



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.0.1 and Avaya Session Border Controller for Enterprise 4.0.5 with CenturyLink SIP Trunk Service (Legacy Qwest) – Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6 and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager, Avaya Session Border Controller for Enterprise, and various Avaya endpoints.

CenturyLink is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Solutions and Interoperability Test Lab, utilizing CenturyLink SIP Trunk Services.

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	7
4.	Equipment and Software Validated	8
5.	Configure Avaya Aura® Communication Manager.....	8
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 Session Border Controller for Enterprise	24
6.1.	Global Profiles.....	27
6.1.1.	Routing Profile.....	27
6.1.2.	Topology Hiding Profile	28
6.1.3.	Server Interworking Profile	32
6.1.4.	Signaling Manipulation.....	40
6.1.5.	Server Configuration.....	43
6.2.	Domain Policies	50
6.2.1.	Media Rule.....	50
6.2.2.	Signaling Rule.....	53
6.2.3.	Application Rules.....	55
6.2.4.	Endpoint Policy Group	57
6.3.	Device Specific Settings.....	58
6.3.1.	Network Management.....	58
6.3.2.	Signaling Interface	60
6.3.3.	Media Interface	60
6.3.4.	End Point Flows - Server Flow	61
7.	CenturyLink SIP Trunk Service Configuration	65
8.	Verification and Troubleshooting	65
8.1.	Verification.....	65

8.2. Troubleshooting	66
9. Conclusion	68
10. Additional References.....	69

1. Introduction

These Application Notes describe a sample configuration of Avaya Aura® Communication Manager and Avaya Session Border Controller for Enterprise 4.0.5 integration with CenturyLink SIP Trunk Service (Legacy Qwest) using Sonus NBS version 7.3.5R6.

In the sample configuration, the Avaya Session Border Controller for Enterprise (Avaya SBCE) is used as an edge device between Avaya Customer Premise Equipment (CPE) and CenturyLink SIP Trunk. The Avaya SBCE performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the CenturyLink SIP Trunk access method.

CenturyLink SIP Trunk 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.

CenturyLink SIP Trunk 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). SIP Trunk will also offer remote DID capability for a customer wishing to offer local numbers to their customers that can be aggregated in SIP format back to customer.

2. General Test Approach and Test Results

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

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 Road Warrior and Telecommuter modes were tested. Avaya one-X Communicator also supports two Voice over IP (VoIP)

protocols: H.323 and SIP. Only the H.323 protocol was tested. Session Manager is needed to support SIP endpoints.

- Various call types including: local, long distance, international, outbound toll-free, operator assisted calls, emergency calls (911) and local directory assistance (411).
- Inbound toll-free calls.
- Codecs G.729A, G.729AB and G.711MU.
- DTMF transmission using RFC 2833.
- T.38 Fax.
- 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).

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk Service (Legacy Qwest) was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **Calling Party Number (PSTN transfers):** The calling party number displayed on the PSTN phone is not updated to reflect the true connected party on calls that are transferred to the PSTN. After the call transfer is complete, the calling party number displays the number of the transferring party and not the actual connected party. The PSTN phone display is ultimately controlled by the PSTN provider, thus this behavior is not necessarily indicative of a limitation of the combined Avaya/CenturyLink SIP Trunk solution. It is listed here simply as an observation.
- **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. A Sigma script in the SBC is also required to prevent one way audio after the transfer. See **Section 6.1.4.**
- **Network Call Redirection using 302 Moved Temporarily:** When Communication Manager is programmed to redirect an inbound call to a PSTN number before answering the call in a vector, CenturyLink will send an ACK to the “302 Moved Temporarily” SIP message from the enterprise but will not redirect the call to the new party in the Contact header of the 302 message. The inbound call initiator hears a fast busy in this failure scenario. A workaround is to use the REFER method to redirect the call by having Communication Manager answer the call first with an announcement.

2.3. Support

For technical support on the CenturyLink SIP Trunk Service, contact CenturyLink using the Customer Care links at www.centurylink.com

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the DevConnect compliance testing. The configuration is comprised of the Avaya CPE location connected via a T1 Internet connection to the CenturyLink SIP Trunks to East and West servers. The Avaya CPE location simulates a customer site. At the edge of the Avaya CPE location, Avaya SBCE provides NAT functionality and SIP header manipulation. Avaya SBCE receives traffic from CenturyLink SIP Trunk on port 5060 and sends traffic to the CenturyLink SIP Trunk using destination port 5060, using the UDP protocol. For security reasons, any actual public IP addresses used in the configuration have been either replaced with private IP addresses or have been blocked out. Similarly, any references to real routable PSTN numbers have also been changed to numbers that cannot be routed by the PSTN.

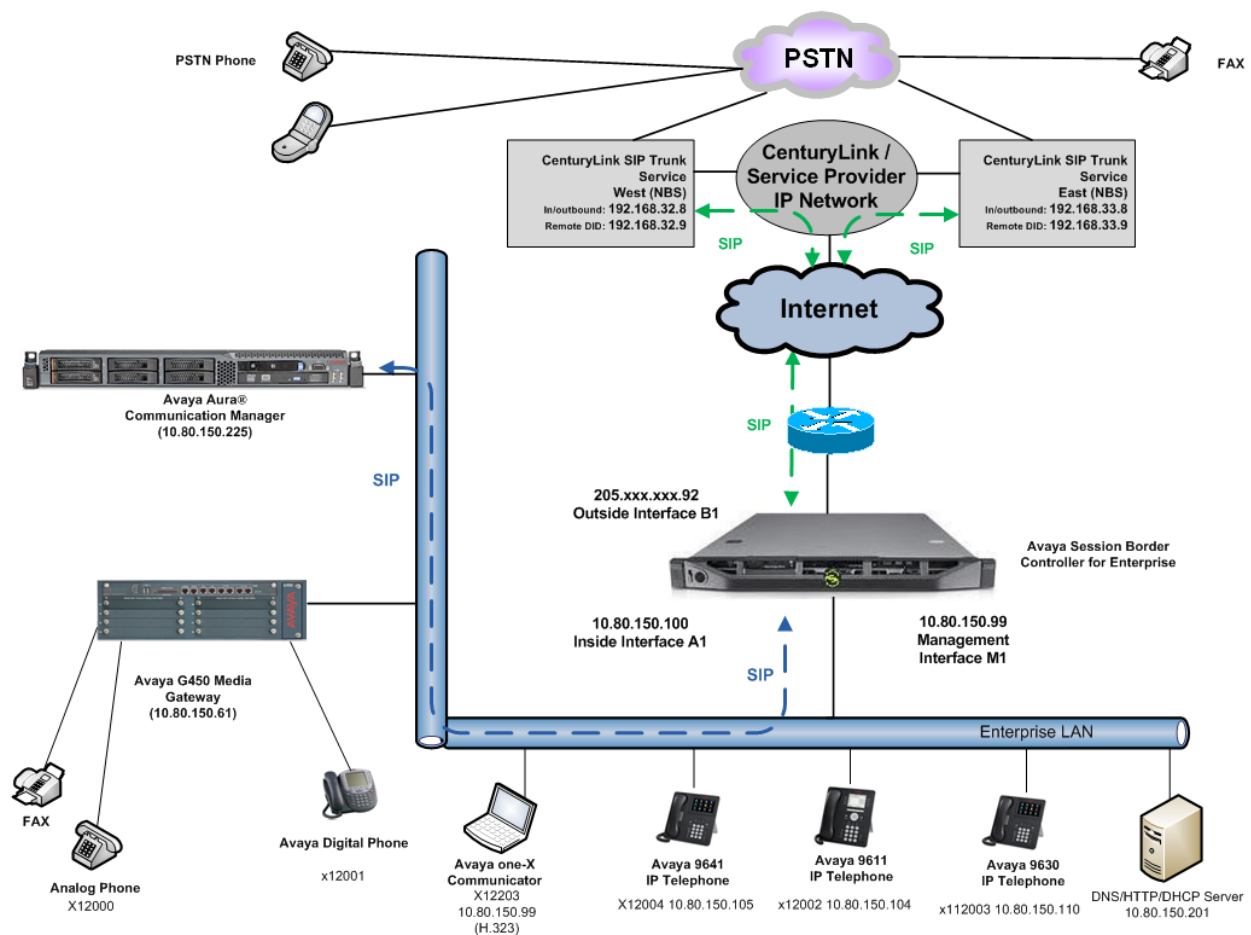


Figure 1: Avaya Interoperability Test Lab Configuration

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 Manger	R016x.00.1.510.1-19528 (SP 7)
Avaya Aura® Communication Manager Messaging	N6.0.1-8.0
Avaya Session Border Controller for Enterprise	4.0.5.Q09
Avaya G450 Media Gateway	31.22.0
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.104S
Avaya 9641 IP Telephone (H.323)	Avaya one-X® Deskphone SIP Edition 6.2009
Avaya 9611 IP Telephone (H.323)	Avaya one-X® Deskphone SIP Edition 6.2009
Avaya one-X® Communicator (H.323)	6.1.3.09
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink (Legacy Qwest) SIP Trunking Solution Components	
Component	Release
Sonus NBS	07.03.05 R006

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.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for CenturyLink SIP Trunk Service. A SIP trunk is established between Communication Manager and Avaya SBCE for use by signaling traffic to and from CenturyLink. It is assumed the general installation of Communication Manager, and Avaya G450 Media Gateway has been previously completed and is not discussed here.

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 **12000** licenses are available and **294** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	0	
Maximum Concurrently Registered IP Stations:		18000	3	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		128	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		18000	0	
Maximum Video Capable IP Softphones:		18000	1	
Maximum Administered SIP Trunks:		12000	294	
Maximum Administered Ad-hoc Video Conferencing Ports:		12000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	
Maximum TN2501 VAL Boards:		10	0	
Maximum Media Gateway VAL Sources:		250	1	
Maximum TN2602 Boards with 80 VoIP Channels:		128	0	
Maximum TN2602 Boards with 320 VoIP Channels:		128	0	
Maximum Number of Expanded Meet-me Conference Ports:		300	0	

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 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      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.

