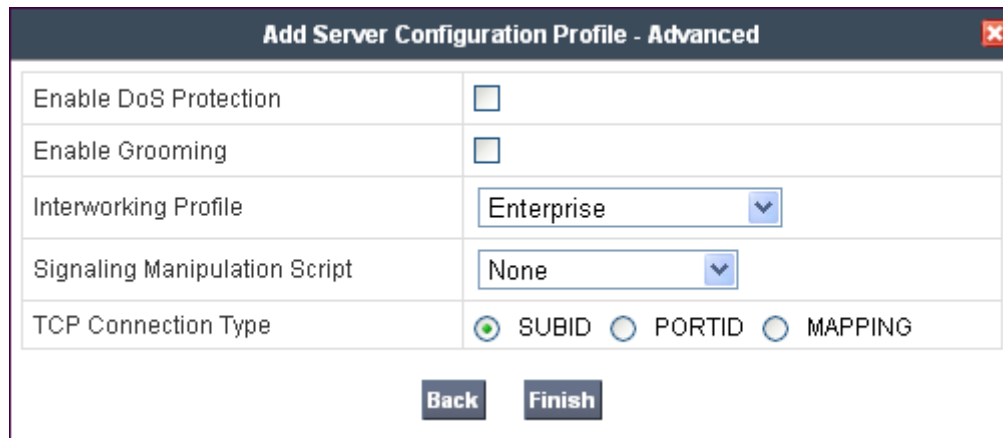
Click **Next** to continue.



Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	PING@avayalab.com
To URI	PING@avayalab.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds

Back **Next**

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.1.3.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.



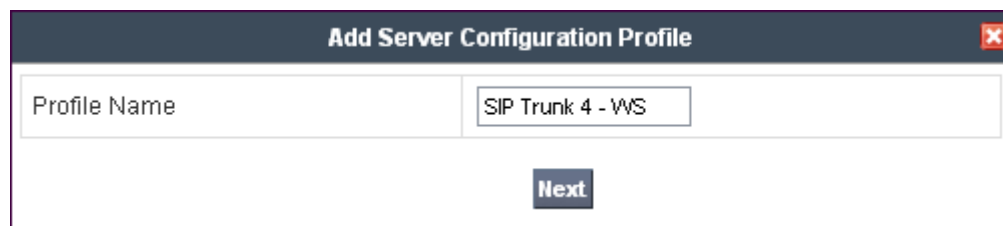
The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains five rows of configuration options:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Enterprise
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

At the bottom of the dialog are two buttons: "Back" and "Finish".

7.1.5.2 Server Configuration - Windstream

To add a Server Configuration Profile for Windstream navigate to **UC-Sec Control Center** → **Global Profiles** → **Server Configuration** and click on **Add Profile** (not shown). Enter a descriptive name for the new profile and click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It contains one row with a text input field:

Profile Name	SIP Trunk 4 - WVS
--------------	-------------------

At the bottom of the dialog is a button labeled "Next".

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

- **Server Type:** Select **Trunk Server** from the drop-down box.
- **IP Addresses / Supported 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 Windstream SIP Trunk IP address. This will associate the inbound SIP messages from Windstream to this Sever Configuration.
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and Windstream.
- **TCP Port:** Enter the port number that Windstream uses to send SIP traffic.

Click **Next** to continue.

Add Server Configuration Profile - General	
Server Type	Trunk Server
IP Addresses / Supported FQDNs Comma seperated list	172.16.1.26
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
<div>Back Next</div>	

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

Add Server Configuration Profile - Authentication

Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Back **Next**

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

- **Enabled 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.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an 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@windstream.com was used in the sample configuration to better identify the SIP OPTIONS in the call traces. Windstream 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).

Add Server Configuration Profile - Heartbeat	
Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	ping@windstream.com
To URI	ping@windstream.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	seconds
<div>Back Next</div>	

In the new window that appears, select the **Interworking Profile** created for Windstream in **Section 7.1.3.2**. Select the **Signaling Manipulation Script** created in **Section 7.1.4**. Use default values for all remaining fields. Click **Finish** to save the configuration.

Add Server Configuration Profile - Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Windstream
Signaling Manipulation Script	SIP Trunk4_Script
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Back

Finish

7.2. 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 in 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.

7.2.1. Media Rules

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

Create a custom Media Rule to set the Quality of Service and Media Anomaly Detection. The sample configuration shows a custom Media Rule **New-Low-Med** created for the enterprise and Windstream.

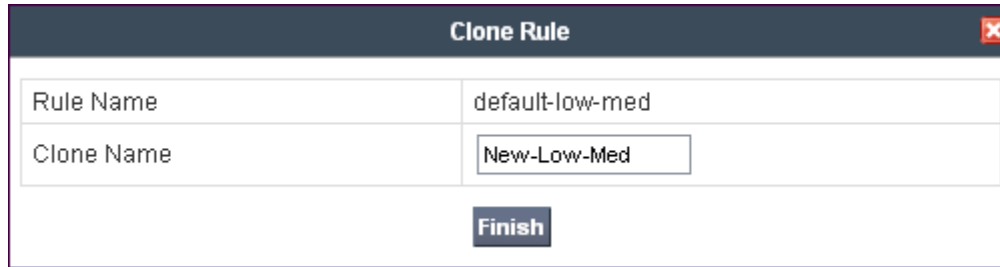
To create a custom Media Rule, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** as shown below.

