



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise 4.0.5 with CenturyLink SIP Trunk (Sonus Platform) – Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk and Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5.

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.....	3
2.	General Test Approach and Test Results.....	3
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	4
2.3.	Support	5
3.	Reference Configuration	5
4.	Equipment and Software Validated	7
5.	Configure Avaya Aura® Communication Manager.....	8
5.1.	Licensing and Capacity	8
5.2.	System Features.....	9
5.3.	IP Node Names.....	10
5.4.	Codecs	10
5.5.	IP Interface for procr	11
5.6.	IP Network Region.....	11
5.7.	Signaling Group	12
5.8.	Trunk Group.....	14
5.9.	Inbound Routing.....	16
5.10.	Calling Party Information.....	17
5.11.	Outbound Routing	18
5.12.	Saving Communication Manager Configuration Changes	21
6.	Configure Avaya Aura® Session Manager	22
6.1.	Avaya Aura® System Manager Login and Navigation	22
6.2.	Specify SIP Domain	23
6.3.	Add Location.....	24
6.4.	Adaptations.....	27
6.5.	Add SIP Entities	29
6.6.	Add Entity Links	33
6.7.	Add Routing Policies	34
6.8.	Add Dial Patterns	35
6.9.	Add/Verify Avaya Aura® Session Manager Instance	38
7.	Configure Avaya Session Border Controller for Enterprise	40
7.1.	Network Management	43
7.2.	Routing Profile	44
7.3.	Topology Hiding Profile	46
7.4.	Server Interworking Profile.....	48
7.4.1.	Server Interworking Profile – Enterprise	48
7.4.2.	Server Interworking Profile – CenturyLink	51
7.5.	Server Configuration.....	53
7.5.1.	Server Configuration – Session Manager	53
7.5.2.	Server Configuration - CenturyLink	56

7.6.	Media Rule	61
7.7.	Signaling Rule	63
7.8.	Application Rule	65
7.9.	Endpoint Policy Group.....	66
7.10.	Media Interface.....	68
7.11.	Signaling Interface.....	69
7.12.	End Point Flows - Server Flow.....	69
8.	CenturyLink SIP Trunk Configuration	73
9.	Verification and Troubleshooting	73
9.1.	Verification.....	73
9.2.	Troubleshooting	74
10.	Conclusion	77
11.	Additional References.....	78

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink SIP Trunk using Sonus NBS version 7.3.5 and Avaya Aura® Communication Manager Evolution Server 6.2, Avaya Aura® Session Manager 6.2, and Avaya Session Border Controller for Enterprise 4.0.5. CenturyLink can offer SIP trunk service using several different platform technologies in the CenturyLink network. These Application Notes correspond to the SIP trunk service offered using a Sonus platform in the network.

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

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, Session Manager and Avaya Session Border Controller for Enterprise (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**.

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

2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types. Phone types included H.323, SIP, 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, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X Communicator (soft client)
- Avaya one-X Communicator supports two modes (Road Warrior and Telecommuter). Each supported mode was tested. Avaya one-X Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Each supported protocol was tested.
- 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
- Off-net call forwarding and mobility (extension to cellular)

Items not supported or not tested included the following:

- Avaya one-X Communicator Telecommuter using the SIP protocol

2.2. Test Results

Interoperability testing of CenturyLink SIP Trunk Service 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 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.

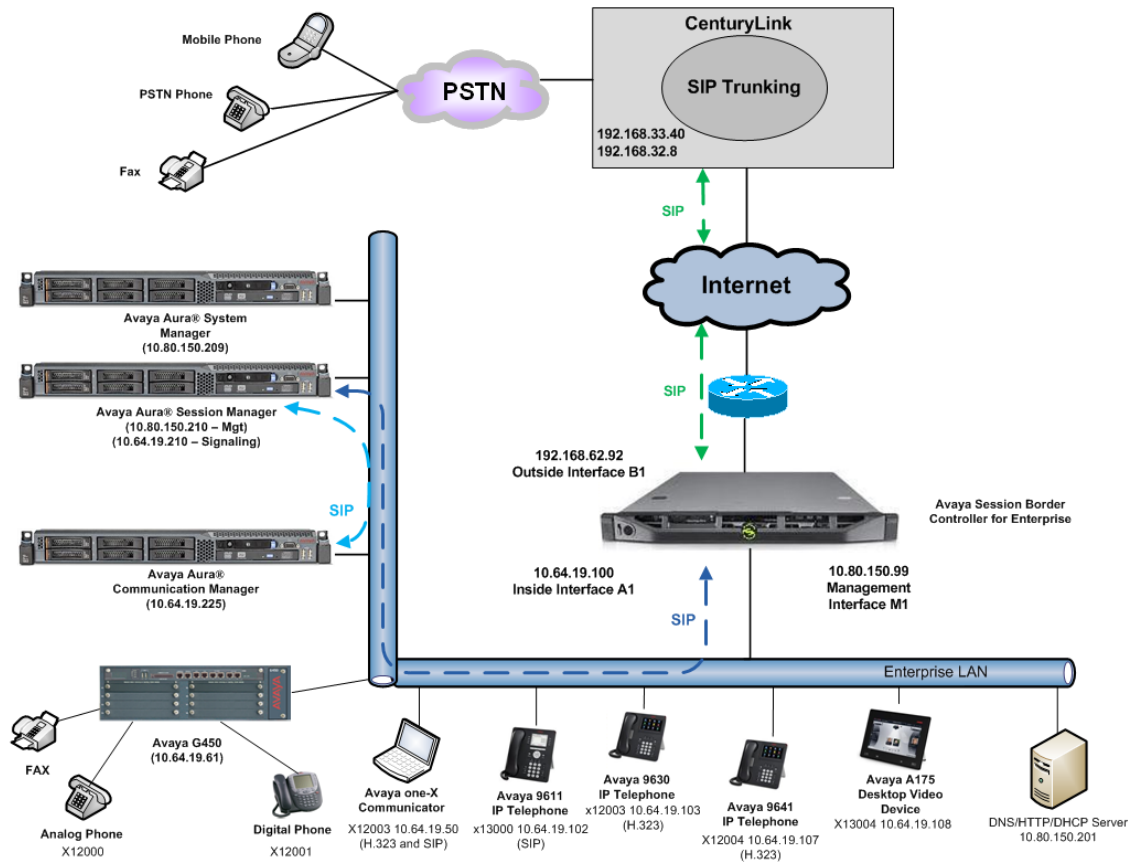


Figure 1: Avaya Interoperability Test Lab Configuration

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.02.0.823.0 -20001
Avaya Aura® Communication Manager Messaging	6.2-22.0
Avaya Aura® System Manager	6.2.0 – SP3
Avaya Aura® Session Manager	6.2.3.0.623006
Avaya Session Border Controller for Enterprise	4.0.5Q19
Avaya G450	31.22.0
Avaya A175 Desktop Video Device	Avaya Flare® Experience 1.1
Avaya 9641 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 6.2009
Avaya 9630 IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.104S
Avaya 9611 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.2.0.72
Avaya 9608 IP Telephone (SIP)	Avaya one-X® Deskphone Edition 6.2.0.72
Avaya one-X® Communicator	6.1.5.07-SP5-37495
Avaya 2420 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
CenturyLink SIP Trunking Solution Components	
Component	Release
NBS	07.03.05

Table 1: Equipment and Software Tested

The specific configuration above was used for the compatibility testing.

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

5. Configure Avaya Aura® Communication Manager

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

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 **290** 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	4	
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:		36000	3	
Maximum Video Capable IP Softphones:		18000	1	
Maximum Administered SIP Trunks:		12000	290	
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	2	
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 **display node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and for Session Manager (**SM**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

display node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
CMM	10.64.19.205	
SM	10.64.19.210	
default	0.0.0.0	
procr	10.64.19.205	
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		
	Mode	Redundancy
FAX	t.38-standard	0
Modem	off	0
TDD/TTY	US	3

5.5. IP Interface for procr

The **add ip-interface procr** or **change ip-interface procr** command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

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

```

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

```

change ip-network-region 2                                     Page 4 of 20

Source Region: 2           Inter Network Region Connection Management
dst codec direct WAN-BW-limits Video Intervening Dyn A G t
rgn set WAN Units Total Norm Prio Shr Regions CAC R L e
1 2 y NoLimit n
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 the recommended default value of **tls** (Transport Layer Security). Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid unused port instead of the default well-known port value. (For TLS, the well-known port value is 5061). The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer Server** field will initially be set to **Others** and cannot be changed via administration. The Peer Server field will automatically change to **SM** once Communication Manager detected a Session Manager peer.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP address of Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **SM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.6**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Initial IP-IP Direct Media?** to **y**. This will minimize the number of SIP messages used by Communication Manager in establishing calls by allowing the RTP media to be initially connected to the IP endpoint rather than the G450 VoIP engine.
- Default values may be used for all other fields.

add signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		SIP Enabled LSP? n
IP Video? n		Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM	
Near-end Listen Port: 5081	Far-end Listen Port: 5081	
	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? y	
	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 2 was configured using the parameters highlighted below.

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

```
add trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                                     Group Type: sip          CDR Reports: y
  Group Name: SIP SP 2                             COR: 1                TN: 1          TAC: *02
  Direction: two-way                               Outgoing Display? n
  Dial Access? n                                    Night Service:
  Queue Length: 0
  Service Type: public-ntwrk                       Auth Code? n
                                                  Member Assignment Method: auto
                                                  Signaling Group: 2
                                                  Number of Members: 10
```

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval** is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

```
add trunk-group 2                                     Page 2 of 21
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: auto
                                     Redirect On OPTIM Failure: 5000
  SCCAN? n                                     Digital Loss Group: 18
                                     Preferred Minimum Session Refresh Interval(sec): 600
Disconnect Supervision - In? y Out? y
```

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

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoints to be replaced with the value set in **Section 5.2**, if the inbound call enabled CPN block. For outbound calls, these same settings request that CPN block be activated on the far-end destination if a local user requests CPN block on a particular call routed out this trunk.

add trunk-group 2		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? n		

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 [13]**. 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. Default values may be used for all other fields.

add trunk-group 2		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		
Block Sending Calling Party Location in INVITE? n		
Enable Q-SIP? n		

5.9. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion using an Adaptation as shown in **Section 6.4**, 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. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were created and tested successfully.