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

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

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

      INTERNATIONAL CALL ROUTING PARAMETERS
      Local Country Code: 1
      International Access Code: 011

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

      CALLER ID ON CALL WAITING PARAMETERS
      Caller ID on Call Waiting Delay Timer (msec): 200
```

5.3. IP Node Names

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

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
ASBCE	10.64.19.100	
CMMessaging	10.80.150.225	
default	0.0.0.0	
procr	10.80.150.225	
procr6	::	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 2 was used for this purpose. The CenturyLink SIP Trunk Service supports G.729A, G.729AB and G.711MU. During compliance testing each of the supported codecs were tested independently by changing the order of preference to list the codec being tested as the first choice. The true order of preference is defined by the end customer. In the example below, **G.729A** and **G.711MU** were 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.729A	n	2
2: G.711MU	n	2
3:		

On **Page 2**, set the **Fax Mode** to **T.38-standard**.

change ip-codec-set 2		Page 2 of 2
		IP Codec Set
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
Modem	t.38-standard	0
TDD/TTY	off	0
	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 2
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	IP Address: 10.80.150.225	
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** 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**.
- Set the **UDP Port Min** and **UDP Port Max** fields to a range suitable for RTP traffic.
- 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 Trunks
MEDIA PARAMETERS                                           Intra-region IP-IP Direct Audio: yes
Codec Set: 2                                               Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                         IP Audio Hairpinning? n
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                           RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

On **Page 4**, define the IP codec set to be used for traffic between region 2 and 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 2 was used for this purpose and was configured using the parameters highlighted below.

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

add signaling-group 1

Page 1 of 1

SIGNALING GROUP

Group Number: 1	Group Type: sip
IMS Enabled? n	Transport Method: tcp
Q-SIP? n	SIP Enabled LSP? n
IP Video? n	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? n	Peer Server: Others
Near-end Node Name: procr	Far-end Node Name: ASBCE
Near-end Listen Port: 5060	Far-end Listen Port: 5060
	Far-end Network Region: 2
Far-end Domain: avayalab.com	
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y	IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n
	Alternate Route Timer(sec): 6

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

```
add trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                                     Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SBC                     COR: 1              TN: 1          TAC: *01
  Direction: two-way                               Outgoing Display? n
  Dial Access? n                                    Night Service:
  Queue Length: 0
  Service Type: public-ntwrk                       Auth Code? n
                                                  Member Assignment Method: auto
                                                  Signaling Group: 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. Default values were used for all other fields.

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
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? 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 [15]**. 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**.

Set the **Telephone Event Payload Type** to **100**, the value preferred by CenturyLink.

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: 100	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	

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. If Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation, and digit manipulation via Communication Manager incoming call handling table may not be necessary. If the DID number sent by CenturyLink 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 1** command to create an entry for each DID. As an example, the following screen illustrates a conversion of DID number **3035557104** to extension **12004**.

change inc-call-handling-trmt trunk-group 1					Page	1 of	30
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	10	3035557104	10	12004			
public-ntwrk	10	3035557105	10	12005			
public-ntwrk	10	3035557106	10	13000			
public-ntwrk	10	3035557107	10	13001			
public-ntwrk	10	3035557108	10	13002			
public-ntwrk	10	3035557127	10	13003			
public-ntwrk	10	6145555714	10	13004			
public-ntwrk	10	6145555715	10	12000			

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 5.7**), 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 row shown in the example abridged output below, a specific Communication Manager extension (x12004) is mapped to a DID number that is known to CenturyLink for this SIP Trunk connection (3035557104), when the call uses trunk group 1.

change public-unknown-numbering 5 ext-digits 12000 trunk-group 1					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
5	12000	1	6145555715	10	Total Administered: 22
5	12001	1	6145555716	10	Maximum Entries: 9999
5	12004	1	3035557104	10	Note: If an entry applies to a SIP connection to Avaya Aura(tm) Session Manager, the resulting number must be a complete E.164 number.
5	12005	1	3035557105	10	
5	13000	1	3035557106	10	
5	13001	1	3035557107	10	
5	13002	1	3035557108	10	
5	13003	1	3035557127	10	
5	13004	1	6145555714	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: 2

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	attd						
1	5	ext						
2	5	ext						
3	5	ext						
4	5	ext						
5	5	ext						
6	5	ext						
7	5	ext						
8	5	ext						
9	1	fac						
*	3	dac						
#	3	dac						

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

change feature-access-codes			Page 1 of 10		
FEATURE ACCESS CODE (FAC)					
Abbreviated Dialing List1 Access Code: *10					
Abbreviated Dialing List2 Access Code: *12					
Abbreviated Dialing List3 Access Code: *13					
Abbreviated Dial - Prgm Group List Access Code: *14					
Announcement Access Code: *19					
Answer Back Access Code:					
Auto Alternate Routing (AAR) Access Code: *00					
Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2:		
Automatic Callback Activation: *33			Deactivation: #33		
Call Forwarding Activation Busy/DA: *30 All: *31			Deactivation: #30		
Call Forwarding Enhanced Status: Act:			Deactivation:		

Figure 18: Feature Access Codes

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:** **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, **Reference [3]** and **[4]**.

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

change ars analysis 1							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
1303	11	11	1	fnpa		n	
1502	11	11	1	fnpa		n	
1720	11	11	1	fnpa		n	
1800	11	11	1	fnpa		n	
1866	11	11	1	fnpa		n	
1877	11	11	1	fnpa		n	
1888	11	11	1	fnpa		n	
1908	11	11	1	fnpa		n	
2	10	10	1	hnpa		n	
3	10	10	1	hnpa		n	
4	10	10	1	hnpa		n	
411	3	3	1	svcl		n	
5	10	10	1	hnpa		n	
555	7	7	deny	hnpa		n	
6	10	10	1	hnpa		n	

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: CENTURYLINK 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 CenturyLink 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
3035557104	10	10	10	12004	ext	y	n	
3035557105	10	10	10	12005	ext	y	n	
3035557106	10	10	10	10000	ext	y	n	
3035557107	10	10	10	13004	ext	y	n	
3035557108	10	10	10	13002	ext	y	n	
3035557109	10	10	10	13001	ext	y	n	
3035557127	10	10	10	13003	ext	y	n	
6145555686	10	10	10	13000	ext	y	n	
6145555711	10	10	10	13003	ext	y	n	
6145555714	10	10	10	13004	ext	y	n	
6145555715	10	10	10	12000	ext	y	n	

5.12. Saving Communication Manager Configuration Changes

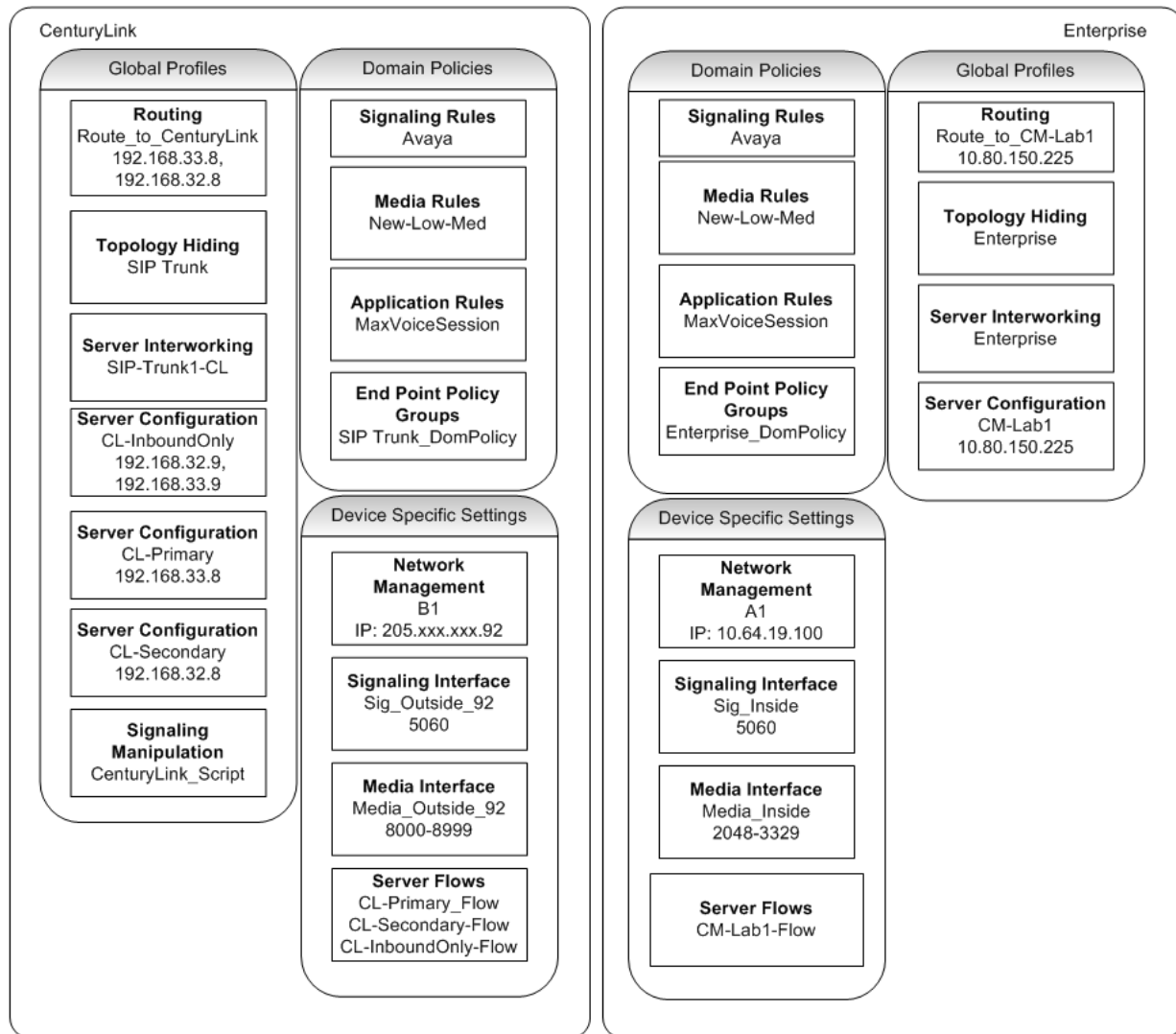
The command **save translation all** can be used to save the configuration.