The screenshot shows the UC-Sec Control Center web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar shows a tree view of the system configuration, with 'Domain Policies' expanded and 'Media Rules' selected. The main content area displays the 'Media Rules' configuration for the 'default-low-med' rule. A 'Clone Rule' button is visible in the top right. Below it, a warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The configuration table shows the following settings:

Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS	Turing Test
Media Anomaly Detection <input checked="" type="checkbox"/>					
Detect RTP Injection Attack <input checked="" type="checkbox"/>					
Asymmetric RTP <input type="checkbox"/>					
Action Alert					

An 'Edit' button is located at the bottom right of the configuration table.

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



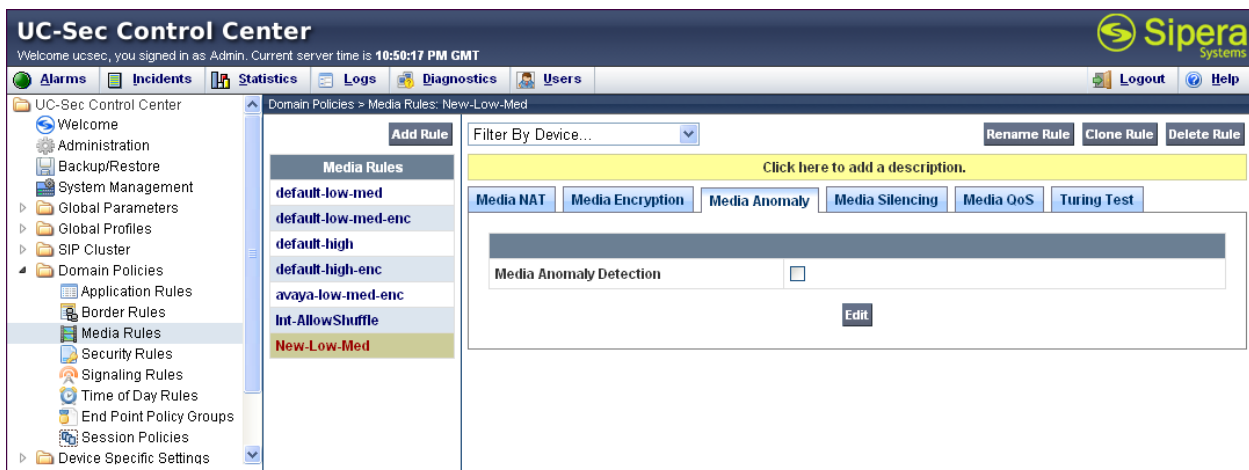
A dialog box titled "Clone Rule" with a close button (X) in the top right corner. It contains two input fields: "Rule Name" with the value "default-low-med" and "Clone Name" with the value "New-Low-Med". Below the fields is a "Finish" button.

Rule Name	default-low-med
Clone Name	New-Low-Med

Finish

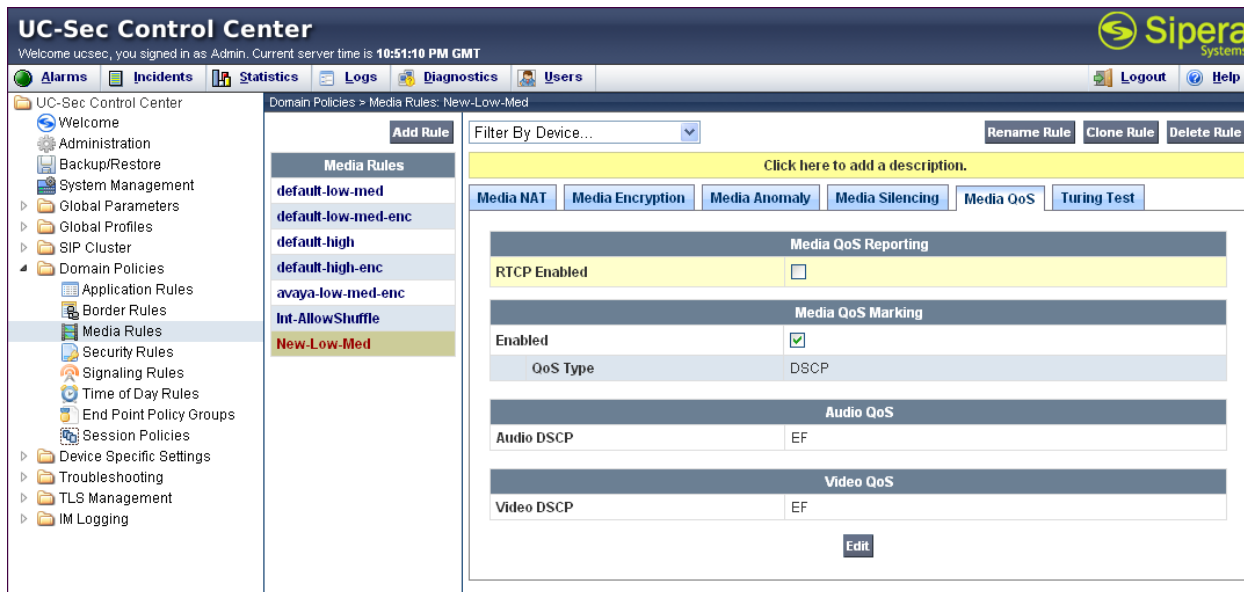
When the RTP packets of a call are shuffled from Communication Manager to an IP Phone, Avaya SBCE will interpret this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created during an audio shuffle. To modify the rule, select the **Media Anomaly** tab and click **Edit**. Uncheck **Media Anomaly Detection** and click **Finish** (not shown).