Use the **change inc-call-handling-trmt trunk-group** command to create an entry for any DID numbers unchanged by Session Manager. As an example, the following screen illustrates a conversion of DID numbers **3035557107** and **8555555224** to extension **10000**.

change inc-call-handling-trmt trunk-group 1					Page	1 of	30
INCOMING CALL HANDLING TREATMENT							
Service/	Number	Number	Del		Insert		
Feature	Len	Digits					
public-ntwrk	10	3035557107	10	10000			
public-ntwrk	10	8555555224	10	10000			

5.10. Calling Party Information

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

In the bolded row shown in the example 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 2.

change public-unknown-numbering 5 ext-digits 12000 trunk-group 2					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	CPN Len	Total
5	12000	2	3035557106	10	Total Administered: 17
5	12001	2	3035557107	10	Maximum Entries: 9999
5	12003	2	3035557108	10	
5	12004	2	3035557104	10	Note: If an entry applies to a SIP connection to Avaya Aura(R) Session Manager, the resulting number must be a complete E.164 number.
5	12005	2	3035557105	10	
5	13000	2	6145555685	10	
5	13001	2	6145555686	10	
5	13002	2	6145555687	10	
5	13004	2	6145555688	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:		

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

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

change ars analysis 1							
ARS DIGIT ANALYSIS TABLE							
Location: all							
Percent Full: 0							
	Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
12		11	11	1	fnpa		n
13		11	11	1	fnpa		n
14		11	11	1	fnpa		n
15		11	11	1	fnpa		n
16		11	11	1	fnpa		n
17		11	11	1	fnpa		n
18		11	11	1	fnpa		n
19		11	11	1	fnpa		n
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 **2** was used.
- **FRL:** Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- **Pfx Mrk: 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 HNP 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		
								Dgts						Intw	
1:	2	0	1									n	user		
2:											n	user			
3:											n	user			
4:											n	user			
5:											n	user			
6:											n	user			
BCC VALUE				TSC	CA-TSC		ITC BCIE Service/Feature PARM				No. Numbering	LAR			
0	1	2	M	4	W	Request							Dgts Format		
												Subaddress			
1:	y	y	y	y	y	n	n	rest						none	
2:	y	y	y	y	y	n	n	rest						none	
3:	y	y	y	y	y	n	n	rest						none	
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	12000	ext	y	n	
3035557107	10	10	10	12001	ext	y	n	
3035557108	10	10	10	12003	ext	y	n	
6145555685	10	10	10	13000	ext	y	n	
6145555686	10	10	10	13001	ext	y	n	
6145555687	10	10	10	13002	ext	y	n	
6145555688	10	10	10	13004	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 Aura® Session Manager

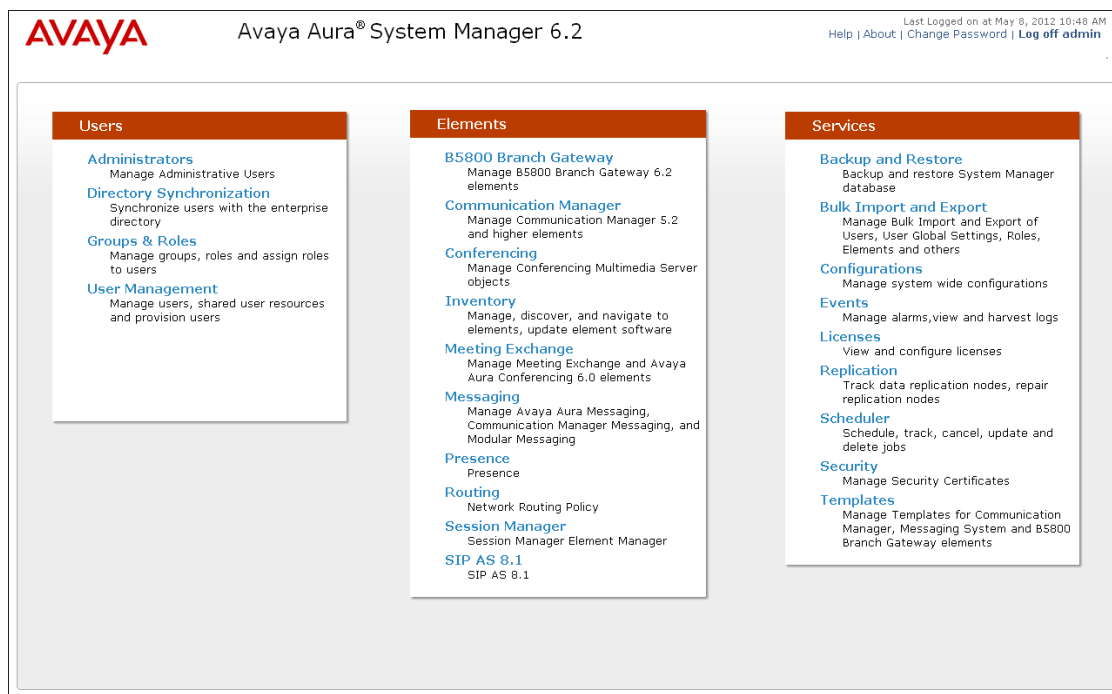
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

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

6.1. Avaya Aura® System Manager Login and Navigation

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



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

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

Routing Home

Home / Elements / Routing Help ?

Introduction to Network Routing Policy

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

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

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

6.2. Specify SIP Domain

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

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

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

Home / Elements / Routing / Domains Help ?

Domain Management

Commit Cancel

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

1 Item | Refresh Filter: Enable

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

6.3. Add Location

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

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

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

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

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

The screenshot displays the 'Add Location' configuration page. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Locations'. The page is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. The 'General' section contains fields for 'Name' (set to 'SessionManager') and 'Notes' (set to 'Session Manager'). The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth', 'Multimedia Bandwidth', and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section includes 'Maximum Multimedia Bandwidth (Intra-Location)' (1000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (1000 Kbit/Sec), '* Minimum Multimedia Bandwidth' (64 Kbit/Sec), and '* Default Audio Bandwidth' (80 Kbit/sec). The 'Alarm Threshold' section includes 'Overall Alarm Threshold' (80 %), 'Multimedia Alarm Threshold' (80 %), '* Latency before Overall Alarm Trigger' (5 Minutes), and '* Latency before Multimedia Alarm Trigger' (5 Minutes). The 'Location Pattern' section has 'Add' and 'Remove' buttons, a table with 0 items, a 'Refresh' button, and a 'Filter: Enable' option. The table header shows 'IP Address Pattern' and 'Notes'.

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

Repeat the preceding procedure to create a separate Location for Communication Manager and Avaya SBCE. Displayed below is the screen for **Loc19-CMLab** used for Communication Manager.

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

[Help ?](#)

Location Details

Commit

Cancel

General

*** Name:**

Loc19-CMLab

Notes:

Lab CM 10.64.19.205

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

*** Minimum Multimedia Bandwidth:**

64

Kbit/Sec

*** Default Audio Bandwidth:**

80

Kbit/sec

Below is the screen for **Loc19-ASBCE** used for Avaya SBCE.

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

[Help ?](#)

Location Details

Commit

Cancel

General

*** Name:**

Loc19-ASBCE

Notes:

Location 19 Avaya SBC

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

*** Minimum Multimedia Bandwidth:**

64

Kbit/Sec

*** Default Audio Bandwidth:**

80

Kbit/sec

6.4. Adaptations

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

The following screen shows the adaptations that were available in the sample configuration.

Home / Elements / Routing / Adaptations [Help ?](#)

Adaptations

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#)

6 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input checked="" type="checkbox"/>	Loc19-CM-Lab Adaptation	DigitConversionAdapter fromto=true		Convert 10 digit DID to Ext.
<input type="checkbox"/>	Remove+	DigitConversionAdapter fromto=true		Remove +

Select : All, None

The adapter named **Loc19-CM-Lab Adaptation** will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving CenturyLink SIP Trunking. This adaptation uses the **DigitConversionAdapter** to convert digits between Communication Manager and CenturyLink. The **Module parameter fromto=true** will include the FROM and TO headers in the digit conversion.

Home / Elements / Routing / Adaptations [Help ?](#)

Adaptation Details [Commit](#) [Cancel](#)

General

* **Adaptation name:**

Module name:

Module parameter:

Egress URI Parameters:

Notes:

Scrolling down, the following screen shows a portion of the **Loc19-CM-Lab Adaptation** adapter that can be used to convert digits between the Communication Manager extension numbers (user extensions, VDNs) and the DID numbers assigned by CenturyLink.

An example portion of the settings for **Digit Conversion for Outgoing Calls from SM** (i.e., inbound to Communication Manager) is shown below. Both Session Manager digit conversion and Communication Manager incoming call handling treatment methods were created and tested successfully.

Digit Conversion for Outgoing Calls from SM

Add
Remove

8 Items
Refresh
Filter: Enable

<input type="checkbox"/>	Matching Pattern ^	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	* 3035557104	* 10	* 10		* 10	12004	both	
<input type="checkbox"/>	* 3035557105	* 10	* 10		* 10	12005	both	
<input type="checkbox"/>	* 3035557106	* 10	* 10		* 10	12000	both	
<input type="checkbox"/>	* 3035557108	* 10	* 10		* 10	12003	both	
<input type="checkbox"/>	* 6145555685	* 10	* 10		* 10	13000	both	
<input type="checkbox"/>	* 6145555686	* 10	* 10		* 10	13001	both	
<input type="checkbox"/>	* 6145555687	* 10	* 10		* 10	13002	both	
<input type="checkbox"/>	* 6145555688	* 10	* 10		* 10	13004	both	

Select : All, None

* Input Required
Commit
Cancel

6.5. Add SIP Entities

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

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

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

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

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Credential name:

SIP Link Monitoring

SIP Link Monitoring:

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

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

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

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

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

Port

TCP Failover port:

TLS Failover port:

4 Items | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5081"/>	TLS <input type="button" value="v"/>	<input type="text" value="avayalab.com"/> <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5071"/>	TLS <input type="button" value="v"/>	<input type="text" value="avayalab.com"/> <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP <input type="button" value="v"/>	<input type="text" value="avayalab.com"/> <input type="button" value="v"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS <input type="button" value="v"/>	<input type="text" value="avayalab.com"/> <input type="button" value="v"/>	<input type="text"/>

Select : [All](#), [None](#)

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

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

- Name:** Loc19-CM-TG2
- * FQDN or IP Address:** 10.64.19.205
- Type:** CM (dropdown menu)
- Notes:** CM Trunk Group 2 for SP Trunks
- Adaptation:** Loc19-CM-Lab Adaptation (dropdown menu)
- Location:** Loc19-CMLab (dropdown menu)
- Time Zone:** America/Denver (dropdown menu)
- Override Port & Transport with DNS SRV:** ☐
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (dropdown menu)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown menu)

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

[Home](#) / [Elements](#) / [Routing](#) / [SIP Entities](#)

[Help ?](#)

SIP Entity Details

Commit

Cancel

General

* Name:

Loc19-ASBCE

* FQDN or IP Address:

10.64.19.100

Type:

Other

Notes:

Avaya SBC

Adaptation:

Location:

Loc19-ASBCE

Time Zone:

America/Denver

Override Port & Transport with DNS SRV:

☐

* SIP Timer B/F (in seconds):

4

Credential name:

Call Detail Recording:

none

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring:

Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds):

900

* Reactive Monitoring Interval (in seconds):

120

* Number of Retries:

1

6.6. Add Entity Links

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

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

Click **Commit** to save. The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE.

Entity Link to Communication Manager:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to Loc19-CM TG2	* DenverSM	TLS	* 5081	* Loc19-CM-TG2	* 5081	Trusted	For PSTN SIP Trunk

Entity Link to Avaya SBCE:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* SM to Loc19-ASBCE	* DenverSM	TCP	* 5060	* Loc19-ASBCE	* 5060	Trusted	To Avaya SBC

6.7. Add Routing Policies

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

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

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

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

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

Routing Policy for Communication Manger:

Home / Elements / Routing / Routing Policies

Routing Policy Details

Help ?