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

6. Configure Avaya Session Border Controller for Enterprise

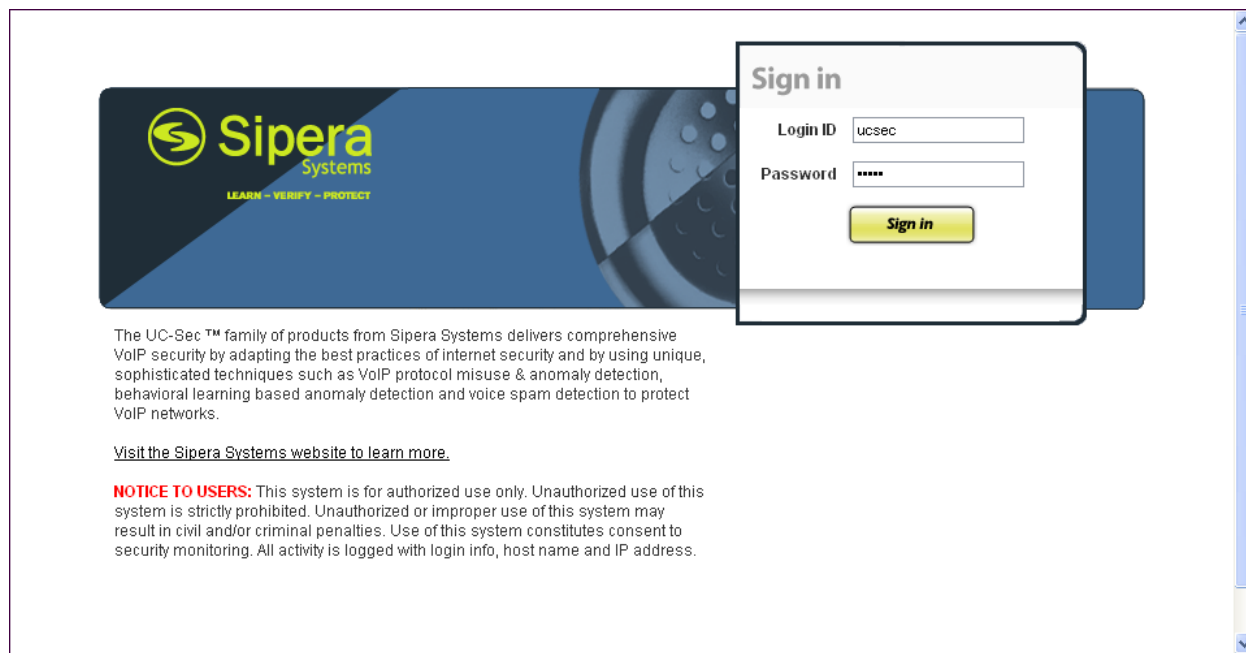
This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see **Reference** [12] and [13].

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



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**.

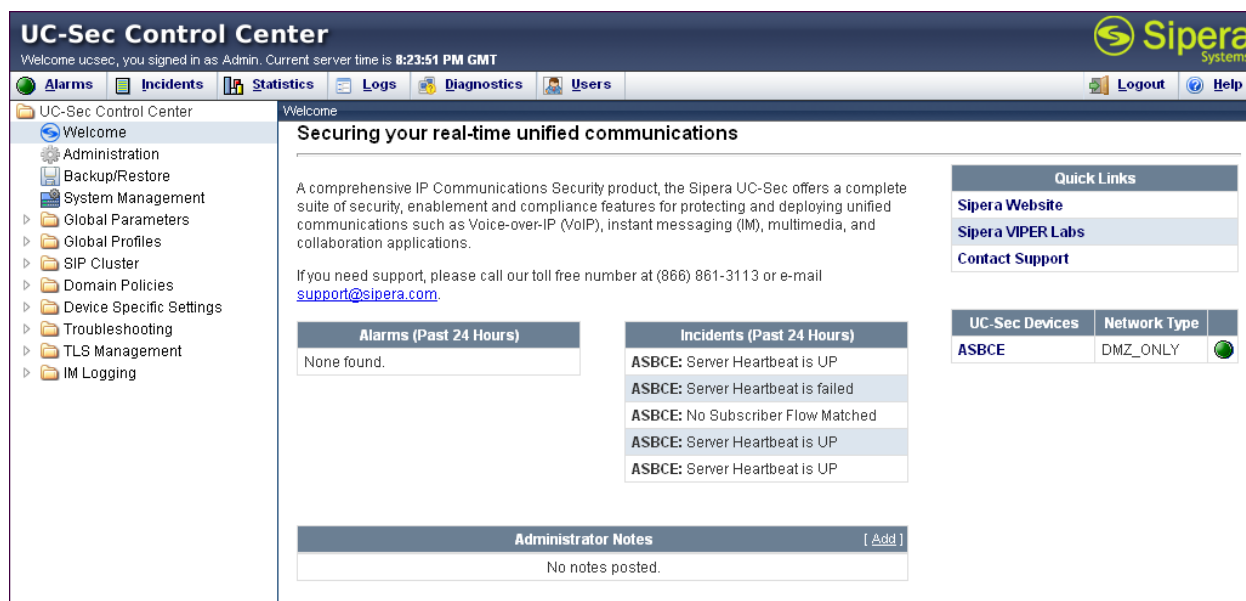


The UC-Sec™ family of products from Sipera Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection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

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

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

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 8:23:51 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
Troubleshooting
TLS Management
IM Logging

Welcome
Securing your real-time unified communications

A comprehensive IP Communications Security product, the Sipera 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: Server Heartbeat is UP
ASBCE: Server Heartbeat is failed
ASBCE: No Subscriber Flow Matched
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 shows the 'System Information: ASBCE' window. It contains several sections for configuration details:

- 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
----	--------------

6.1. Global Profiles

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

6.1.1. Routing Profile

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

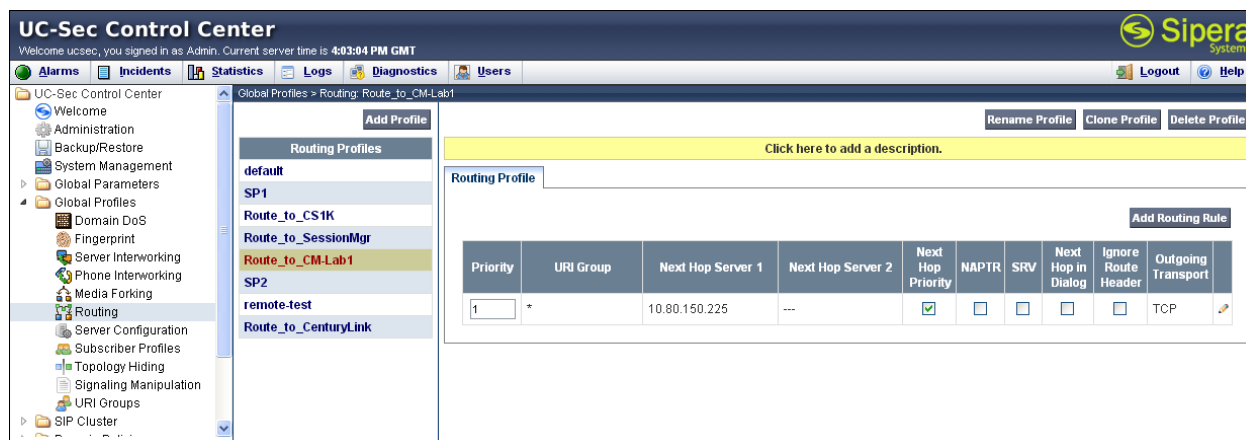
Create a Routing Profile for Communication Manager and CenturyLink. To add a routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue (not shown).

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

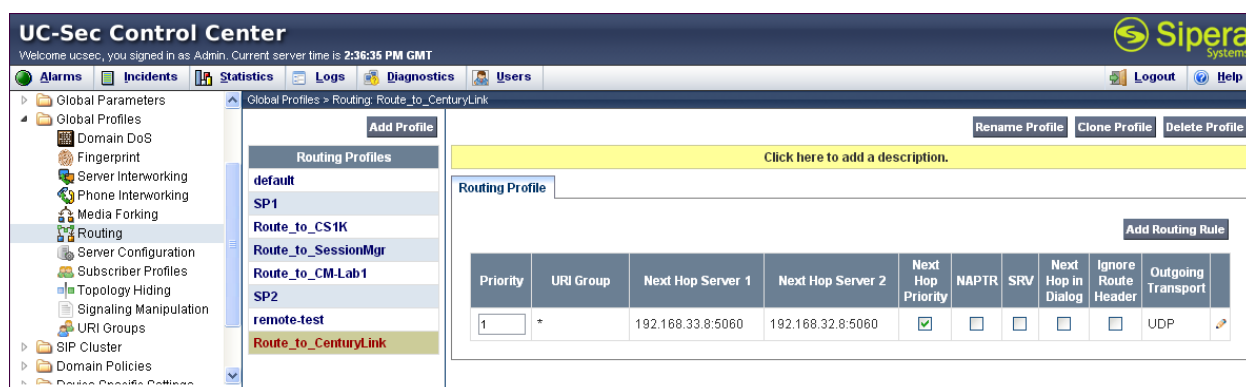
- **URI Group:** Select “*” from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server:** Checked.
- **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** is the IP address of the Communication Manager Processor Ethernet as defined in **Section 5.3**. The Outgoing Transport is set to **TCP** and matches the **Transport Method** set in the Communication Manager Signaling Group in **Section 5.7**.



The following screen shows the Routing Profile to CenturyLink. For compliance testing CenturyLink had four SIP servers assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound traffic. Only the two SIP servers allocated for outbound traffic were added to the Routing Profile.



6.1.2. 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 CenturyLink SIP Trunk. In the sample configuration, the **Enterprise** and **CenturyLink** 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 in **Figure 46**.

UC-Sec Control Center
 Welcome ucsec, you signed in as Admin. Current server time is 10:41:18 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center
 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

Global Profiles > Topology Hiding: default

Add Profile

Topology Hiding Profiles
 default

Clone Profile

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

Topology Hiding

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

Edit

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

Clone Profile

Profile Name	default
Clone Name	Enterprise

Finish

Edit the **Enterprise** profile to overwrite the headers shown below to the enterprise domain. The **Overwrite Value** should match the Domain set in the Communication Manager signaling group Far-end Domain (**Section 5.6**). 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 **CenturyLink** profile from the default values. The following screen shows the Topology Hiding Policy created for CenturyLink.

