



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring CenturyLink BroadWorks SIP Trunk with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink BroadWorks SIP Trunk and an Avaya SIP-enabled enterprise solution. CenturyLink BroadWorks SIP Trunk is a business trunking product supported by the BroadWorks platform. The Avaya solution consists of Avaya Aura® Session Manager R6.1, Avaya Aura® Communication Manager Evolution Server R6.0.1, Avaya Aura® Messaging R6.1, Avaya Session Border Controller for Enterprise R4.0.5 and various Avaya endpoints.

CenturyLink is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

TABLE OF CONTENTS

| | |
|--|-----------|
| 1. INTRODUCTION..... | 4 |
| 2. GENERAL TEST APPROACH AND TEST RESULTS | 4 |
| 2.1. INTEROPERABILITY COMPLIANCE TESTING | 4 |
| 2.2. TEST RESULTS | 5 |
| 2.3. SUPPORT | 6 |
| 3. REFERENCE CONFIGURATION | 6 |
| 4. EQUIPMENT AND SOFTWARE VALIDATED..... | 9 |
| 5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER..... | 10 |
| 5.1. LICENSING AND CAPACITY | 10 |
| 5.2. SYSTEM FEATURES..... | 11 |
| 5.3. IP NODE NAMES | 12 |
| 5.4. CODECS..... | 12 |
| 5.5. IP NETWORK REGION | 13 |
| 5.6. SIGNALING GROUP | 14 |
| 5.7. TRUNK GROUP | 16 |
| 5.8. CALLING PARTY INFORMATION..... | 19 |
| 5.9. OUTBOUND ROUTING | 20 |
| 6. CONFIGURE AVAYA AURA® SESSION MANAGER..... | 23 |
| 6.1. SYSTEM MANAGER LOGIN AND NAVIGATION | 24 |
| 6.2. SPECIFY SIP DOMAIN | 26 |
| 6.3. ADD LOCATION | 26 |
| 6.4. ADD ADAPTATION MODULE..... | 29 |
| 6.5. ADD SIP ENTITIES | 31 |
| 6.6. ADD ENTITY LINKS | 35 |
| 6.7. ADD ROUTING POLICIES..... | 37 |
| 6.8. ADD DIAL PATTERNS | 39 |
| 6.9. ADD/VIEW SESSION MANAGER | 42 |
| 7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE | 44 |
| 7.1. ACCESS MANAGEMENT INTERFACE | 44 |
| 7.2. SYSTEM STATUS..... | 45 |
| 7.3. GLOBAL PROFILES – SERVER INTERWORKING | 45 |
| 7.3.1. <i>Server Interworking: Avaya-SM.....</i> | <i>46</i> |
| 7.3.2. <i>Server Interworking: SP-CTL</i> | <i>48</i> |
| 7.4. GLOBAL PROFILES – SERVER CONFIGURATION | 49 |
| 7.4.1. <i>Server Configuration for Session Manager.....</i> | <i>49</i> |
| 7.4.2. <i>Server Configuration for CenturyLink SIP Trunking.....</i> | <i>52</i> |
| 7.5. GLOBAL PROFILES – ROUTING | 56 |
| 7.5.1. <i>Routing Configuration for Session Manager</i> | <i>56</i> |
| 7.5.2. <i>Routing Configuration for CenturyLink SIP Trunking.....</i> | <i>58</i> |
| 7.6. GLOBAL PROFILES – TOPOLOGY HIDING | 58 |
| 7.6.1. <i>Topology Hiding for Session Manager</i> | <i>58</i> |
| 7.6.2. <i>Topology Hiding for CenturyLink SIP Trunking.....</i> | <i>60</i> |
| 7.7. DOMAIN POLICIES – MEDIA RULES | 60 |
| 7.8. DOMAIN POLICIES – SIGNALING RULES..... | 62 |
| 7.9. DOMAIN POLICIES – END POINT POLICY GROUPS | 65 |
| 7.10. DEVICE SPECIFIC SETTINGS – NETWORK MANAGEMENT | 67 |
| 7.11. DEVICE SPECIFIC SETTINGS – MEDIA INTERFACE..... | 68 |

| | | |
|------------|---|-----------|
| 7.12. | DEVICE SPECIFIC SETTINGS – SIGNALING INTERFACE | 69 |
| 7.13. | DEVICE SPECIFIC SETTINGS – END POINT SERVER FLOWS | 70 |
| 8. | CENTURYLINK BROADWORKS SIP TRUNK CONFIGURATION | 73 |
| 9. | VERIFICATION AND TROUBLESHOOTING | 73 |
| 10. | CONCLUSION..... | 75 |
| 11. | REFERENCES..... | 75 |

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between CenturyLink BroadWorks SIP Trunk and an Avaya SIP-enabled enterprise solution. CenturyLink BroadWorks SIP Trunk is a business trunking product supported by the BroadWorks platform. The Avaya solution consists of Avaya Aura® Session Manager R6.1, Avaya Aura® Communication Manager Evolution Server R6.0.1, Avaya Aura® Messaging R6.1, Avaya Session Border Controller for Enterprise (Avaya SBCE) R4.0.5 and various Avaya endpoints.