Commit Cancel

General

* Name: To-CM-TG2

Disabled: ☐

* Retries: 0

Notes: To CM Trunk Group 2 (SP Trunk)

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Loc19-CM-TG2	10.64.19.205	CM	CM Trunk Group 2 for SP Trunks

Routing Policy for Avaya SBCE:

Home / Elements / Routing / Routing Policies

Routing Policy Details

Help ?

Commit Cancel

General

* Name: To-ASBCE

Disabled: ☐

* Retries: 0

Notes: To Avaya SBCE

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Loc19-ASBCE	10.64.19.100	Other	Avaya SBC

6.8. Add Dial Patterns

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

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

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

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

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

Two examples of the dial patterns used for the compliance test are shown below. The first example shows that in the shared test environment, 11 digit dialed numbers that begin with 1 originating from **Loc19-CMLab** uses route policy **To-ASBCE**.

Home / Elements / Routing / Dial Patterns

Help ?

Dial Pattern Details

Commit
Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call:
☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add
Remove

2 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CS1K-Location	CS1000 lab 140	To-ASBCE	0	<input type="checkbox"/>	Loc19-ASBCE	
<input type="checkbox"/>	Loc19-CMLab	Lab CM 10.64.19.205	To-ASBCE	0	<input type="checkbox"/>	Loc19-ASBCE	

Select : All, None

The second example shows that a **10** digit number starting with **30355571** and originating from **Loc19-ASBCE** uses route policy **To-CM-TG2**. This is a DID range 303-555-7100 through 303-555-7199 assigned to the enterprise from CenturyLink.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details
[Help ?](#)

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item | [Refresh](#)
Filter: [Enable](#)

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Loc19-ASBCE	Location 19 Avaya SBC	To-CM-TG2	0	<input type="checkbox"/>	Loc19-CM-TG2	To CM Trunk Group 2

Select : All, None

6.9. Add/Verify Avaya Aura® Session Manager Instance

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

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

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

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

Home / Elements / Session Manager

Edit Session Manager [Help ?](#)

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

General ▾

SIP Entity Name DenverSM

Description

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

***Direct Routing to Endpoints** ▾

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

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

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

Security Module ▼

SIP Entity IP Address

10.64.19.210

*Network Mask

255.255.255.0

*Default Gateway

10.64.19.1

*Call Control PHB

46

*QOS Priority

6

*Speed & Duplex

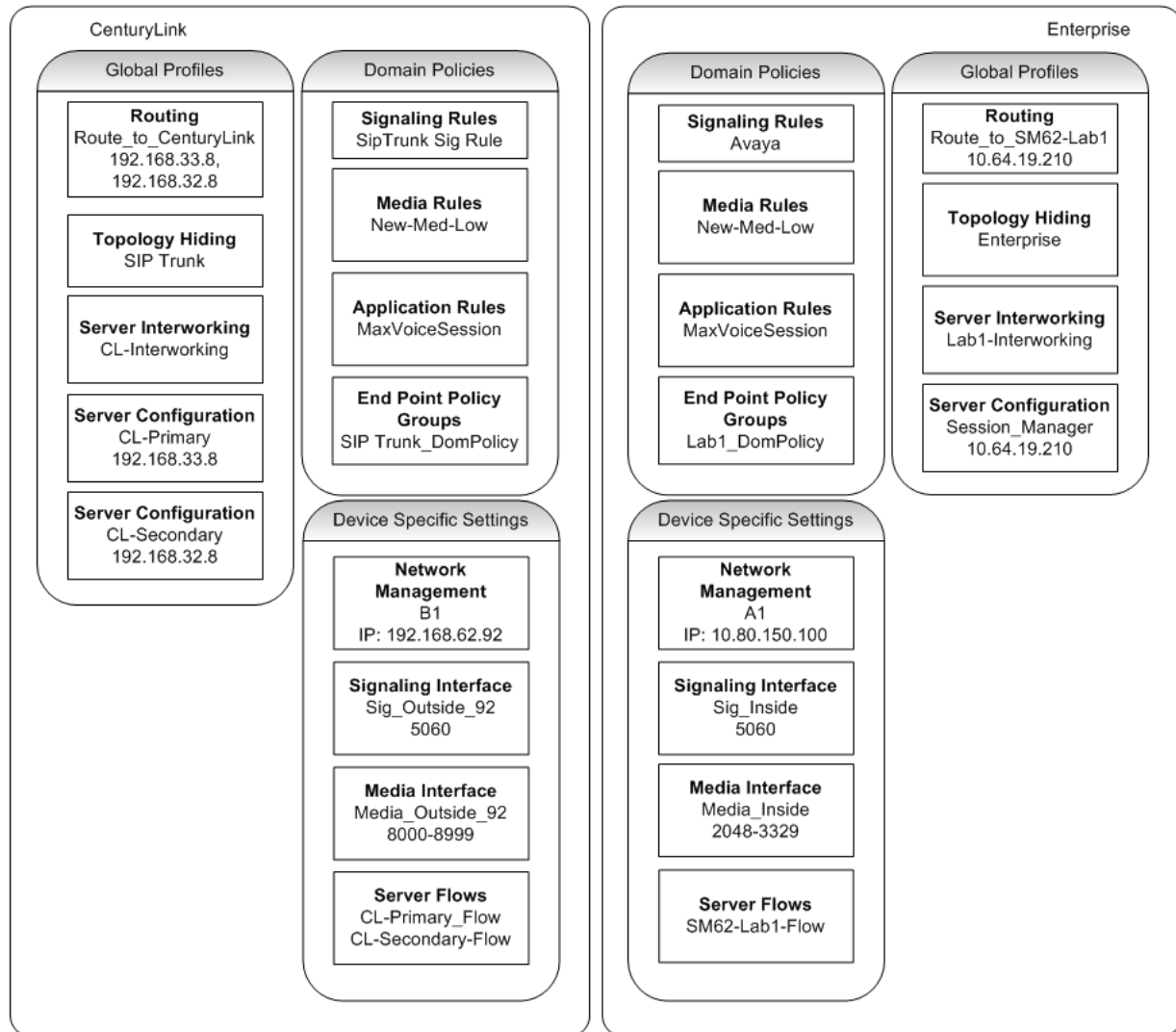
Auto ▼

VLAN ID

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed.

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 Element Management Server (EMS) web interface, and enter `https://<ip-addr>/ucsec` in the address field of the web browser, where `<ip-addr>` is the management LAN IP address of the Avaya SBCE.

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 6:24:08 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.

Quick Links

- [Sipera Website](#)
- [Sipera VIPER Labs](#)
- [Contact Support](#)

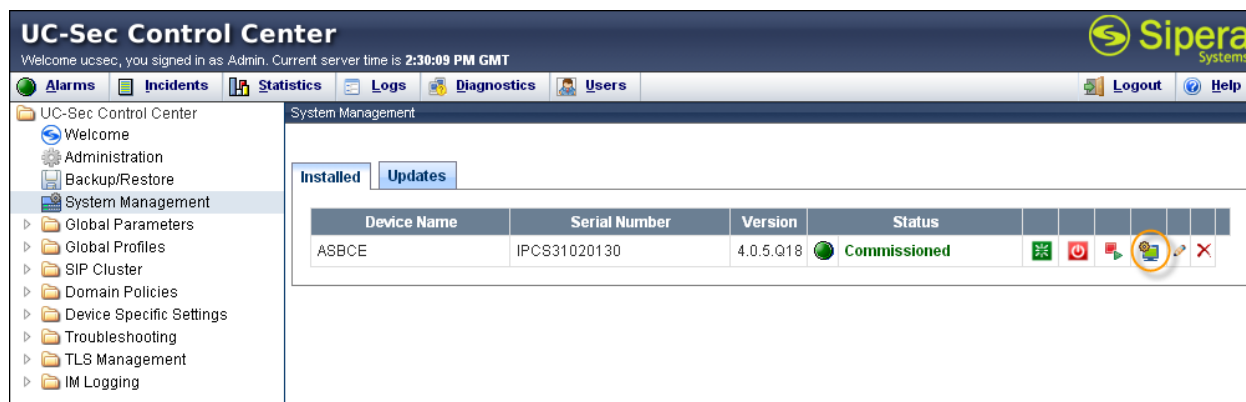
UC-Sec Devices	Network Type
ASBCE	DMZ_ONLY

Alarms (Past 24 Hours)
None found.

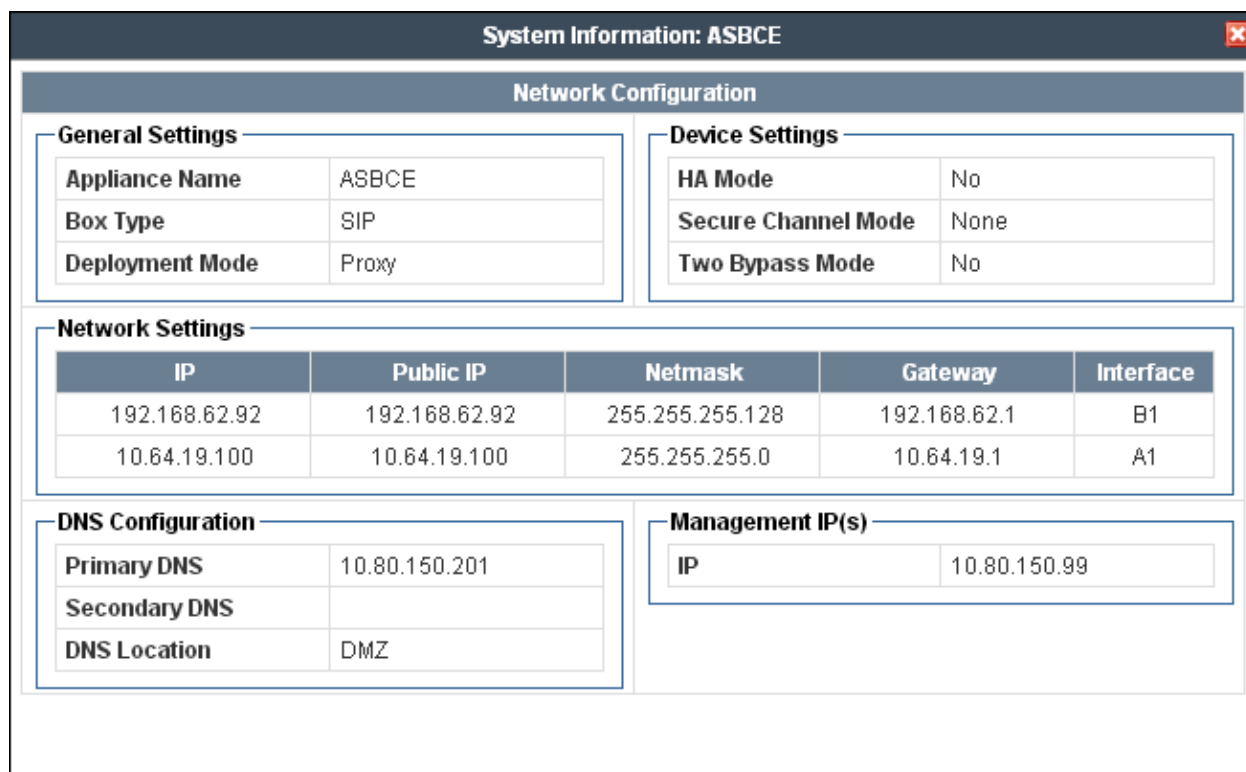
Incidents (Past 24 Hours)
None found.