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

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

Add Profile

Topology Hiding Profiles

default

cisco_th_profile

SIP Trunk

Enterprise

Global Profiles > Topology Hiding: SIP Trunk

Rename Profile
Clone Profile
Delete Profile

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

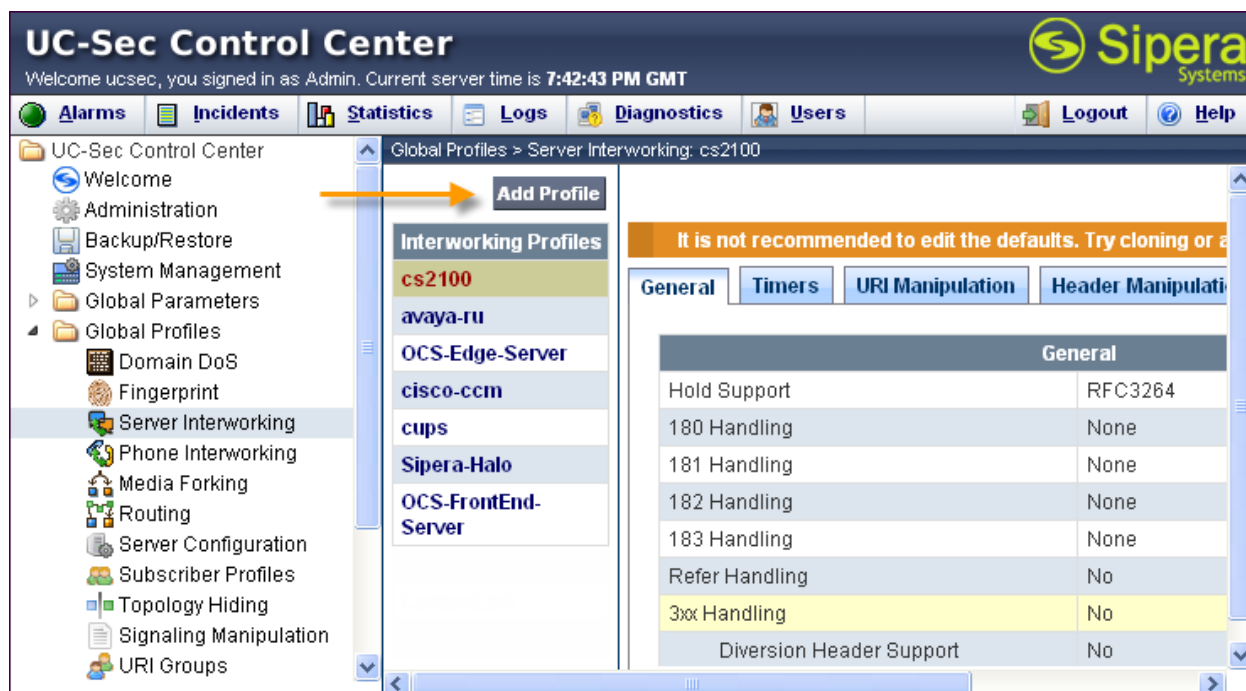
6.1.3. Server Interworking Profile

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

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

6.1.3.1 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 in **Figure 52**.



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, enter the following values. Use default values for all remaining fields:

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

Click **Next** to continue.

The screenshot shows a dialog box titled "Editing Profile: Enterprise" with a close button (X) in the top right corner. The dialog contains a table with configuration options for a profile. The table has two columns: the first column lists the configuration items, and the second column shows the selected values. The "General" tab is active, as indicated by the header. The configuration items and their values are as follows:

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

At the bottom of the dialog, there is a "Next" button.

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**
- **Has Remote SBC**

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**

6.1.3.2 Server Interworking Profile – CenturyLink

To create a new Server Interworking Profile for CenturyLink, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on **Add Profile** as shown in Figure 58.

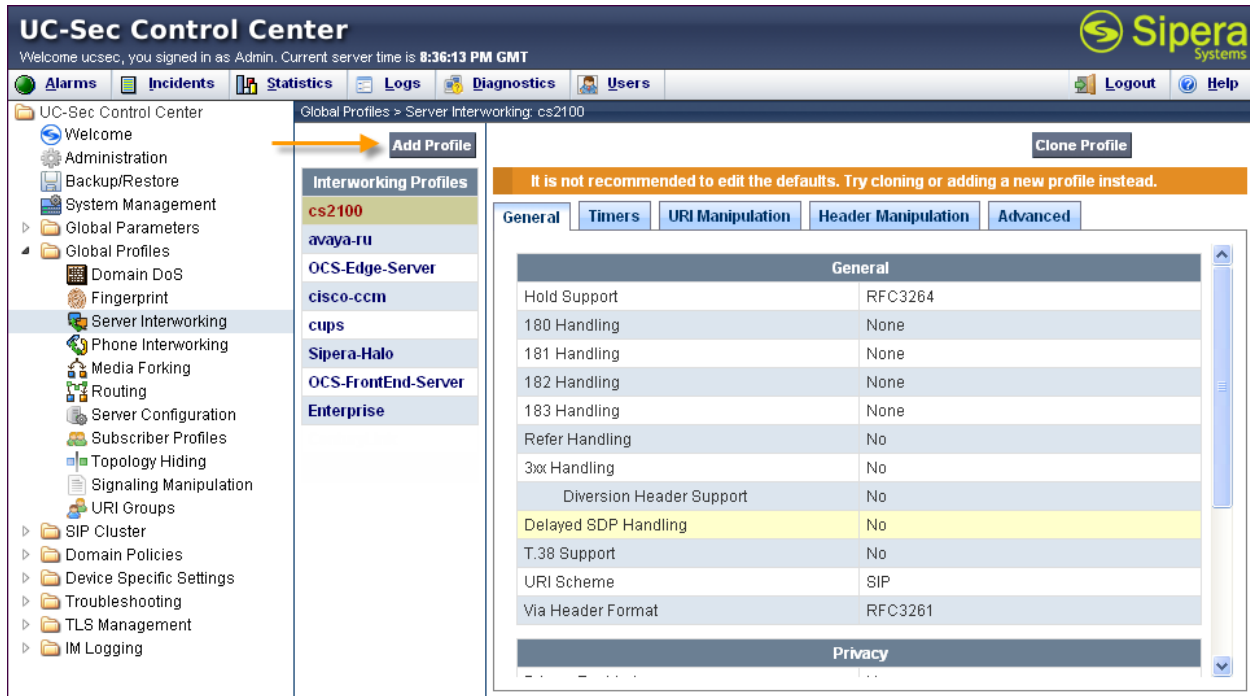


Figure 58: Server Interworking – Add Profile for CenturyLink

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

Interworking Profile

Profile Name

SIP-Trunk-1-CL

Next

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

- **Hold Support:** Select **RFC3264 - a=sendonly**.
- **T.38 Support:** Checked.

Click **Next** to continue.

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

Next

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 type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input 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**

6.1.4. Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will 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”.

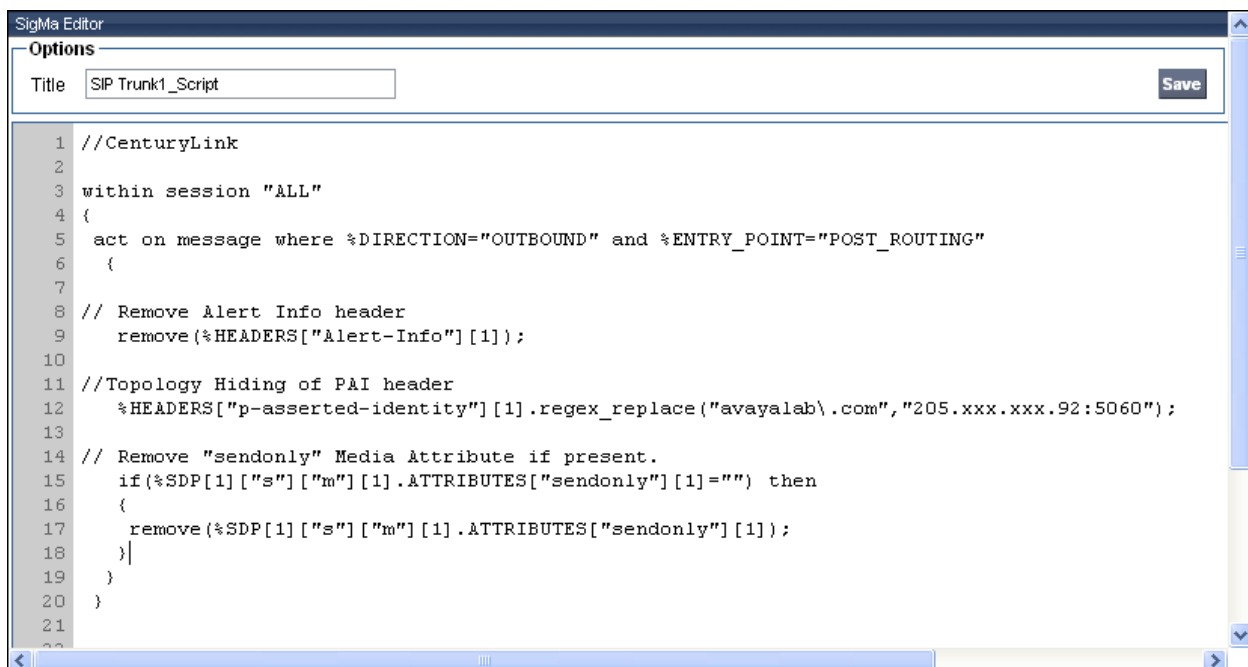
These application notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in topology hiding and to remove the *sendonly* media attribute sent by Communication Manager when a call is placed on hold. CenturyLink will stop sending RTP packets when the *sendonly* media attribute is received on a PSTN to PSTN transfer resulting in one way audio. The *sendrecv* media attribute is assumed as the default for the session when no other attribute is sent. So rather than replacing *sendonly* with *sendrecv*, the *sendonly* media attribute was simply removed.

To create a new Signaling Manipulation, navigate to **UC-Sec Control Center → Global Profiles → Signaling Manipulation** and click on **Add Script**. A new blank SigMa Editor window will pop up.

The following sample script will act on the response of an inbound call from CenturyLink (e.g., 180 Ringing and 200 OK) and the request of an outbound call to CenturyLink (e.g., INVITE messages from Communication Manager). 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 messages leaving the Sipera E-SBC.
- **%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).

With this script, 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. Also, the “sendonly” media attribute is being removed to prevent one way audio during PSTN to PSTN transfers when the Network Call Redirection feature is activated on the Communication Manager trunk group.



```

1 //CenturyLink
2
3 within session "ALL"
4 {
5   act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
6   {
7
8   // Remove Alert Info header
9     remove(%HEADERS["Alert-Info"][1]);
10
11 //Topology Hiding of PAI header
12   %HEADERS["p-asserted-identity"][1].regex_replace("avayalab.com","205.xxx.xxx.92:5060");
13
14 // Remove "sendonly" Media Attribute if present.
15   if(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]=="") then
16   {
17     remove(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]);
18   }
19 }
20 }
21

```

The following screen shows the finished Signaling Manipulation Script **SIP Trunk1_Script** used during compliance testing. This script will later be applied to the CenturyLink Server Configuration in **Section 6.1.5.2**.