The following screen shows the **New-Low-Med** rule with **Media Anomaly Detection** disabled.



The screenshot shows the UC-Sec Control Center interface. The top bar includes the title "UC-Sec Control Center", a welcome message, the user "Admin", the server time "10:50:17 PM GMT", and the Siper Systems logo. Below the top bar is a navigation menu with tabs: Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The main content area is titled "Domain Policies > Media Rules: New-Low-Med". It features a list of media rules on the left, including "default-low-med", "default-low-med-enc", "default-high", "default-high-enc", "avaya-low-med-enc", "Int-AllowShuffle", and "New-Low-Med" (highlighted). On the right, there is a "Filter By Device..." dropdown and buttons for "Add Rule", "Rename Rule", "Clone Rule", and "Delete Rule". Below these is a yellow bar with the text "Click here to add a description.". A tabbed interface shows "Media NAT", "Media Encryption", "Media Anomaly", "Media Silencing", "Media QoS", and "Turing Test". The "Media Anomaly" tab is active, showing a checkbox for "Media Anomaly Detection" which is unchecked, and an "Edit" button.

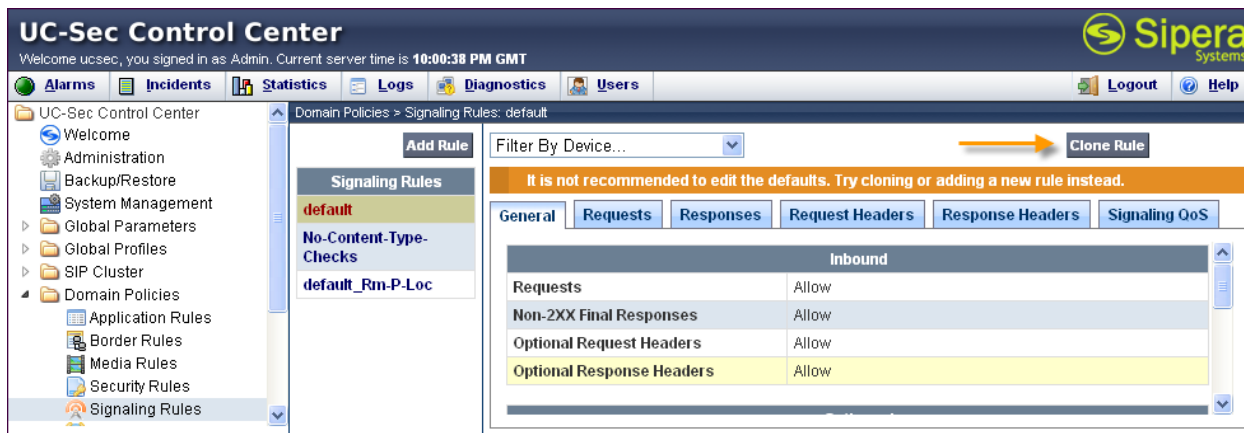
On the **Media QoS** tab select the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for compliance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



7.2.2. 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 have the Avaya SBCE respond to SIP OPTION requests and to set the Quality of Service. To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.



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

Clone Rule

Rule Name

default

Clone Name

Avaya

Finish

On the **Requests** tab, click on **Add In Request Control** to add a new Request Control to block OPTIONS request from passing through the Avaya SBCE and return 200 OK as the response as shown below.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 3:10:45 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

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

Domain Policies > Signaling Rules: Avaya

Add Rule

Filter By Device...

Rename Rule Clone Rule Delete Rule

Click here to add a description.

General Requests Responses Request Headers Response Headers Signaling QoS

Add In Request Control Add Out Request Control

Row	Method Name	In Dialog Action	Out of Dialog Action	Proprietary	Direction	
1	OPTIONS	Block with "200 OK"	Block with "200 OK"	No	IN	

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). 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

Welcome ucsec, you signed in as Admin. Current server time is 10:54:16 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

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

Domain Policies > Signaling Rules: Avaya

Add Rule

Filter By Device...

Rename Rule Clone Rule Delete Rule

Click here to add a description.