Administrator Notes [Add]
No notes posted.

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 **ASBCE** is shown. To view the configuration of this device, click the monitor icon as shown below.

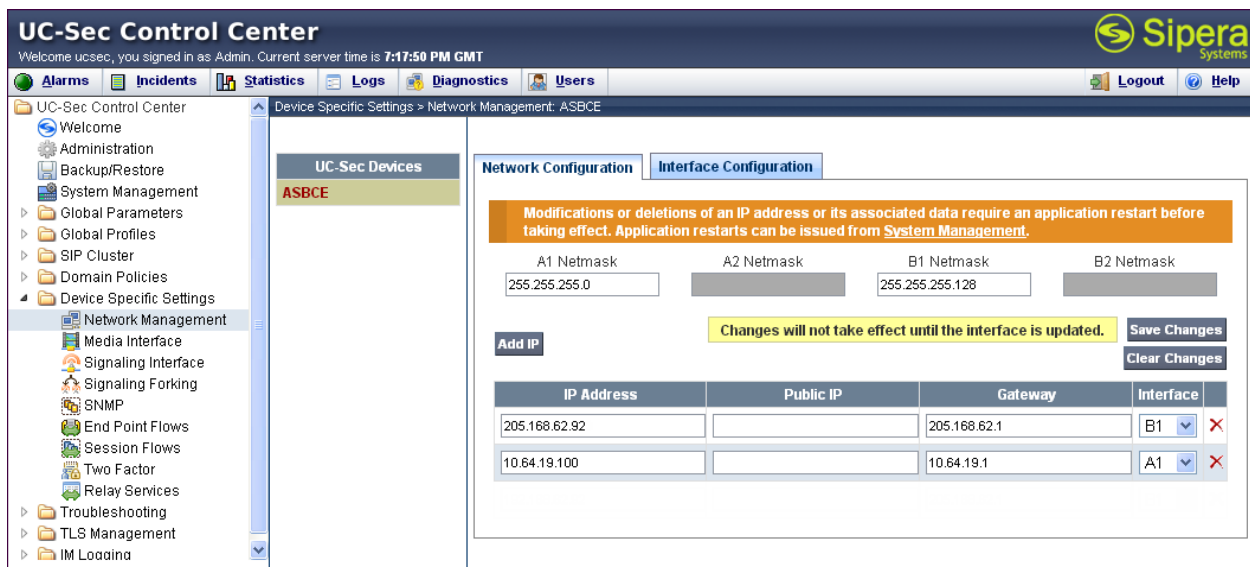


The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all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



7.1. Network Management

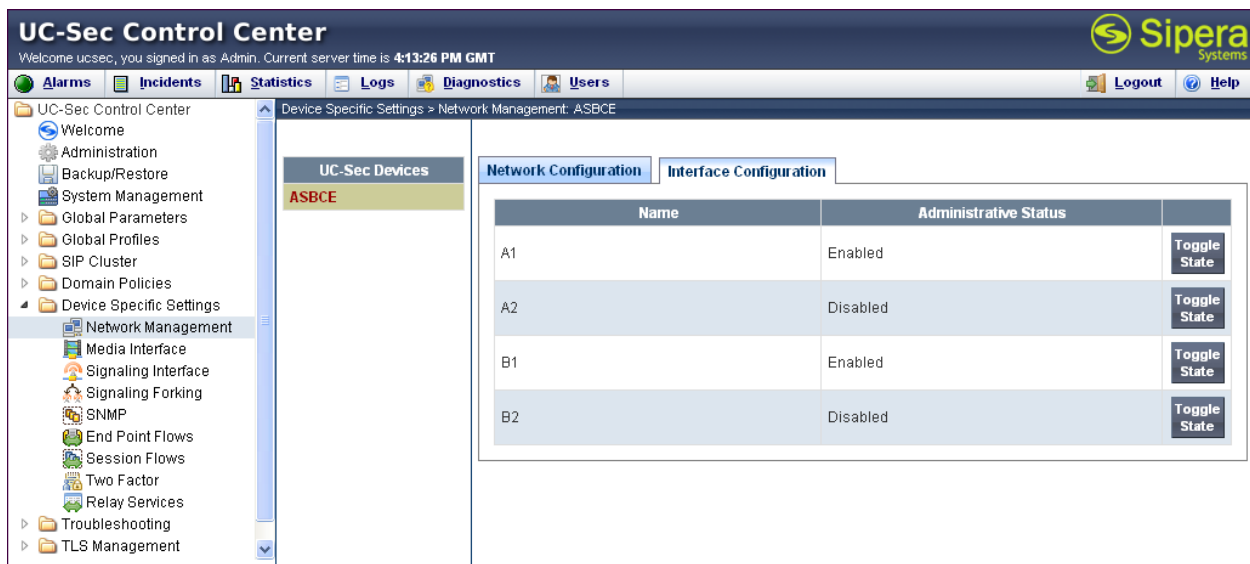
The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the external interface is assigned to **B1**.



The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Device Specific Settings' expanded to show 'Network Management'. The main panel is titled 'Device Specific Settings > Network Management: ASBCE'. It has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are input fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.128), and 'B2 Netmask'. There are 'Add IP', 'Save Changes', and 'Clear Changes' buttons. A table lists IP configurations:

IP Address	Public IP	Gateway	Interface	
205.168.62.92		205.168.62.1	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 its **Toggle State** button.



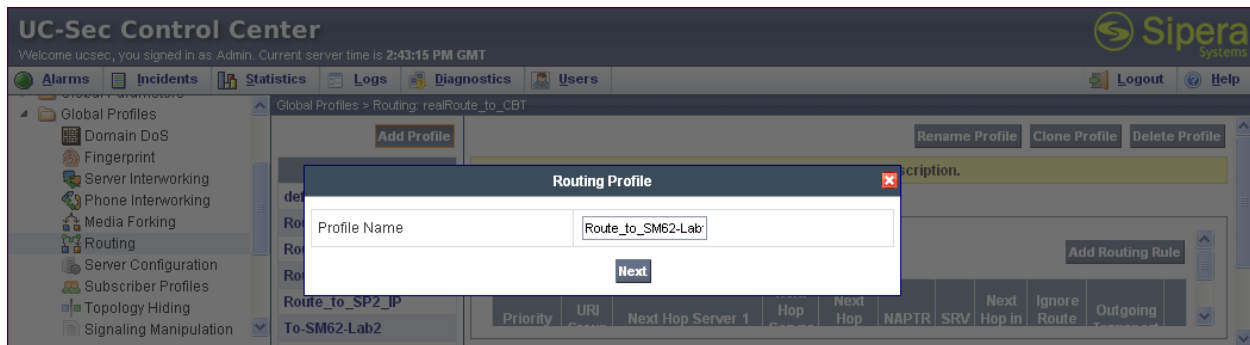
The screenshot shows the UC-Sec Control Center interface, specifically the 'Interface Configuration' tab. The left sidebar is the same as the previous screenshot. The main panel is titled 'Device Specific Settings > Network Management: ASBCE'. It has two tabs: 'Network Configuration' and 'Interface Configuration' (active). A table lists the interfaces and their administrative status:

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

7.2. Routing Profile

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

Create a Routing Profile for Session Manager and CenturyLink SIP Trunk Service. 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.



In the new window that appears, enter the following values (not shown). Use default values for all remaining fields:

- **URI Group:** Select “*” from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority Based on Next Hop Server:** Checked.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish**.

In the shared test environment the following screen shows the Routing Profile to Session Manager. The **Next Hop Server 1** IP address must match the IP address of Session Manager Entity created in **Section 6.5**. The **Outgoing Transport** is set to **TCP** and matched the **Protocol** set in the Session Manager Entity Link for Avaya SBCE in **Section 6.6**.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 4:52:24 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: Route_to_SM62-Lab1

Add Profile Rename Profile Clone Profile Delete Profile

Click here to add a description.

Routing Profiles

- default
- SP1
- Route_to_CS1K
- Route_to_SM62-Lab1
- Route_to_CM62
- SP2
- remote-test
- Route_to_CenturyLink

Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.64.19.210	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP

The following screen shows the Routing Profile to CenturyLink. In the **Next Hop Server 1** field enter the IP address and port that CenturyLink uses to listen for SIP traffic. Enter **UDP** for the **Outgoing Transport** field.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 4:54:43 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: Route_to_CenturyLink

Add Profile Rename Profile Clone Profile Delete Profile

Click here to add a description.

Routing Profiles

- default
- SP1
- Route_to_CS1K
- Route_to_SM62-Lab1
- Route_to_CM62
- SP2
- remote-test
- Route_to_CenturyLink

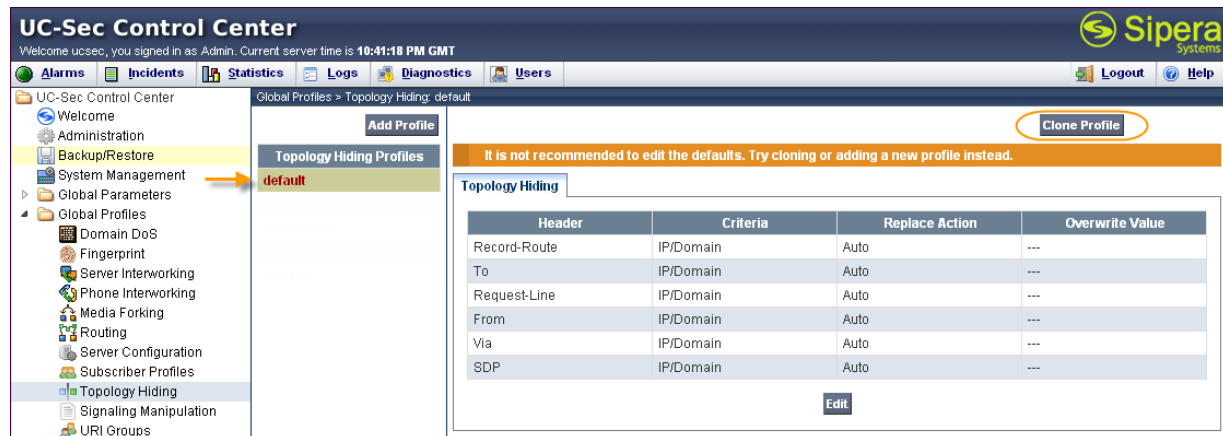
Add Routing Rule

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	192.168.33.8:5060	192.168.32.8:5060	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	UDP

7.3. Topology Hiding Profile

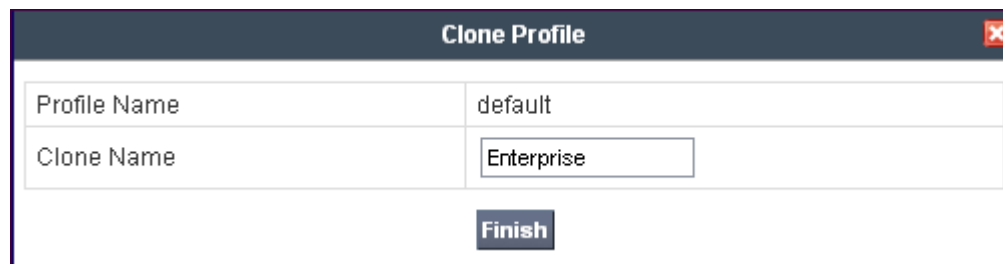
The Topology Hiding profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks.