The screenshot displays the UC-Sec Control Center web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users, along with a Logout button and a Help icon. The main content area is titled "Global Profiles > Signaling Manipulation: SIP Trunk1_Script". On the left, a sidebar menu lists various system management options, with "Signaling Manipulation" selected. The central panel shows a list of signaling manipulation scripts, including "SIP Trunk1_Script", which is highlighted. The right-hand pane displays the script's configuration, including a description field and a code editor containing the following script:

```
//CenturyLink
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    // Remove Alert Info header
    remove(%HEADERS["Alert-Info"][1]);

    //Topology Hiding of PAI header
    %HEADERS["p-asserted-identity"][1].regex_replace("avaya\.", "205.168.62.92:5060");

    // Remove "sendonly" Media Attribute if present.
    if (%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]="" ) then
    {
      remove(%SDP[1]["s"]["m"][1].ATTRIBUTES["sendonly"][1]);
    }
  }
}
```

Buttons for "Upload Script", "Add Script", "Download Script", "Clone Script", and "Delete Script" are visible at the top of the script configuration area. An "Edit" button is located at the bottom right of the code editor.

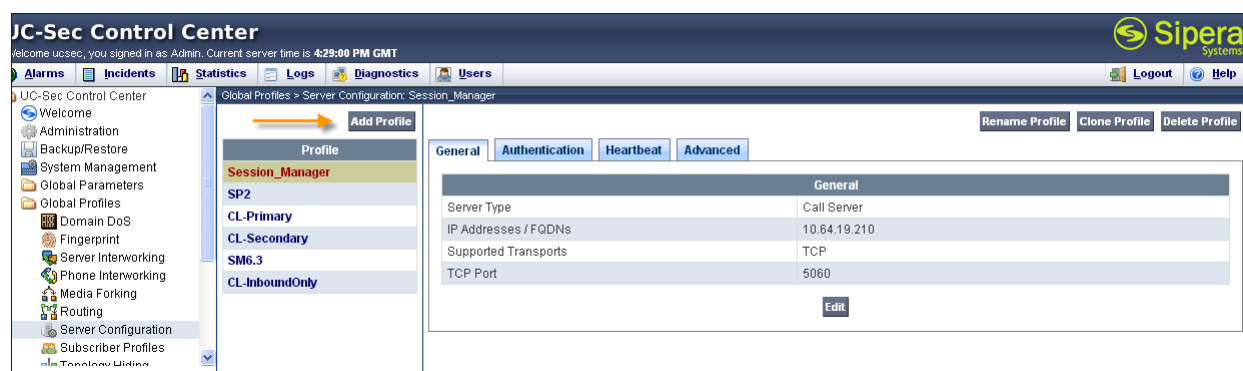
6.1.5. Server Configuration

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

In the sample configuration, separate Server Configurations were created for **Communication Manager** and **CenturyLink**.

6.1.5.1 Server Configuration – Communication Manager

To add a Server Configuration Profile for Communication 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**.

Add Server Configuration Profile

Profile Name

CM-Lab1

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 Communication Manager Processor Ethernet as defined in **Section 5.3**.
- **Supported Transports:** Select **TCP**.
- **TCP Port:** Port number on which to send SIP requests to Communication Manager. This should match the port number used in the **Far-end Listen Port** in the Communication Manager Signaling Group as defined **Section 5.7**.

Click **Next** to continue.

Add Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.80.150.225
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
<div>Back Next</div>	

Verify **Enable Authentication** is unchecked as Communication 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:

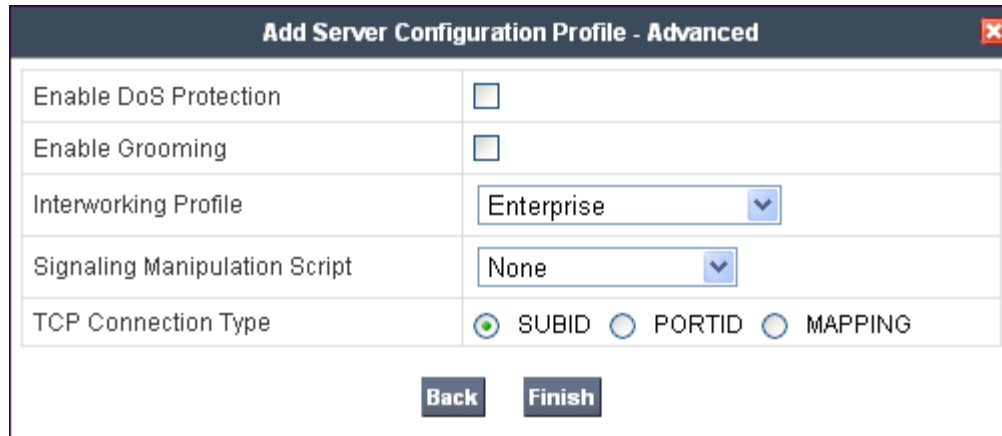
- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP 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 6.1.3.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.



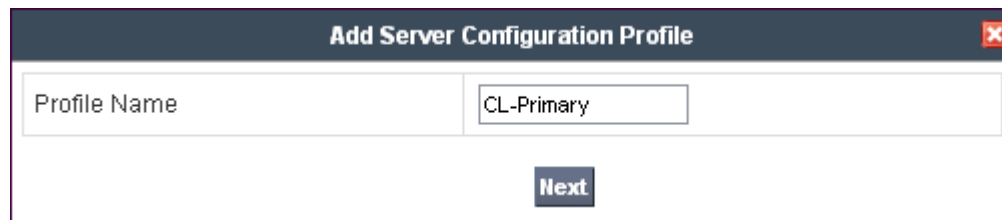
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Enterprise
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Back Finish

6.1.5.2 Server Configuration - CenturyLink

For compliance testing CenturyLink had four SIP servers assigned. Two of them were used for remote DIDs and were allocated for inbound only, while the other two were used for both inbound and outbound. Separate Server Configuration Profiles were created for the Primary and Secondary inbound and outbound IP addresses. A third Server Configuration Profile was created for the inbound only IP addresses.

To add Server Configuration Profiles for CenturyLink 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**.



Profile Name	CL-Primary
--------------	------------

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 of the SIP proxy of the service provider. In the sample configuration, this is 192.168.33.8 for the Primary server and 192.168.32.8 for the Secondary

- **Supported Transports:**

server. This will associate the inbound SIP messages from CenturyLink's SIP server to this Sever Configuration. Select the transport protocol to be used for SIP traffic between Avaya SBCE and CenturyLink.

- **UDP Port:**

Enter the port number that CenturyLink 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	192.168.33.8
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	
UDP Port	5060
TLS Port	
<div>Back</div> <div>Next</div>	

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

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

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 servers entered in the **IP Addresses /Supported FQDNs** in the **Server Configuration Profile** as show previously. The URI of PING@centurylink.com was used in the sample configuration to better identify the SIP OPTIONS in the call traces. CenturyLink 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@centurylink.com
To URI	PING@centurylink.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 CenturyLink in **Section 6.1.3.2**. Select the **Signaling Manipulation Script** created in **Section 6.1.4**. Use default values for all remaining fields. Click **Finish** to save the configuration.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SIP-Trunk-1-CL
Signaling Manipulation Script	SIP Trunk1_Script
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Once configuration is completed, the **CL-Primary** server configuration profile will appear as follows.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:50:33 PM GMT

Global Profiles > Server Configuration: CL-Primary

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.33.8
Supported Transports	UDP
UDP Port	5060

Repeat these procedures to create a separate server configuration for the secondary IP address for CenturyLink. Once configuration is completed, the **CL-Secondary** server configuration profile will appear as follows.

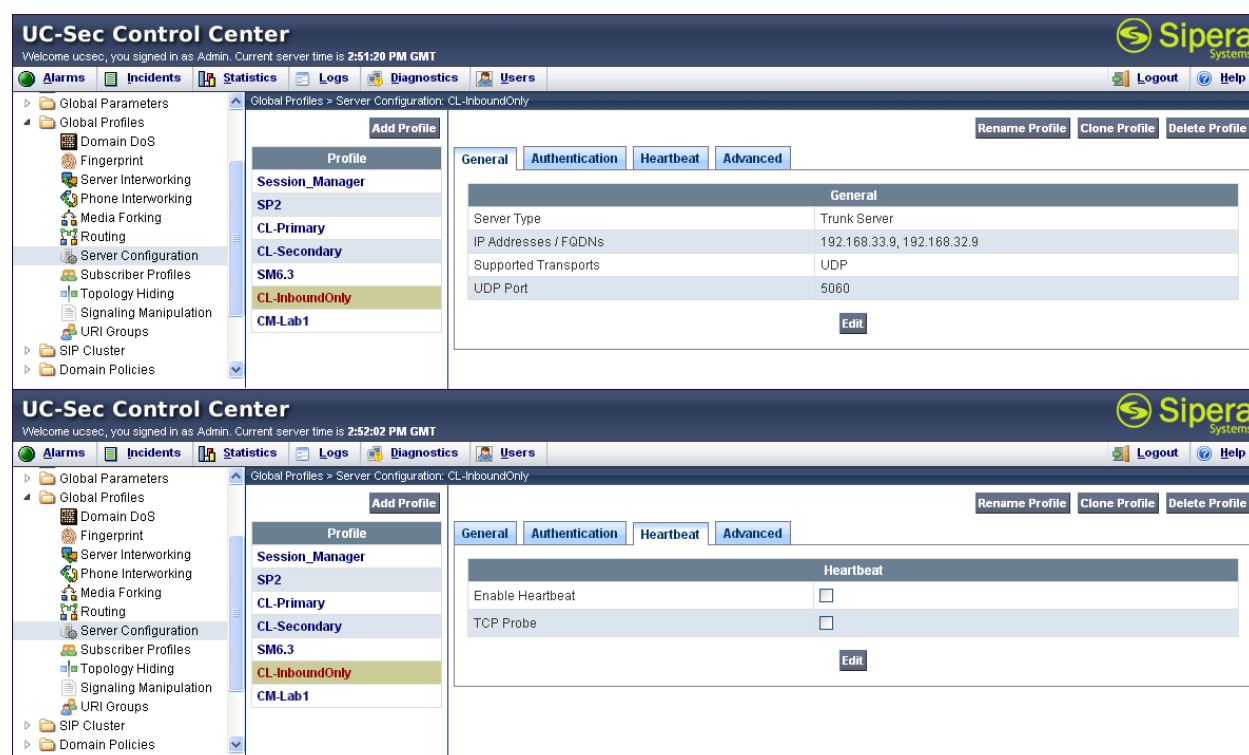
UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 2:51:03 PM GMT

Global Profiles > Server Configuration: CL-Secondary

General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.32.8
Supported Transports	UDP
UDP Port	5060

The inbound only IP addresses can be placed into one server configuration profile with the Heartbeat disabled as shown below.