General Requests Responses Request Headers Response Headers Signaling QoS

Signaling QoS☒

QoS Type

DSCP

DSCP

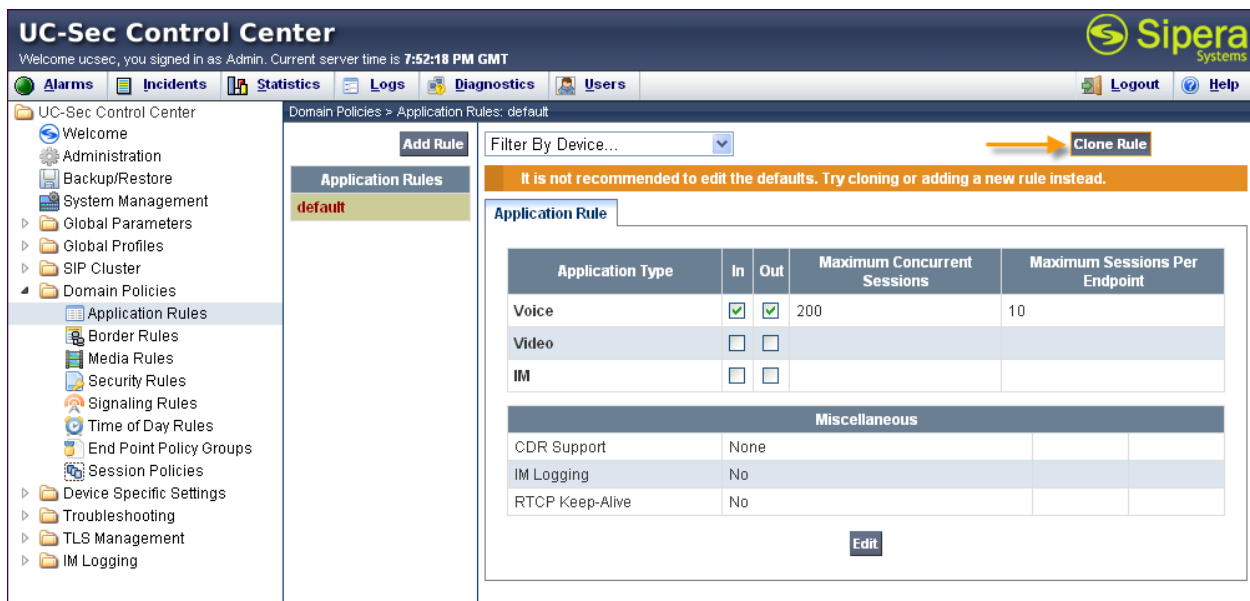
EF

Edit

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



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

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

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

Clone Rule

Rule Name	default
Clone Name	MaxVoiceSession

Finish

Modify the rule by clicking the **Edit** button. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. Keep in mind Avaya SBCE takes 30 seconds for sessions to be cleared after disconnect. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. In the sample configuration, Communication Manager was programmed to control the concurrent sessions by setting the number of members in the trunk group (**Section 5.8**) to the allotted amount. Therefore, the values in the Application Rule **MaxVoiceSession** were set high enough to be considered non-blocking.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration areas, with 'Domain Policies' expanded. The main panel displays the 'MaxVoiceSession' rule under 'Application Rules'. The rule is configured for 'Voice' with 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint' both set to 2000. There are also checkboxes for 'Video' and 'IM' which are currently unchecked. A 'Miscellaneous' section at the bottom shows settings for 'CDR Support', 'IM Logging', and 'RTCP Keep-Alive', all set to 'None' or 'No'. An 'Edit' button is visible at the bottom right of the rule configuration area.

7.2.4. 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 7.3.4**. Create a separate Endpoint Policy Group for the enterprise and the Windstream SIP Trunking service.

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

The screenshot shows the UC-Sec Control Center interface with the 'Endpoint Policy Groups' section selected. The left sidebar shows 'Domain Policies' expanded, and 'Endpoint Policy Groups' is highlighted. The main panel displays a list of existing policy groups: 'default-low', 'default-low-enc', 'default-med', 'default-med-enc', 'default-high', 'default-high-enc', 'OCS-default-high', and 'avaya-def-low-enc'. An 'Add Group' button is visible at the top left of the main panel. Below the list, there is a table with columns for 'Order', 'Application', 'Border', 'Media', 'Security', 'Signaling', and 'Time of Day'. The first row shows a policy group with 'Order' 1, 'Application' 'default', 'Border' 'default', 'Media' 'default-low-med', 'Security' 'default-low', 'Signaling' 'default', and 'Time of Day' 'default'. A 'View Summary' button and an 'Add Policy Set' button are also present.

The following screen shows **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**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration areas, with 'Domain Policies' expanded. The main panel displays the 'Enterprise_DomPolicy' configuration. A table lists the policy rules:

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

The following screen shows **SIP Trunk_DomPolicy** created for Windstream. Set the **Application**, **Media** and **Signaling** rules to the ones previously created. Set the **Border**, **Signaling**, and **Time of Day** rules to **default** and set the **Security** rule to **default-high**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration areas, with 'Domain Policies' expanded. The main panel displays the 'SIP Trunk_DomPolicy' configuration. A table lists the policy rules:

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

7.3. 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.

7.3.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of 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.