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



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	---

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



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 Session Manager (**Section 6.2**). Click **Finish** to save the changes.

Edit Topology Hiding Profile ✕

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

Finish

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

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 7:27:43 PM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

- 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
- Troubleshooting
- TLS Management
- IM Logging

Global Profiles > Topology Hiding: SIP Trunk

Add Profile
Rename Profile
Clone Profile
Delete Profile

Topology Hiding Profiles

default

cisco_th_profile

SIP Trunk

Enterprise

Click here to add a description.

Topology Hiding

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

Edit

DDT; Reviewed:
SPOC 5/6/2013

Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

47 of 79
CLCM62SM62ASBCE

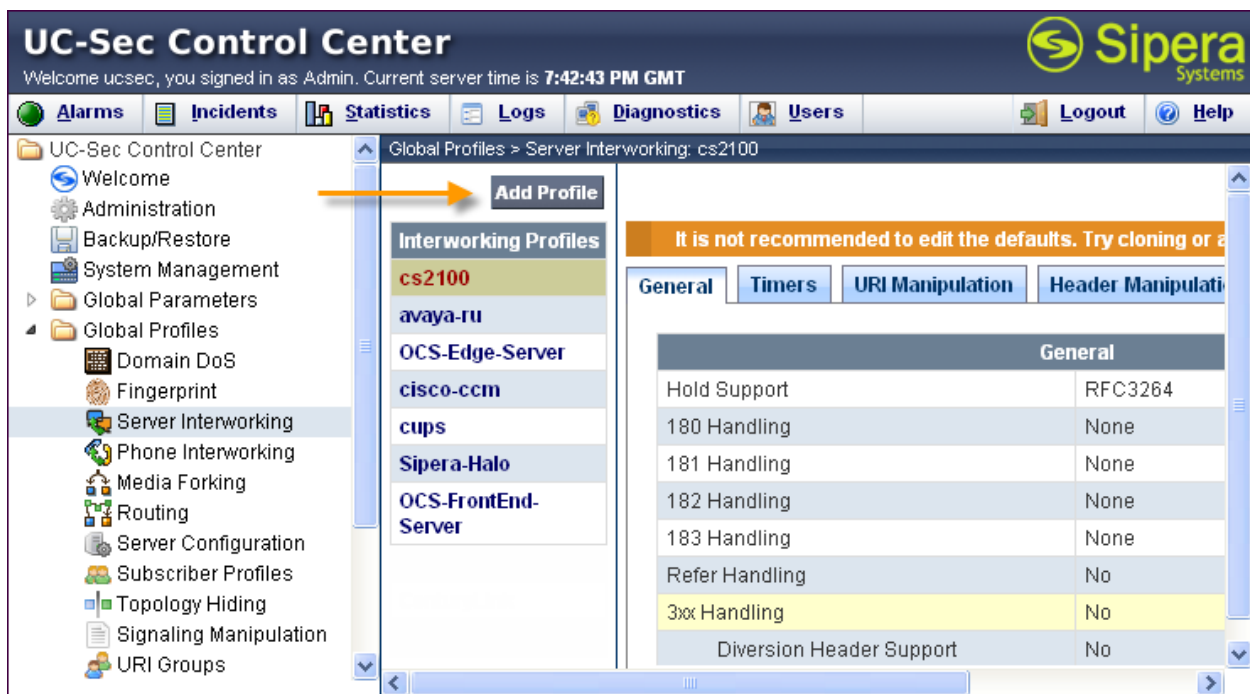
7.4. Server Interworking Profile

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.

7.4.1. Server Interworking Profile – Enterprise

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



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

Interworking Profile

Profile Name

Lab1-Interworking

Next

In the new window that appears, check the **T.38 Support** field. Use default values for all remaining fields. Click **Next** to continue.

Interworking Profile	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
T.38 Support	<input 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

Default values can 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

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]

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

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

Click **Finish** to save changes.

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

Back **Finish**

7.4.2. Server Interworking Profile – CenturyLink

The CenturyLink profile will be created by cloning the Enterprise profile created in the previous section. To clone a Server Interworking Profile for CenturyLink, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking** and click on the previously created profile for the enterprise, then click on **Clone Profile** as shown below.



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

Clone Profile

Profile Name	Lab1-Interworking
Clone Name	CL-Interworking

Finish

Beginning with Communication Manager 6.0 public numbers are automatically preceded with a + sign (E.164 numbering format). CenturyLink does not support the E.164 numbering format, therefore the + sign must be removed. Create a URI Manipulation to remove the + sign
Communication Manager places in the FROM, CONTACT, and P-Asserted Identity headers.

Within the **CL-Interworking** Profile, select the **URI Manipulation** tab and click the **Add Regex** button. The Add Regex screen is presented (not shown). In the **User Regex** field, enter a regular expression to match. In the sample configuration **\+.*** was entered. In this expression the backslash is used to escape the special meaning of “+” in a regular expression. The expression “.*” will match anything after the plus sign. In the **User Action** field, select **Remove prefix** [Value] from the drop-down box. In the **User Values** field enter +. Click **Finish** to save the configuration.

The following screen shows the completed URI Manipulation for CenuryLink.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'Global Profiles' expanded, and 'Server Interworking' selected. The main content area shows the 'CL-Interworking' profile configuration. The 'URI Manipulation' tab is active, displaying a table with one entry:

User Regex	Domain Regex	User Action	Domain Action
\+.*		Remove prefix +	None

The interface also includes buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile' at the top right of the configuration area.

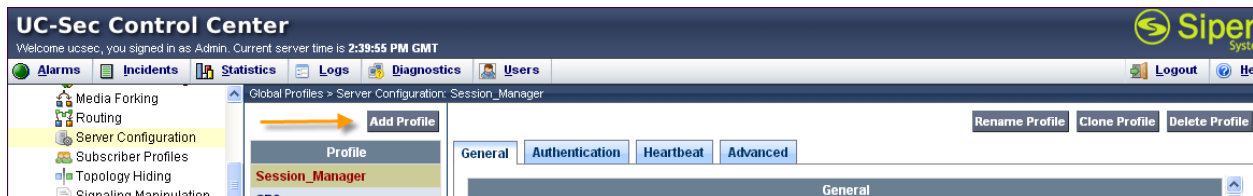
7.5. Server Configuration

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

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

7.5.1. Server Configuration – Session Manager

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



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

The screenshot shows a modal dialog box titled 'Add Server Configuration Profile'. It contains a 'Profile Name' text input field with the value 'Session_Manager' entered. Below the input field is a 'Next' button.

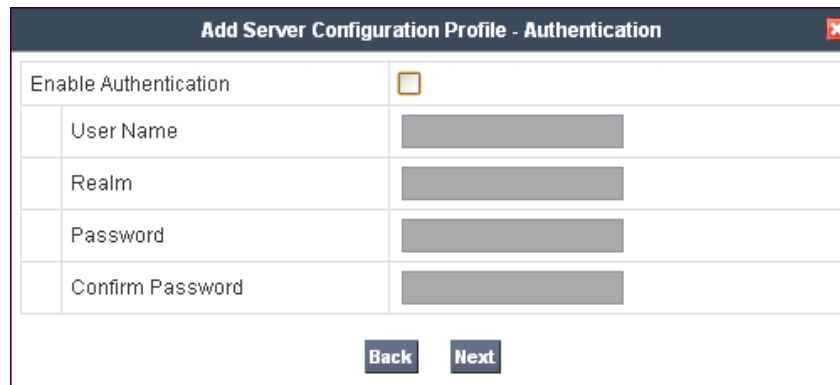
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **Server Type:** Select **Call Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address of Session Manager. This should match the IP address of the SIP Entity for Session Manager in **Section 6.5**.
- **Supported Transports:** Select the transport protocol used to create the Avaya SBCE Entity Link in Session Manager in **Section 6.6**.
- **TCP Port:** Port number on which to send SIP requests to Session Manager. This should match the port number used in the Avaya SBCE Entity Link in Session Manager in **Section 6.6**.

Click **Next** to continue.

Add Server Configuration Profile - General	
Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.64.19.210
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 Session Manager does not require authentication. Click **Next** to continue.

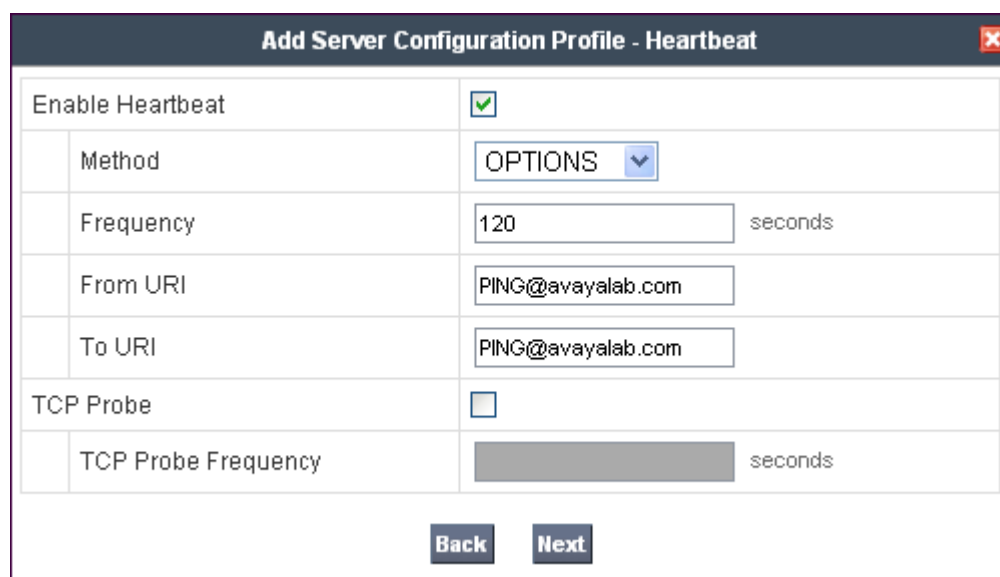


Add Server Configuration Profile - Authentication	
Enable Authentication	<input type="checkbox"/>
User Name	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
<div>Back Next</div>	