6.2. Domain Policies

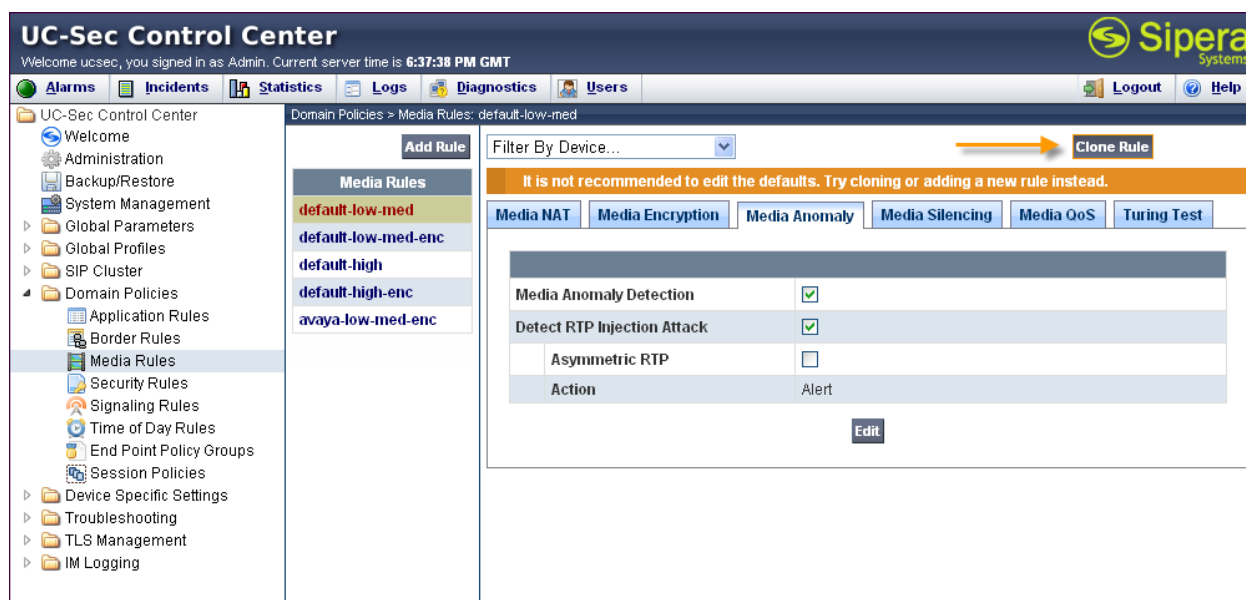
The Domain Policies feature configures, applies, and manages various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger policies which, in turn, activate 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.

6.2.1. Media Rule

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 CenturyLink.

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.



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

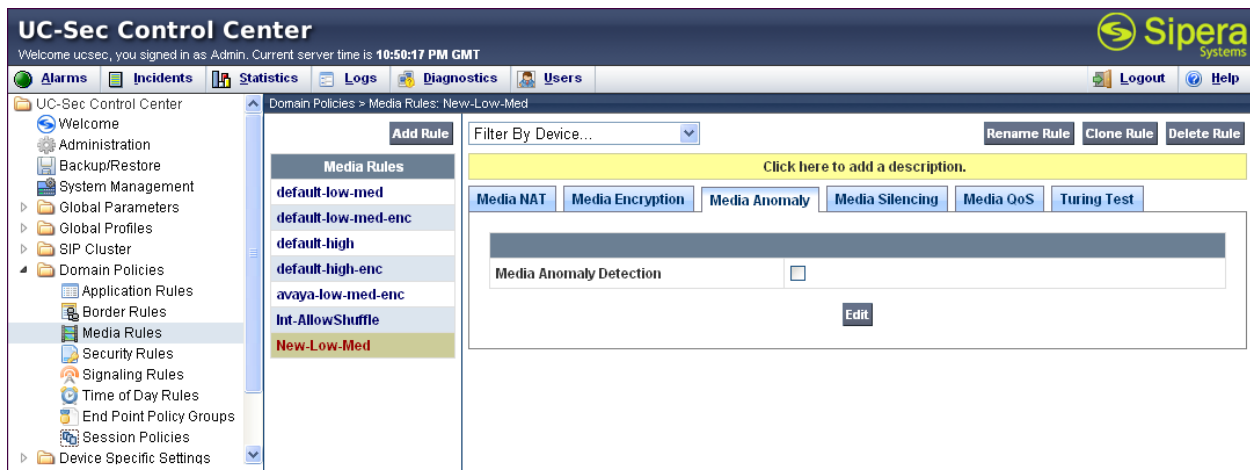
Clone Rule

Rule Name	default-low-med
Clone Name	<input type="text" value="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 **Internal-media** rule with **Media Anomaly Detection** disabled.



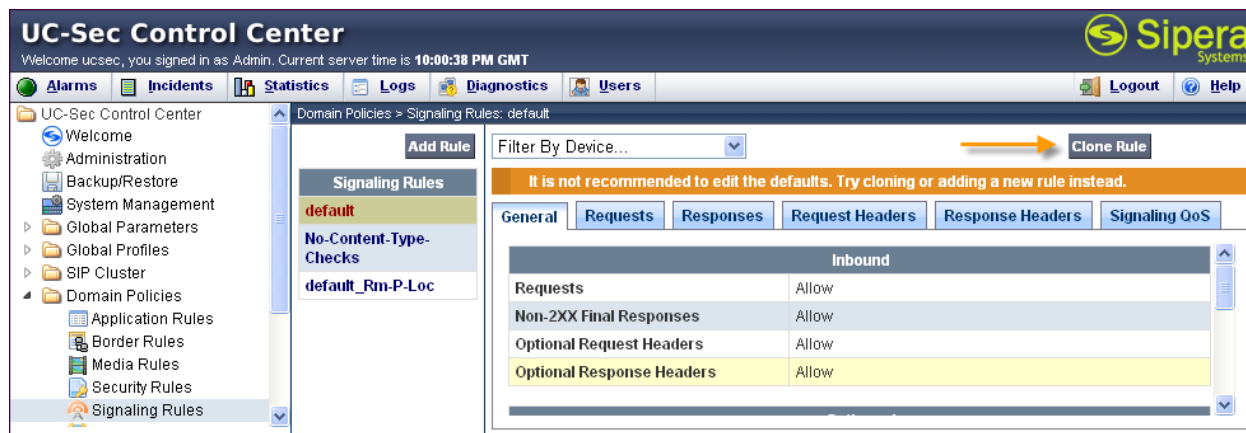
On the **Media QoS** tab select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for compliance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

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'Media Rules' selected. 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' (which is highlighted). The right pane shows the configuration for the 'New-Low-Med' rule, with tabs for 'Media NAT', 'Media Encryption', 'Media Anomaly', 'Media Silencing', 'Media QoS', and 'Tuning Test'. The 'Media QoS' tab is active, showing sections for 'Media QoS Reporting' (with 'RTCP Enabled' set to false), 'Media QoS Marking' (with 'Enabled' checked and 'QoS Type' set to 'DSCP'), 'Audio QoS' (with 'Audio DSCP' set to 'EF'), and 'Video QoS' (with 'Video DSCP' set to 'EF'). An 'Edit' button is located at the bottom right of the configuration pane.

6.2.2. Signaling Rule

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

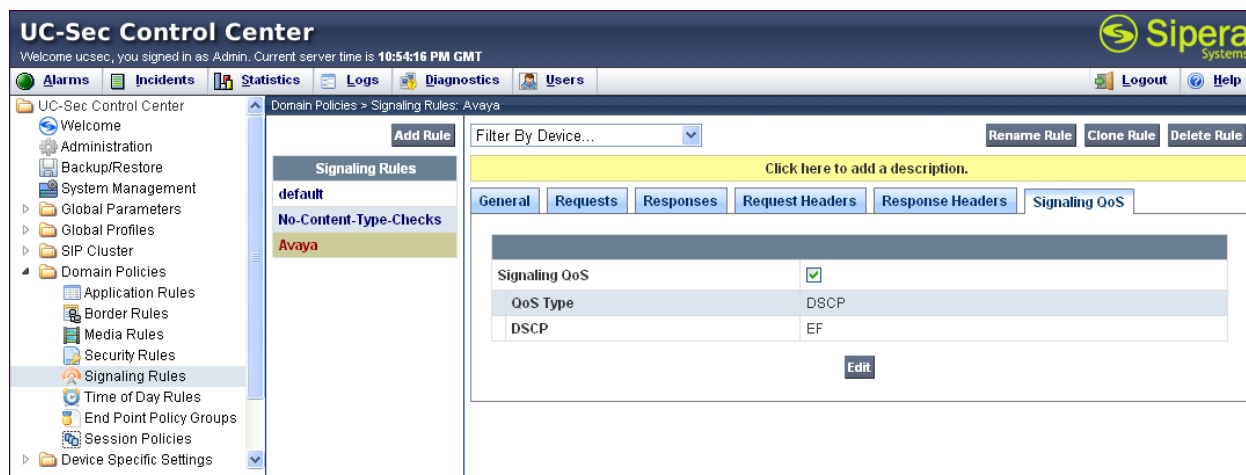
Clone and modify the default signaling rule to strip the P-Location and Alert Info headers from the SIP message before it is sent to the CenturyLink SIP Trunk. To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** as shown below.



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

The 'Clone Rule' dialog box is shown. It has two input fields: 'Rule Name' (containing 'default') and 'Clone Name' (containing 'Avaya'). A 'Finish' button is located at the bottom right of the dialog.

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.