Navigate to **UC-Sec Control Center** → **Device Specific Settings** → **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**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Device Specific Settings' expanded, showing 'Network Management' selected. The main content area is titled 'Device Specific Settings > Network Management: ASBCE'. It has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.128), and 'B2 Netmask'. An 'Add IP' button is present. A yellow banner says 'Changes will not take effect until the interface is updated.' Below this is a table with columns: IP Address, Public IP, Gateway, and Interface. The table contains two rows: one with IP 205.xxx.xxx.92, Gateway 205.xxx.xxx.1, and Interface B1; the other with IP 10.64.19.100, Gateway 10.64.19.1, and Interface A1. 'Save Changes' and 'Clear Changes' buttons are at the bottom right of the table.

IP Address	Public IP	Gateway	Interface
205.xxx.xxx.92		205.xxx.xxx.1	B1
10.64.19.100		10.64.19.1	A1

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

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 3:34:07 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - Signaling Forking
 - SNMP
 - End Point Flows
 - Session Flows
 - Two Factor

Device Specific Settings > Network Management: ASBCE

UC-Sec Devices

ASBCE

Network Configuration Interface Configuration

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

7.3.2. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. 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 → Device Specific Settings → 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.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 4:08:35 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

- Welcome
- Administration
- Backup/Restore
- System Management
- Global Parameters
- Global Profiles
- SIP Cluster
- Domain Policies
- Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - Signaling Forking
 - SNMP
 - End Point Flows

Device Specific Settings > Signaling Interface: ASBCE

UC-Sec Devices

ASBCE

Signaling Interface

Add Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Inside	10.64.19.100	5060	5060	---	None	
Sig_Outside_92	205.191.92	5060	5060	---	None	

7.3.3. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will listen for SIP media on the defined ports. Create a SIP 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 created in **Section 5.6**.

To create a new Media Interface, navigate to **UC-Sec Control Center → Device Specific Settings → 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.

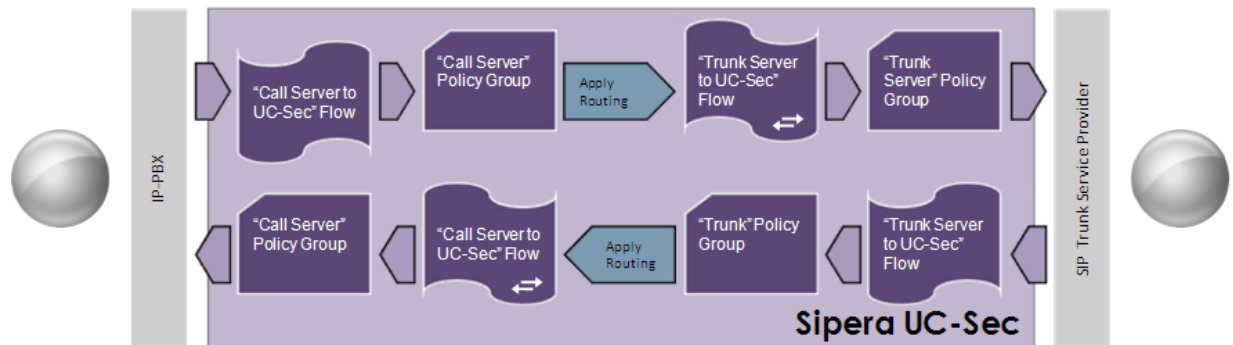


The screenshot displays the UC-Sec Control Center web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar shows a tree view of the system configuration, with 'Device Specific Settings' expanded to show 'Media Interface'. The main content area is titled 'Media Interface' and contains a warning message: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' Below this is a table listing the configured media interfaces.

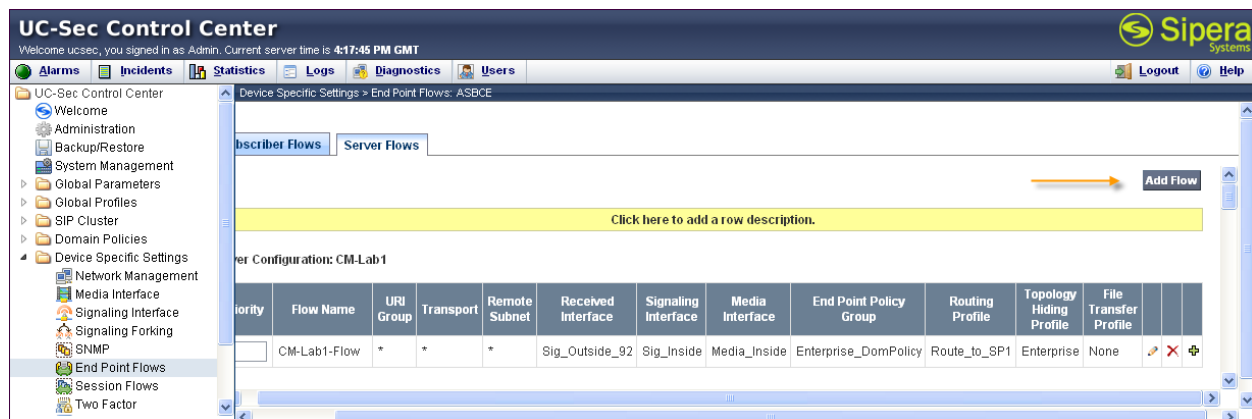
Name	Media IP	Port Range		
Media_Inside	10.64.19.100	2048 - 3329		
Media_Outside_92	205.160.1.92	8000 - 8999		

7.3.4. 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 Avaya SBCE to secure a SIP Trunk call.