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

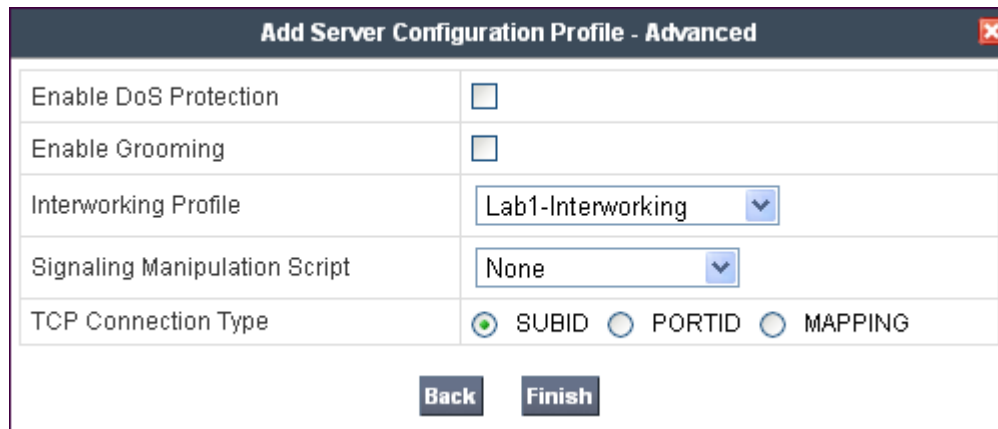
- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS to Session Manager. For compliance testing **120** seconds was chosen.
- **From URI:** Enter an URI to be sent in the 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 <input type="button" value="v"/>
Frequency	120 seconds
From URI	PING@avayalab.com
To URI	PING@avayalab.com
TCP Probe	<input type="checkbox"/>
TCP Probe Frequency	<input type="text"/> seconds
<div>Back Next</div>	

In the new window that appears, select the **Interworking Profile** created for the enterprise in **Section 7.4.1**. Use default values for all remaining fields. Click **Finish** to save the configuration.



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

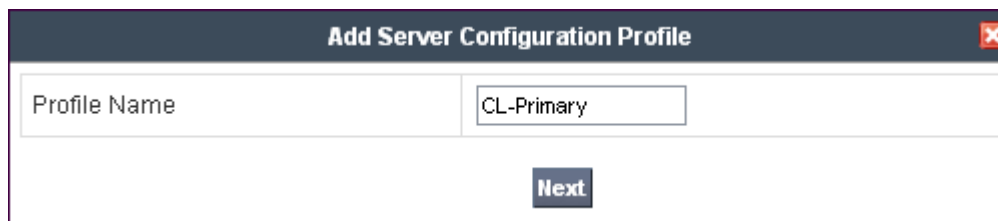
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Lab1-Interworking
Signaling Manipulation Script	None
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

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

7.5.2. Server Configuration - CenturyLink

For compliance testing CenturyLink had two SIP servers assigned for both inbound and outbound traffic; one as the primary and one as the secondary. Separate server configuration profiles were created for the primary and secondary CenturyLink SIP servers.

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**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It contains a single row with a text input field for the "Profile Name".

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

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

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

- **Server Type:** Select **Trunk Server** from the drop-down box.
- **IP Addresses / Supported FQDNs:** Enter the IP address 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 server. This will associate the inbound SIP messages from CenturyLink's SIP server to this Sever Configuration.
- **Supported Transports:** Select the transport protocol to be used for SIP traffic between Avaya SBCE and CenturyLink. For compliance testing **UDP** was used.
- **UDP Port:** Enter the port number that CenturyLink uses to send SIP traffic. For compliance testing **5060** was used.

Click **Next** to continue.

The screenshot shows a window titled "Add Server Configuration Profile - General". It contains the following fields and options:

Server Type	Trunk Server (dropdown)
IP Addresses / Supported FQDNs <small>Comma seperated list</small>	192.168.33.8
Supported Transports	<input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	(disabled text box)
UDP Port	5060
TLS Port	(disabled text box)

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

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	<input type="text"/>
Realm	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Back **Next**

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

- **Enabled Heartbeat:** Checked.
- **Method:** Select **OPTIONS** from the drop-down box.
- **Frequency:** Choose the desired frequency in seconds the Avaya SBCE will send SIP OPTIONS. For compliance testing **60** seconds was chosen.
- **From URI:** Enter an URI to be sent in the FROM header for SIP OPTIONS.
- **TO URI:** Enter an URI to be sent in the TO header for SIP OPTIONS.

Click **Next** to continue.

The SIP OPTIONS are sent to the SIP proxy(ies) entered in the **IP Addresses /Supported FQDNs** in the **Server Configuration Profile**. The URI of PING@CenturyLink.com was used in the sample configuration to better identify the SIP OPTIONS in the call traces. 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

Back Next

In the new window that appears, select the **Interworking Profile** created for CenturyLink in **Section 7.4.2**. 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	CL-Interworking
Signaling Manipulation Script	None
UDP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING

Back Finish

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

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.

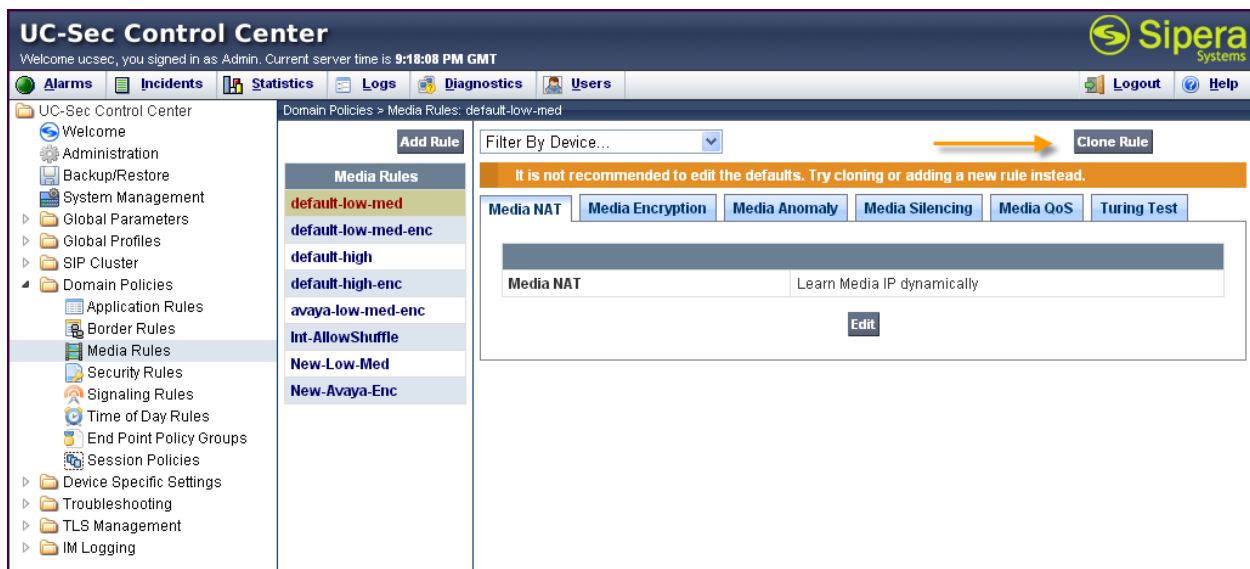
General	
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.32.8
Supported Transports	UDP
UDP Port	5060

7.6. 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 Avaya SBCE 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** was created for CenturyLink SIP Trunk Service and the enterprise.

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	

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

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 3:45:44 PM GMT

Alarms
Incidents
Statistics
Logs
Diagnostics
Users
Logout
Help

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

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

Media Rules
default-low-med
default-low-med-enc
default-high
default-high-enc
avaya-low-med-enc
Int-AllowShuffle
New-Low-Med

Click here to add a description.

Media NATMedia EncryptionMedia AnomalyMedia SilencingMedia QoS Turing Test

Media QoS Reporting

RTCP Enabled
☐

Media QoS Marking

Enabled
☒
QoS Type
DSCP

Audio QoS

Audio DSCP
EF

Video QoS

Video DSCP
EF

Edit

DDT; Reviewed:
SPOC 5/6/2013

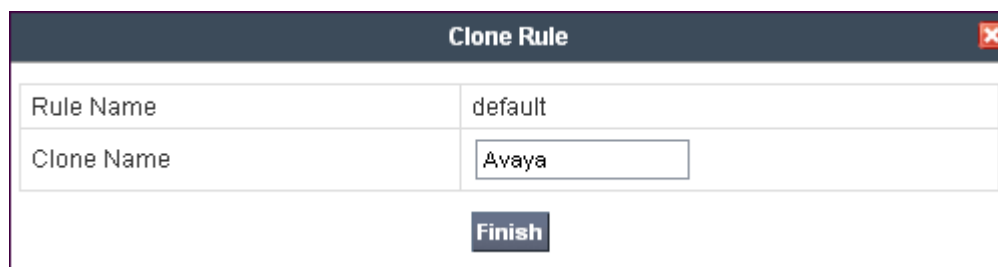
Solution & Interoperability Test Lab Application Notes
©2013 Avaya Inc. All Rights Reserved.

62 of 79
CLCM62SM62ASBCE

7.7. Signaling Rule

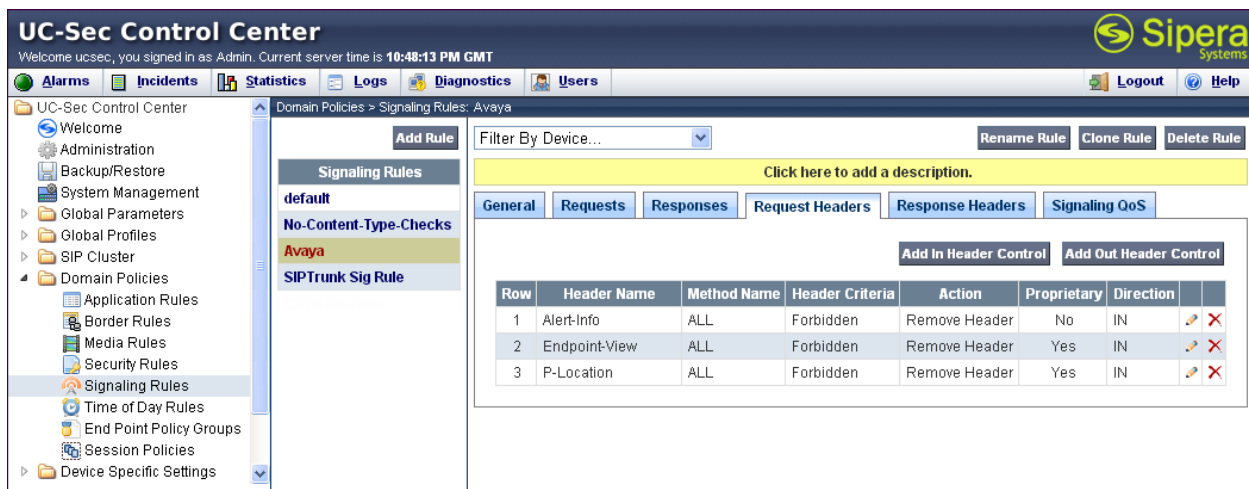
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined 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 remove unnecessary SIP headers and add the proper quality of service to the SIP message. To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** (not shown). Enter a descriptive name for the new rule and click **Finish**.