6.2.3. Application Rules

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

Create an Application Rule to set the number of concurrent voice traffic. 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		

Edit

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

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 web interface. The left sidebar contains a navigation tree with categories like Administration, System Management, Global Parameters, SIP Cluster, Domain Policies, and Device Specific Settings. The main content area is titled 'Domain Policies > Application Rules: MaxVoiceSession'. It features a table for 'Application Rules' with columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The 'Voice' application is configured with 'In' and 'Out' checked and both session limits set to 2000. Below this is a 'Miscellaneous' section with settings for CDR Support, IM Logging, and RTP Keep-Alive. An 'Edit' button is located at the bottom right of the configuration area.

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

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

6.2.4. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 6.3.4**. Create a separate Endpoint Policy Group for the enterprise and the CenturyLink SIP Trunk.

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. The left sidebar contains a tree view with 'Domain Policies' expanded, and 'End Point Policy Groups' selected. The main area displays the 'Add Group' dialog for 'default-low'. The dialog includes a 'Filter By Device...' dropdown, a warning message, and a table for defining the policy group.

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

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 with 'Enterprise_DomPolicy' selected in the 'End Point Policy Groups' list. The main area displays the configuration for this policy group, including a table for defining the policy group.

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 CenturyLink. 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 contains a tree view with categories like Welcome, Administration, 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, and Device Specific Settings. The main area is titled 'Domain Policies > End Point Policy Groups: SIP Trunk_DomPolicy'. It features a 'Policy Groups' list on the left with items like default-low, default-low-enc, default-med, default-med-enc, default-high, default-high-enc, OCS-default-high, avaya-def-low-enc, Enterprise_DomPolicy, and SIP Trunk_DomPolicy (highlighted). The right pane shows a table for the selected policy group with columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and a final column with edit and delete icons. The table contains one row with the following values: Order 1, Application MaxVoiceSession, Border default, Media New-Low-Med, Security default-high, Signaling Avaya, Time of Day default.

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

6.3. Device Specific Settings

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

6.3.1. Network Management

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

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**.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 11:04:30 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

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

Device Specific Settings > Network Management: ASBCE

UC-Sec Devices
ASBCE

Network Configuration Interface Configuration

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

A1 Netmask 255.255.255.0 A2 Netmask B1 Netmask 255.255.255.128 B2 Netmask

Add IP Changes will not take effect until the interface is updated. Save Changes Clear Changes

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

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
Troubleshooting
TLS Management
IM Logging

Device Specific Settings > Network Management: ASBCE

UC-Sec Devices
ASBCE

Network Configuration Interface Configuration

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.

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

6.3.2. 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 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	205.192.92	5060	5060	---	None		

6.3.3. 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**. The outside port range should match the RTP port range provided by CenturyLink.

To create a new Signaling 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.

UC-Sec Control Center
 Welcome ucsec, you signed in as Admin. Current server time is 4:12:34 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

UC-Sec Control Center

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

Device Specific Settings > Media Interface: ASBCE

UC-Sec Devices
ASBCE

Media Interface

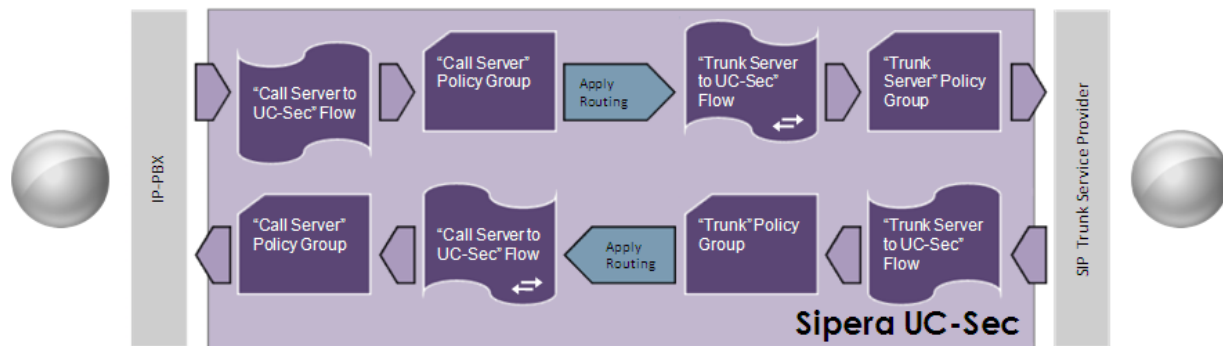
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add Media Interface

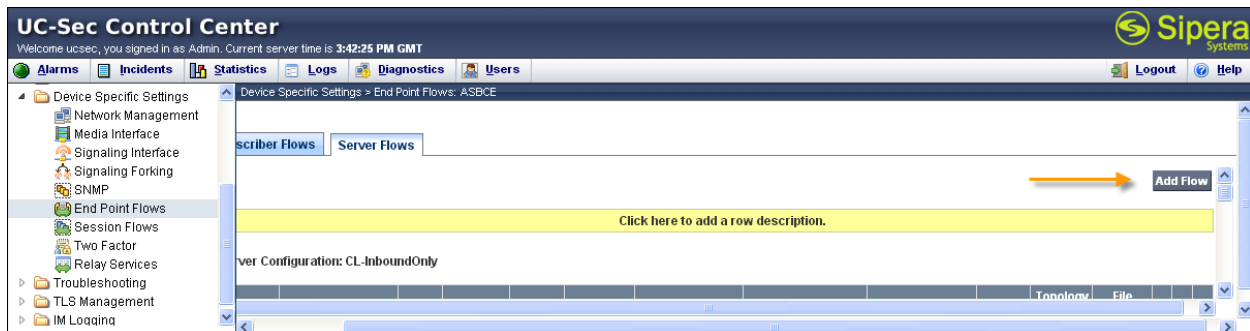
Name	Media IP	Port Range		
Media_Inside	10.64.19.100	2048 - 3329		
Media_Outside_92	205. . . .92	8000 - 8999		

6.3.4. End Point Flows - Server Flow

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



Create a Server Flow for Communication Manager and the CenturyLink SIP Trunk. 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.

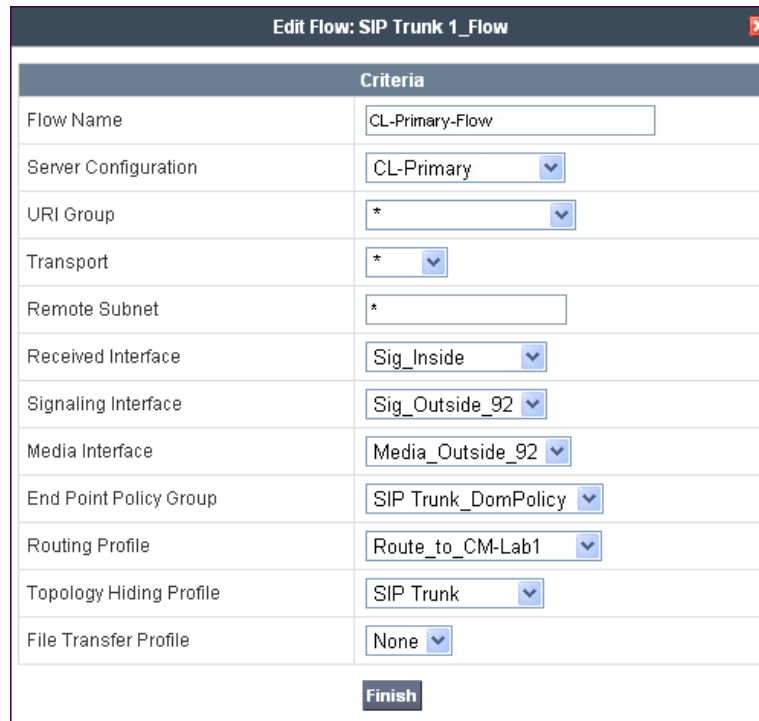


In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 6.1.5** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **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 Server Flow for CL-Primary:

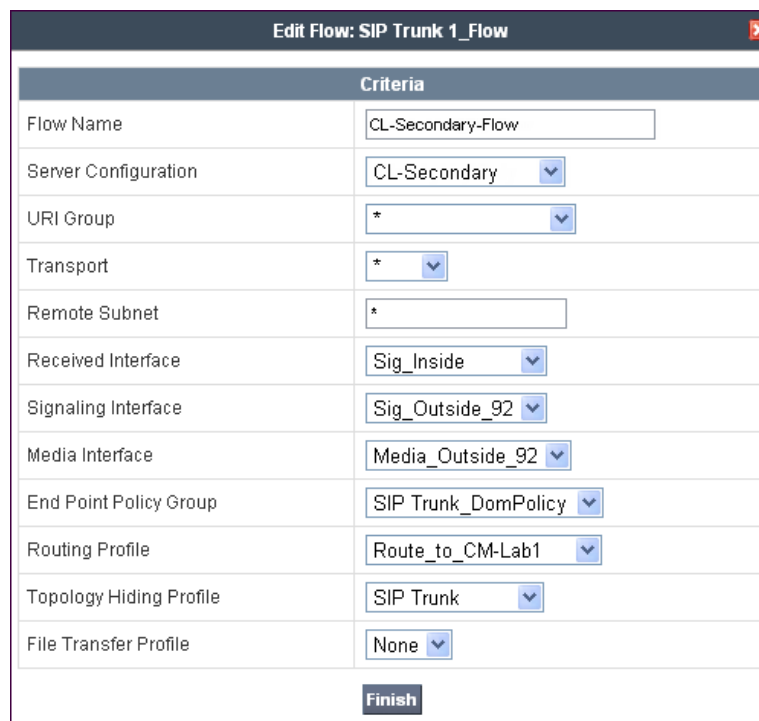


The screenshot shows a window titled "Edit Flow: SIP Trunk 1_Flow" with a close button in the top right corner. Below the title bar is a section labeled "Criteria" containing a table of configuration fields. The fields are as follows:

Criteria	
Flow Name	CL-Primary-Flow
Server Configuration	CL-Primary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside_92
Media Interface	Media_Outside_92
End Point Policy Group	SIP Trunk_DomPolicy
Routing Profile	Route_to_CM-Lab1
Topology Hiding Profile	SIP Trunk
File Transfer Profile	None

At the bottom of the table is a "Finish" button.

The following screen shows the Server Flow for CL-Secondary:



The screenshot shows a window titled "Edit Flow: SIP Trunk 1_Flow" with a close button in the top right corner. Below the title bar is a section labeled "Criteria" containing a table of configuration fields. The fields are as follows:

Criteria	
Flow Name	CL-Secondary-Flow
Server Configuration	CL-Secondary
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside_92
Media Interface	Media_Outside_92
End Point Policy Group	SIP Trunk_DomPolicy
Routing Profile	Route_to_CM-Lab1
Topology Hiding Profile	SIP Trunk
File Transfer Profile	None

At the bottom of the table is a "Finish" button.