Create a Server Flow for Session Manager and Windstream. To create a Server Flow, navigate to **UC-Sec Control Center** → **Device Specific Settings** → **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 7.1.5** 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.
- **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 Windstream:

Edit Flow: SIP Trunk 4_Flow
✖

Criteria	
Flow Name	<input type="text" value="Windstream_Flow"/>
Server Configuration	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="SIP Trunk 4 - WS"/>
URI Group	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="*"/>
Transport	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="*"/>
Remote Subnet	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="*"/>
Received Interface	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="Sig_Inside"/>
Signaling Interface	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="Sig_Outside_92"/>
Media Interface	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="Media_Outside_92"/>
End Point Policy Group	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="SIP Trunk_DomPolicy"/>
Routing Profile	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="To-SM62-Lab2"/>
Topology Hiding Profile	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="SIP Trunk"/>
File Transfer Profile	<input style="background-color: #eee; border: 1px solid #ccc;" type="text" value="None"/>

Finish

The following screen shows the Sever Flow for Session Manager:

Criteria	
Flow Name	SM62-Lab2_Flow
Server Configuration	SM62-Lab2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_92
Signaling Interface	Inside_TLS
Media Interface	Media_Inside
End Point Policy Group	Enterprise_DomPolicy
Routing Profile	Route_to_Windstream
Topology Hiding Profile	Enterprise
File Transfer Profile	None

Finish

8. Windstream SIP Trunking Configuration

Windstream is responsible for the configuration of Windstream SIP Trunking. The customer will need to provide the IP address used to reach the Avaya SBCE. Windstream will provide the customer the necessary information to configure Communication Manager, Session Manager and Avaya SBCE to connect to Windstream including:

- IP address of the Windstream SIP proxy
- Supported codecs
- DID numbers
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

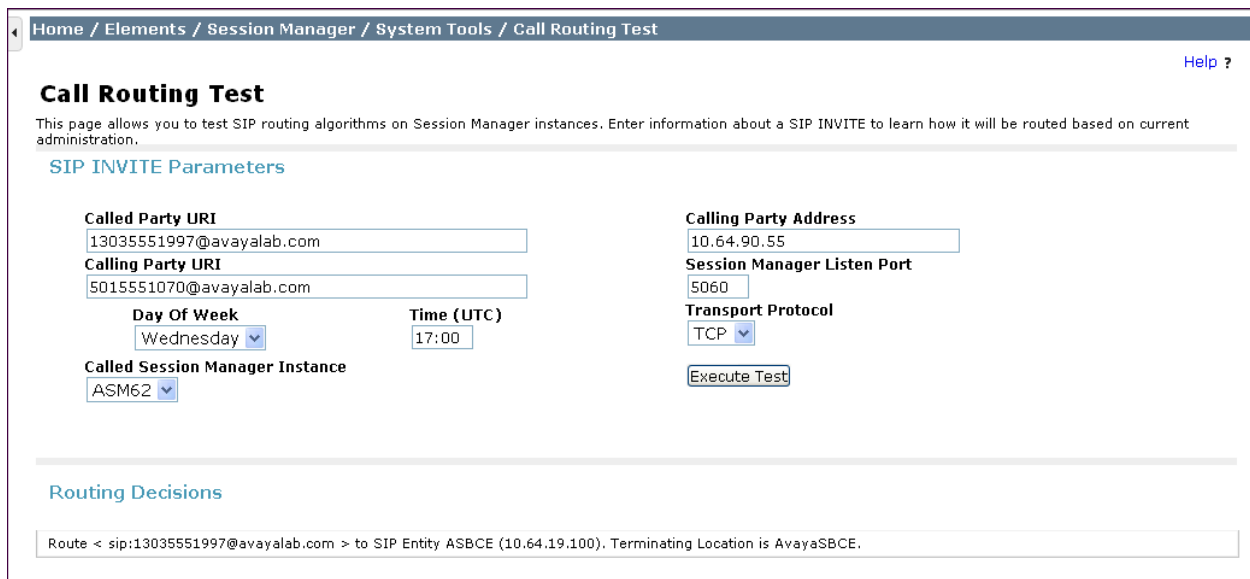
9. Verification and Troubleshooting

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.

9.1. Verification

The following steps may be used to verify the configuration:

1. Verify the call routing administration on Session Manager by logging in to System Manager and executing the Call Routing Test. Expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Populate the field for the call parameters of interest. For example, the following screen shows an example call routing test for an outbound call to PSTN via Windstream. Under **Routing Decisions**, observe the call will route via the Avaya SBCE SIP Entity to Windstream. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).



2. 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.
3. 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.
4. Verify that the user on the PSTN can end an active call by hanging up.
5. 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 Windstream SIP Trunking defined in **Section 5.8**.

Below is an example of an active call.

status trunk 1				
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	in-service/active	no	S00000
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

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

status trunk 1				
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0001/001	T00001	in-service/idle	no	
0001/002	T00002	in-service/idle	no	
0001/003	T00003	in-service/idle	no	
0001/004	T00004	in-service/idle	no	

9.2. Troubleshooting

1. Communication Manager:

- **list trace station** <extension number> - Traces calls to and from a specific station.
- **list trace tac** <trunk access code number> - Trace 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 number> - Displays trunk group information.