The image shows a 'Clone Rule' dialog box. It has a title bar with a close button. Inside, there are two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'Avaya'. Below these fields is a 'Finish' button.

In the sample configuration, signaling rule **Avaya** was created for Session Manager to prevent certain headers in the SIP messages sent from Session Manager from being propagated to CenturyLink. Select this rule in the center pane, then select the **Request Headers** tab to view the manipulations performed on the request messages such as the initial INVITE or UPDATE message. The following screen shows the **Alert-Info**, **Endpoint-View**, and **P-Location** headers removed during the compliance test.



The image shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, System Management, SIP Cluster, and Domain Policies. The main area displays the 'Signaling Rules' for the 'Avaya' rule. It includes tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', and 'Signaling QoS'. The 'Request Headers' tab is selected, showing a table of headers to be removed.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	
2	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	
3	P-Location	ALL	Forbidden	Remove Header	Yes	IN	

Similarly, manipulations can be performed on the SIP response messages. These can be viewed by selecting the **Response Headers** tab as shown below.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Domain Policies' expanded. The main area displays 'Signaling Rules' for the 'Avaya' domain. The 'SIPTrunk Sig Rule' is selected, and the 'Response Headers' tab is active. A table lists four response headers:

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	
2	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	
3	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	
4	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	

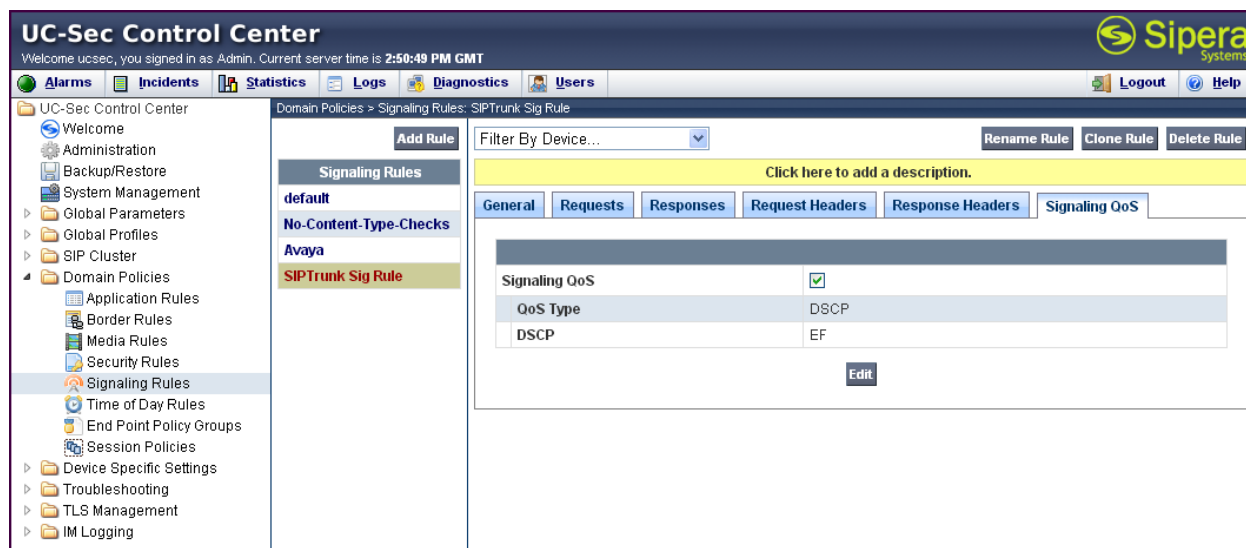
On the **Signaling QoS** tab select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Service policies for signaling. The following screen shows the QoS values used for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

The screenshot shows the UC-Sec Control Center interface. The left sidebar is the same as the previous screenshot. The main area displays 'Signaling Rules' for the 'Avaya' domain. The 'SIPTrunk Sig Rule' is selected, and the 'Signaling QoS' tab is active. The configuration details are as follows:

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

An 'Edit' button is located below the configuration details.

A separate signaling rule **SIPTrunk Sig Rule** was created for CenturyLink SIP Trunk Service by cloning the **default** signaling rule and changing the **Signaling QoS** parameters as shown below.



7.8. Application Rule

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE 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 increase 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** (not shown). Enter a descriptive name for the new rule and click **Finish**.

Clone Rule
✕

Rule Name	default
Clone Name	<input style="width: 90%;" type="text" value="MaxVoiceSession"/>

Finish

Modify the rule by clicking the **Edit** button. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **2000**. Set the values 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 screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration areas, with 'Domain Policies' expanded. The main area displays the 'MaxVoiceSession' Application Rule. The rule is configured with 'Voice' as the Application Type, 'In' and 'Out' checkboxes checked, 'Maximum Concurrent Sessions' set to 2000, and 'Maximum Sessions Per Endpoint' set to 2000. The 'Miscellaneous' section shows 'CDR Support' as None, 'IM Logging' as No, and 'RTCP Keep-Alive' as No. An 'Edit' button is visible at the bottom right of the rule configuration area.

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

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

7.9. Endpoint Policy Group

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in **Section 7.12**. Create a separate Endpoint Policy Group for the enterprise and the CenturyLink SIP Trunk Service.

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

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration areas, with 'Domain Policies' expanded. The main area displays the 'default-low' Endpoint Policy Group. The group is configured with 'Order' 1, 'Application' default, 'Border' default, 'Media' default-low-med, 'Security' default-low, 'Signaling' default, and 'Time of Day' default. An 'Add Policy Set' button is visible at the bottom right of the group configuration area.

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 for the enterprise. Set the **Border**, **Security** and **Time of Day** rules to either the **default** or **default-low** policies.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists various configuration categories, with 'Domain Policies' expanded. The main area displays the configuration for 'Lab1_DomPolicy'. A table lists the policy rules:

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

The following screen shows **SIP Trunk_DomPolicy** created for CenturyLink. Set the **Application**, **Media**, and **Signaling** rules to the one previously created for CenturyLink. Set the **Border**, **Security**, and **Time of Day** rules to either the **default** or **default-high** policies.

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

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

7.10. 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.

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.

The screenshot shows the UC-Sec Control Center interface. The left sidebar lists navigation options, with 'Media Interface' selected under 'Device Specific Settings'. The main content area is titled 'Media Interface' and contains a table of existing media interfaces. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add Media Interface' button is located above the table.

Name	Media IP	Port Range		
Media_Inside	10.64.19.100	2048 - 5059		
Media_Outside_92	192.168.62.92	8000 - 8999		

After the media interfaces are created, an application restart is necessary before the changes will take effect. Navigate to **UC-Sec Control Center → System Management** and click the forth icon from the right to restart the applications as highlighted below.

The screenshot shows the UC-Sec Control Center interface with 'System Management' selected in the sidebar. The main content area displays a table of installed devices. A red circle highlights the fourth icon from the right in the action column, which represents the restart function.

Device Name	Serial Number	Version	Status						
ASBCE	IPCS31020130	4.0.5.Q09	Commissioned						

7.11. 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**.

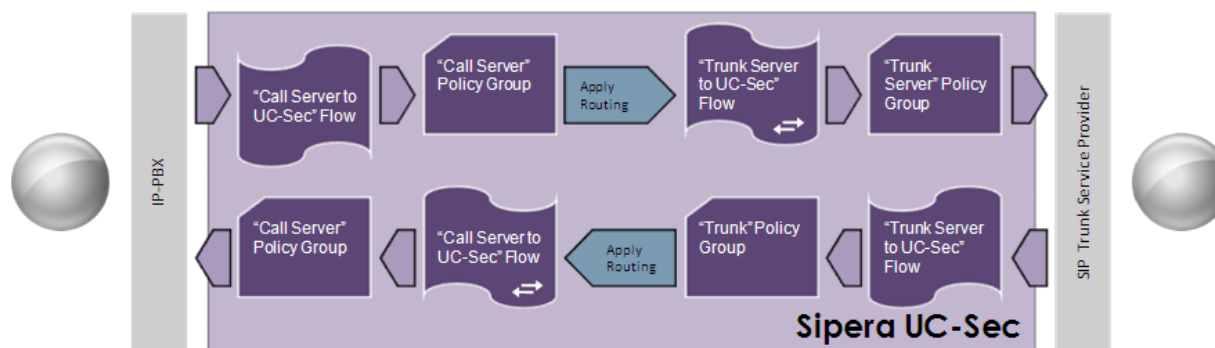
The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.

The screenshot shows the UC-Sec Control Center web interface. The left sidebar contains a navigation tree with 'Signaling Interface' selected. The main content area shows the 'Signaling Interface' configuration page for the 'ASBCE' device. It includes a table of existing interfaces and an 'Add Signaling Interface' button.

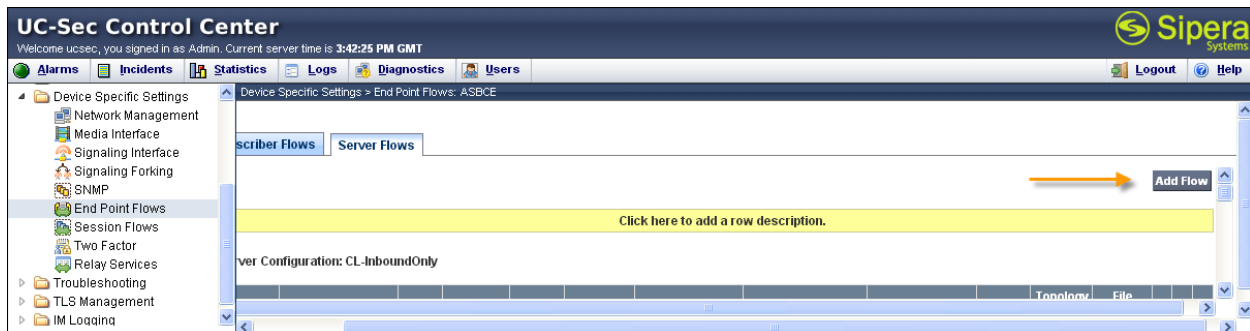
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig_Inside	10.64.19.100	5060	5060	---	None	
Sig_Outside_92	192.168.62.92	5060	5060	---	None	
Inside_TLS	10.64.19.100	---	---	5061	Avaya_tls_server	
Outside_TLS_92	192.168.62.92	---	---	5061	Avaya_tls_server	

7.12. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, 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 Session Manager and CenturyLink SIP Trunk Service. 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 in below.



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

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.5** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface created in **Section 7.11** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.11** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.10** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy created in **Section 7.9** assigned to the Server Configuration.
- **Routing Profile:** Select the profile created in **Section 7.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile created in **Section 7.3** 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: CenturyLink_Flow" with a close button in the top right corner. Below the title bar is a section labeled "Criteria" containing a table of configuration options. The table has two columns: a label column and a value column. The values are either text inputs or dropdown menus. At the bottom of the table is a "Finish" button.