The following screen shows the Server Flow for CL-InboundOnly-Flow:

Criteria	
Flow Name	CL-InboundOnly-Flow
Server Configuration	CL-InboundOnly
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Inside
Signaling Interface	Sig_Outside_92
Media Interface	Media_Outside_92
End Point Policy Group	SIP Trunk_DomPolicy
Routing Profile	Route_to_CM-Lab1
Topology Hiding Profile	SIP Trunk
File Transfer Profile	None

Finish

The following screen shows the Sever Flow for Communication Manager:

Criteria	
Flow Name	CM-Lab1-Flow
Server Configuration	CM-Lab1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_92
Signaling Interface	Sig_Inside
Media Interface	Media_Inside
End Point Policy Group	Enterprise_DomPolicy
Routing Profile	Route_to_CenturyLink
Topology Hiding Profile	Enterprise
File Transfer Profile	None

Finish

7. CenturyLink SIP Trunk Service Configuration

To use CenturyLink SIP Trunk Service, a customer must request the service from CenturyLink using their sales processes. This process can be initiated by contacting CenturyLink via the corporate web site at www.centurylink.com and requesting information via the online sales links or telephone numbers

8. Verification and Troubleshooting

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

8.1. Verification

The following steps may be used to verify the configuration:

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

Use the SAT interface on Communication Manager to verify status of SIP trunks. Specifically use the **status trunk n** command to verify the active call has ended. Where **n** is the trunk group number used for CenturyLink SIP Trunk service 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

8.2. Troubleshooting

1. Communication Manager:

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

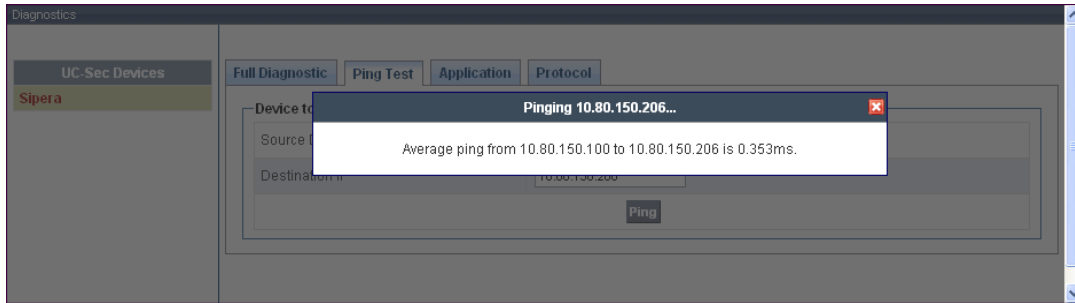
4

5

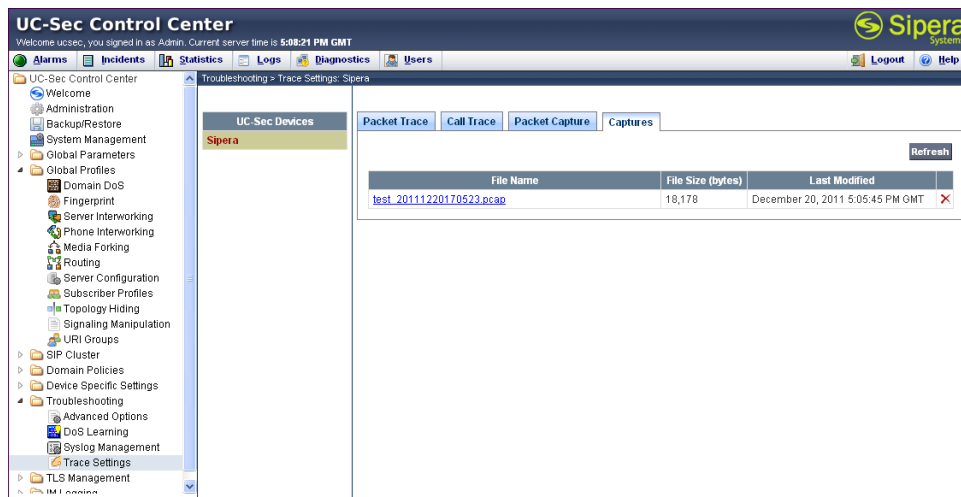
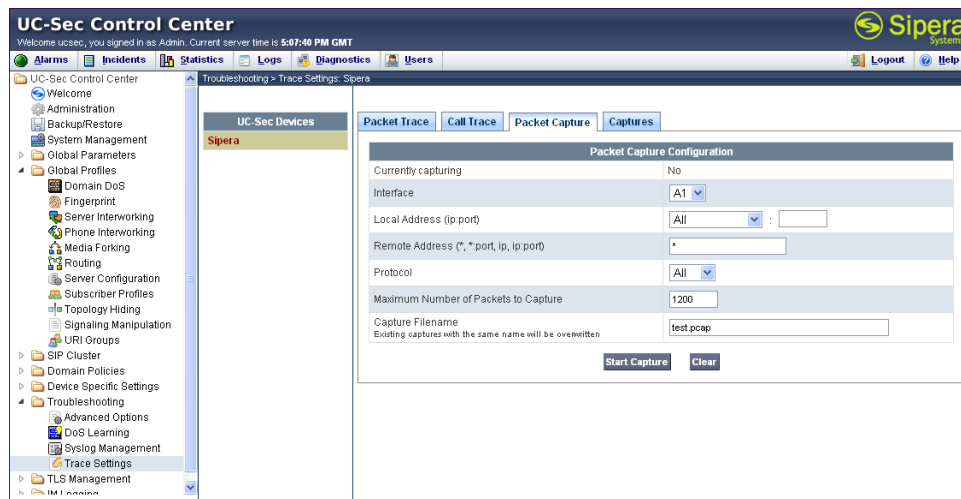
>

>>

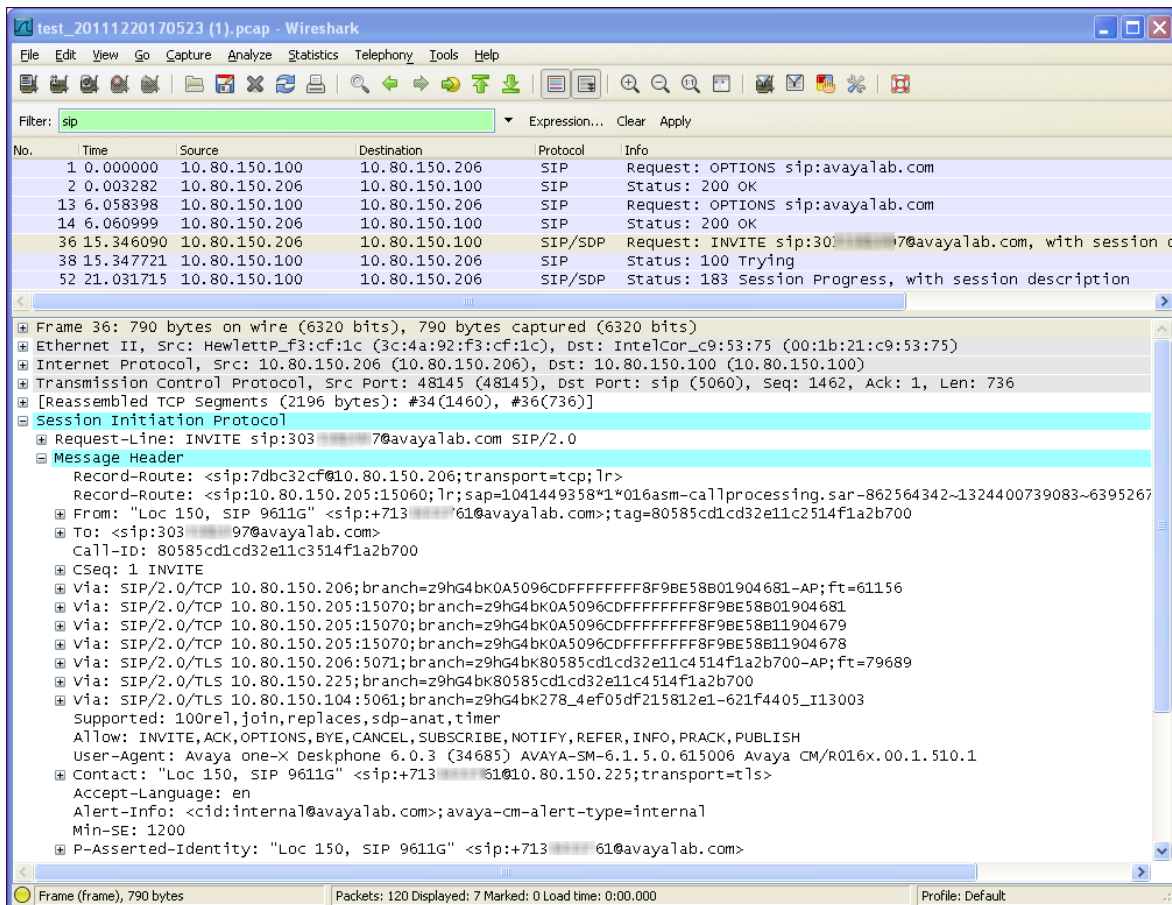
- **Diagnostics** – Allows for PING tests and displays application and protocol use.



- **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 like Wireshark:



9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager Access Element Server and Avaya Session Border Controller for Enterprise to the CenturyLink SIP Trunk Service (Legacy Qwest). The CenturyLink SIP Trunk Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. The CenturyLink SIP Trunk Service provides businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

10. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>. Sipera 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] *Avaya 1600 Series IP Deskphones Administrator Guide Release 1.3.x*, April 2010, Document Number 16-601443.
- [6] *4600 Series IP Telephone LAN Administrator Guide*, July 2008, Document Number 555-233-507.
- [7] *Avaya one-X Deskphone H.323 Administrator Guide*, May 2011, Document Number 16-300698.
- [8] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1*, December 2010, Document Number 16-603838
- [9] *Administering Avaya one-X Communicator*, July 2011
- [10] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3, Document Number 03-300509.
- [11] *Feature Description and Implementation for Avaya Communication Manager, Issue 5*, Document Number 555-245-205
- [12] *UC-Sec Install Guide (102-5224-400v1.01)*
- [13] *UC-Sec Administration Guide (010-5423-400v106)*
- [14] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [15] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [16] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [17] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

©2013 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.