2. Session Manager:

- **traceSM -x -uni** - Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.

3. Avaya SBCE:

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

Incident Viewer

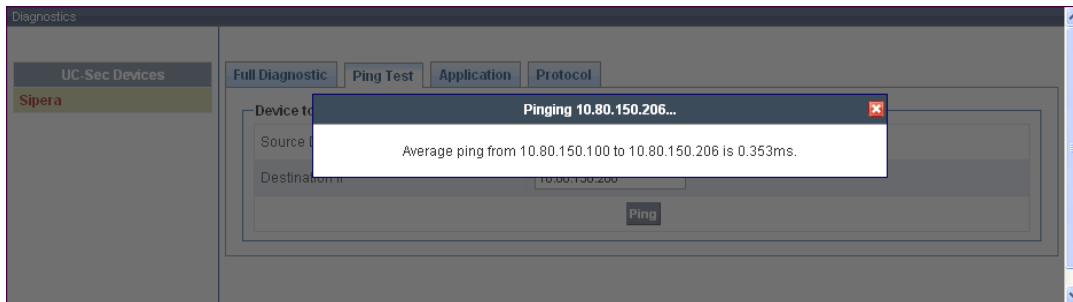
Device: **All** Category: **All** **Clear Filters** **Refresh** **Show Chart** **Generate Report**

Displaying results 1 to 15 out of 102.

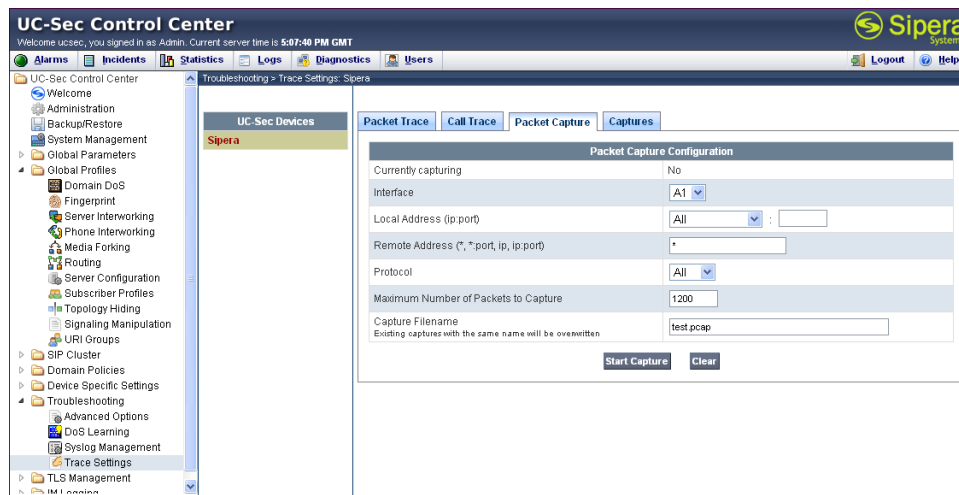
Incident Type	Incident ID	Date	Time	Category	Device	Cause
Message Dropped	662168149391824	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168147389246	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168146388212	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145887753	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168145636658	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168142392101	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168140391726	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168138390782	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168136390456	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168134389013	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168132388591	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168131388258	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130886109	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Message Dropped	662168130635815	12/19/11	11:11 PM	Policy	Sipera	No Server Flow Matched for Incoming Message
Server Heartbeat	662165350683634	12/19/11	9:38 PM	Policy	Sipera	Server Heartbeat is UP