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_SM62-Lab1
Topology Hiding Profile	SIP Trunk
File Transfer Profile	None

Finish

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

The screenshot shows a window titled "Edit Flow: CenturyLink_Flow" with a close button in the top right corner. Below the title bar is a section labeled "Criteria" containing a table of configuration options. The table has two columns: a label column and a value column. The values are either text inputs or dropdown menus. At the bottom of the table is a "Finish" button.

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_SM62-Lab1
Topology Hiding Profile	SIP Trunk
File Transfer Profile	None

Finish

The following screen shows the Sever Flow for Session Manager:

Edit Flow: SM62-Lab1-Flow

Criteria	
Flow Name	SM62-Lab1-Flow
Server Configuration	SM62-Lab1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Sig_Outside_92
Signaling Interface	Sig_Inside
Media Interface	Media_Inside
End Point Policy Group	Lab1_DomPolicy
Routing Profile	Route_to_CenturyLink
Topology Hiding Profile	Enterprise
File Transfer Profile	None

Finish

8. CenturyLink SIP Trunk 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.

9. Verification and Troubleshooting

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

9.1. Verification

The following steps may be used to verify the configuration:

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

[Home](#) / [Elements](#) / [Session Manager](#) / [System Tools](#) / [Call Routing Test](#)[Help ?](#)

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI

Calling Party Address

Calling Party URI

Session Manager Listen Port

Day Of Week

Time (UTC)

Transport Protocol

Called Session Manager Instance

Routing Decisions

Route < sip:7205551234@avayalab.com > to SIP Entity Loc19-ASBCE (10.64.19.100). Terminating Location is Loc19-ASBCE.

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

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

9.2. Troubleshooting

1. Communication Manager:

- **list trace station** <extension number> - Traces calls to and from a specific station.
- **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
- **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
- **status trunk** <trunk access code number> - Displays trunk group information.

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

3. Avaya SBCE:

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

Incident Viewer

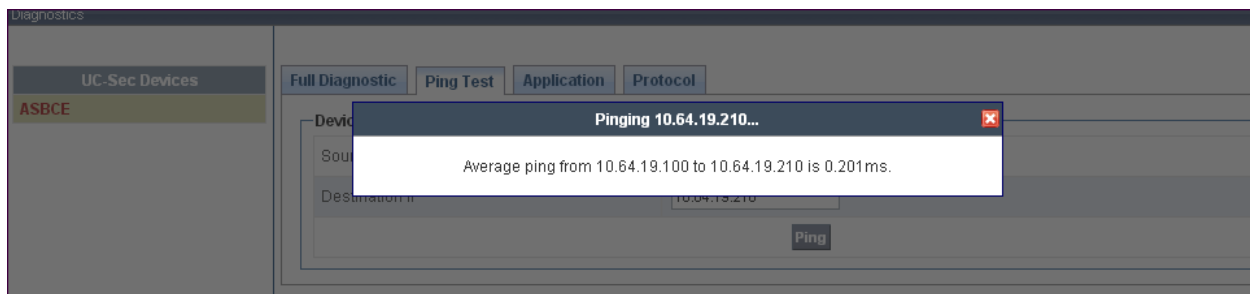
Device: All Category: All Clear Filters Refresh Show Chart Generate Report

Displaying results 1 to 15 out of 829.

Incident Type	Incident ID	Date	Time	Category	Device	Cause
Server Heartbeat	677626218369560	12/11/12	7:00 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677625332521293	12/11/12	6:31 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677625276170295	12/11/12	6:29 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677623965751299	12/11/12	5:45 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677623890418242	12/11/12	5:43 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677585247087809	12/10/12	8:14 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Server Heartbeat	677583086633859	12/10/12	7:02 PM	Policy	ASBCE	Heartbeat Failed, Server is Down
Routing Failure	677574431620086	12/10/12	2:14 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574431620044	12/10/12	2:14 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message
Routing Failure	677574416592850	12/10/12	2:13 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574416592807	12/10/12	2:13 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message
Routing Failure	677574401570113	12/10/12	2:13 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574401570070	12/10/12	2:13 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message
Routing Failure	677574386540355	12/10/12	2:12 PM	Policy	ASBCE	Server Config Found. But no server flow matched, Sending 403 Forbidden
Message Dropped	677574386540292	12/10/12	2:12 PM	Policy	ASBCE	No Server Flow Matched for Outgoing Message

<< < 1 2 3 4 5 > >>

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



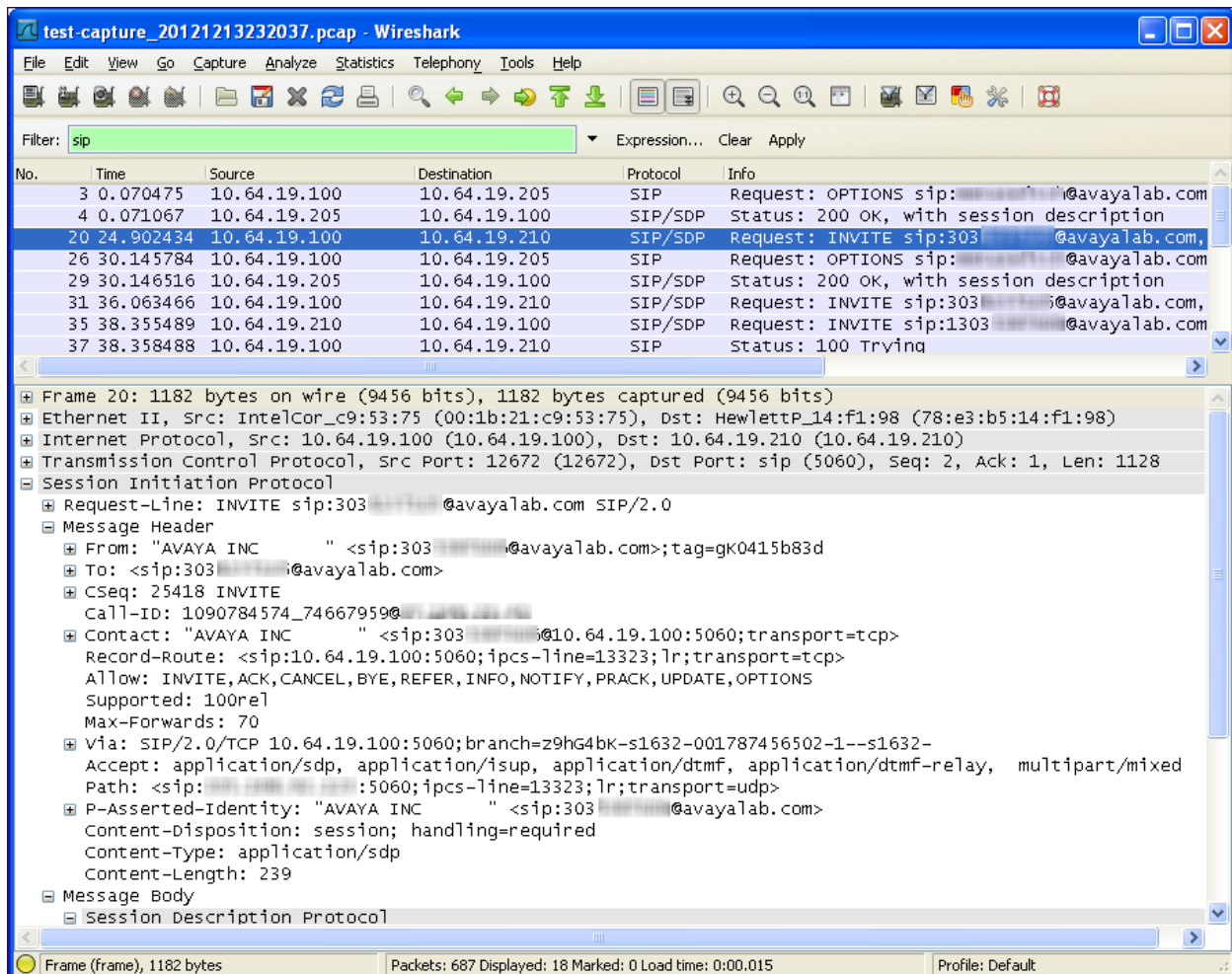
- **Troubleshooting → Trace Settings** – Configure and display call traces and packet captures for the UC-Sec appliance.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a navigation menu with options like Administration, System Management, Troubleshooting, and Trace Settings. The main content area is titled 'Troubleshooting > Trace Settings: ASBCE'. It features tabs for 'Packet Trace', 'Call Trace', 'Packet Capture', and 'Captures'. The 'Packet Capture' tab is active, displaying the 'Packet Capture Configuration' form. The form includes fields for 'Currently capturing' (No), 'Interface' (A1), 'Local Address (ip:port)' (10.64.19.100), 'Remote Address (*, *:port, ip, ip:port)' (*), 'Protocol' (All), 'Maximum Number of Packets to Capture' (1200), and 'Capture Filename' (test-capture.pcap). 'Start Capture' and 'Clear' buttons are at the bottom.

The screenshot shows the same UC-Sec Control Center interface, but the 'Captures' tab is active. It displays a table of captured files. A 'Refresh' button is located at the top right of the table area. The table has columns for 'File Name', 'File Size (bytes)', and 'Last Modified'. One entry is shown: 'test-capture_20121213232037.pcap' with a file size of 167,936 bytes and a last modified time of December 13, 2012 11:21:26 PM GMT. A red 'X' icon is visible in the rightmost column of the table row.

File Name	File Size (bytes)	Last Modified
test-capture_20121213232037.pcap	167,936	December 13, 2012 11:21:26 PM GMT

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



10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Session Manager, Avaya Aura® Communication Manager Evolution Server, and Avaya Session Border Controller for Enterprise to the CenturyLink SIP Trunk Service. 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.

11. Additional References

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

- [1] *Installing and Configuring Avaya Aura® System Platform, Release 6.2.0*, March 2012.
- [2] *Administering Avaya Aura® System Platform, Release 6.2.0*, February 2012.
- [3] *Implementing Avaya Aura® Communication Manager Solution Release 6.2*, February 2012
Document Number 03-603559
- [4] *Administering Avaya Aura® Communication Manager*, Release 6.2, February 2012,
Document Number 03-300509
- [5] *Avaya Aura® Communication Manager Feature Description and Implementation*, June 2010,
Document Number 555-245-205.
- [6] *Implementing Avaya Aura® System Manager*, Release 6.2, March 2012
- [7] *Installing Service Packs for Avaya Aura® Session Manager*, February 2012, Document
Number 03-603863
- [8] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473.
- [9] *Avaya one-X Deskphone H.323 Administrator Guide*, May 2011, Document Number 16-
300698.
- [10] *Avaya one-X Deskphone SIP Administrator Guide Release 6.1*, December 2010, Document
Number 16-603838
- [11] *Administering Avaya one-X Communicator*, July 2011
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [13] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [14] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*,
<http://www.ietf.org/>
- [15] *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.