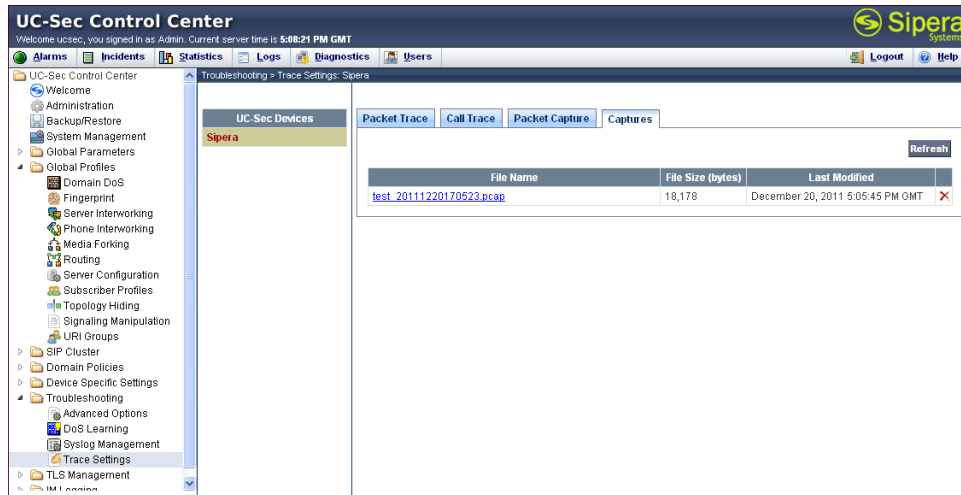
<< < 1 2 3 4 5 > >>

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

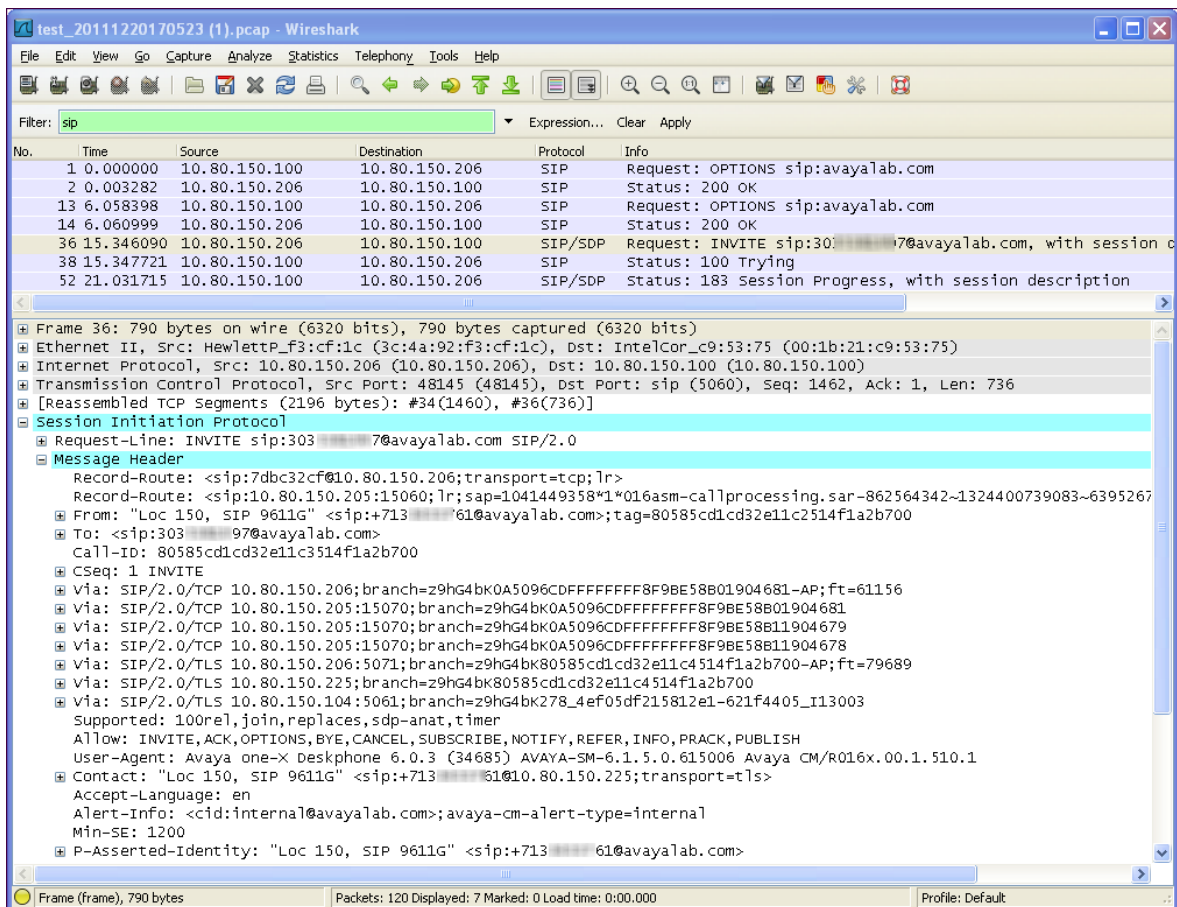


- **Troubleshooting → Trace Settings** - Configure and display call traces and packet captures for the UC-Sec appliance.





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



10. Conclusion

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

11. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform, Release 6.0.3*, February 2011.
- [2] *Administering Avaya Aura® System Platform, Release 6.0.3*, February 2011.
- [3] *Administering Avaya Aura® Communication Manager*, June 2010, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, June 2010, Document Number 555-245-205.
- [5] *Installing and Upgrading Avaya Aura® System Manager 6.1 GA Version*, November 2010.
- [6] *Installing and Configuring Avaya Aura® Session Manager*, April 2011, Document Number 03-603473
- [7] *Administering Avaya Aura® Session Manager*, November 2010, Document Number 03-603324.
- [8] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, April 2010, Document Number 16-601443.
- [9] *4600 Series IP Telephone LAN Administrator Guide*, July 2008, Document Number 555-233-507.
- [10] *Avaya one-X Deskphone H.323 Administrator Guide*, May 2011, Document Number 16-300698.
- [11] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1*, December 2010, Document Number 16-603838
- [12] *Administering Avaya one-X Communicator*, July 2011
- [13] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3, Document Number 03-300509.
- [14] *Feature Description and Implementation for Avaya Communication Manager, Issue 5*, Document Number 555-245-205
- [15] *UC-Sec Install Guide (102-5224-400v1.01)*
- [16] *UC-Sec Administration Guide (010-5423-400v1.06)*
- [17] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [18] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [19] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [20] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

©2012 Avaya Inc. All Rights Reserved.

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

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