Avaya Aura® Session Manager is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. The Avaya Session Border Controller for Enterprise is the point of connection between Avaya Aura® Session Manager and the CenturyLink SIP trunking service and is used to not only secure the SIP trunk, but also to make adjustments to SIP signaling for interoperability.

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

2. General Test Approach and Test Results

A simulated enterprise site using Communication Manager, Session Manager and Avaya SBCE was connected to the public Internet using a broadband connection. The enterprise site was configured to connect to CenturyLink SIP trunking service through the public IP network.

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:

- Response to SIP OPTIONS queries.
- 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. Both protocols were tested.
- Various call types including: local, long distance, international, outbound toll-free, operator, operator-assisted calls (0 + 10-digits), local directory assistance (411), and 911 emergency.
- G.711MU codec.
- Voicemail navigation for inbound and outbound calls using DTMF transmission per RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- User features such as hold and resume, internal call forwarding, transfer, and conference
- Off-net call forwarding, transfer, conference and mobility (extension to cellular).

Items not supported or not tested included the following:

- SIP REFER message is not supported on the CenturyLink test circuit and therefore was not tested.
- T.38 faxing is not supported by CenturyLink and therefore was not tested.

2.2. Test Results

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

- **G.729A Codec** – CenturyLink officially supports G.711MU codec only, but was able to accept outbound calls with G.729A codec (and negotiated to this codec on the call) in compliance test.
- **Mis-Matched Codec** – When an outbound call did not have matching codec with CenturyLink (with the exception stated above with G.729A codec), CenturyLink would respond to the outbound INVITE with "180 Ringing" followed with "480 Exhausted Redirects (302: moved temporarily)"; caller hears fast busy tones. A more appropriate status message like "488 Not Acceptable Here" is desirable. CenturyLink support stated that this was due to an artifact of the Acme Packet SBC configuration on the network side; CenturyLink would investigate.
- **Network Call Redirection** – When a Communication Manager vector was programmed to redirect an inbound call to a PSTN number before answering the call in the vector, CenturyLink would send an ACK to the "302 Moved Temporarily" SIP message from the enterprise but would not redirect the call to the new party in the Contact header of the 302 message. The inbound call initiator would hear a recorded announcement about

called party not answering after a few minutes. Note that CenturyLink does not officially support the SIP 302 message.

- **Off-Net Call Redirection:** When INVITE from the enterprise to CenturyLink for off-net call redirection contained both Diversion and History-Info headers, CenturyLink would respond with "404 Not found" resulting in redirection failure. Off-net call redirection includes forwarding a call with PSTN back out to PSTN or re-directing an inbound call to a PSTN mobile number associated with an enterprise extension. This failure was addressed in the compliance test by turning off the History-Info header in the call-redirection INVITE from the enterprise. Century Link support indicated that using Diversion header is the standard way of handling off-net call redirection on the CenturyLink BroadWorks SIP Trunk.
- **Media Anomaly Detection** – When a call with PSTN (either inbound or outbound) was forwarded off-net back out to PSTN, there was no audio occasionally on the answered call. This problem was corrected in the compliance test by turning off Media Anomaly Detection on Avaya SBCE (see **Section 7.7**). Media Anomaly Detection basically measures the jitter in the audio flow and is a bit overly sensitive in the tested software release (and also the past releases). Developers of Avaya SBCE are currently working on an improved implementation of this feature.
- **G.711MU Pass-Through Faxing** – Outbound multi-page fax was successful, but inbound multi-page fax was only partially received. Note that Communication Manager does not officially support G.711 pass-through fax on SIP trunks.

2.3. Support

For technical support on CenturyLink BroadWorks SIP Trunk, contact CenturyLink using the Support link at <http://www.CenturyLink.com>

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to CenturyLink SIP Trunking service (using a lab test circuit) through a public Internet WAN connection.

For security purposes, any actual public IP addresses and PSTN routable phone numbers used in the compliance test are masked in these Application Notes.

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

- Avaya S8800 Server running Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Session Manager
- Avaya S8800 Server running System Manager
- Avaya S8800 Server running Avaya SBCE
- Avaya 9600-Series IP Telephones (H.323 and SIP)
- Avaya 1600-Series IP Telephone (H.323)
- Avaya A175 Desktop Video Device a.k.a. Flare (used as a SIP voice endpoint)
- Avaya one-X® Communicator soft phones (H.323 and SIP)

- Avaya digital and analog telephones
- Dell R210 V2 Server running Avaya messaging application

Located at the edge of the enterprise is the Avaya SBC for Enterprise. It has a public interface that connects to the external network and a private interface that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise flows through this enterprise SBC. In this way, the SBC can protect the enterprise against any SIP-based attacks. The transport protocol between the enterprise SBC and CenturyLink across the public IP network is UDP; the transport protocol between the enterprise SBC and Session Manager across the enterprise IP network is TCP.

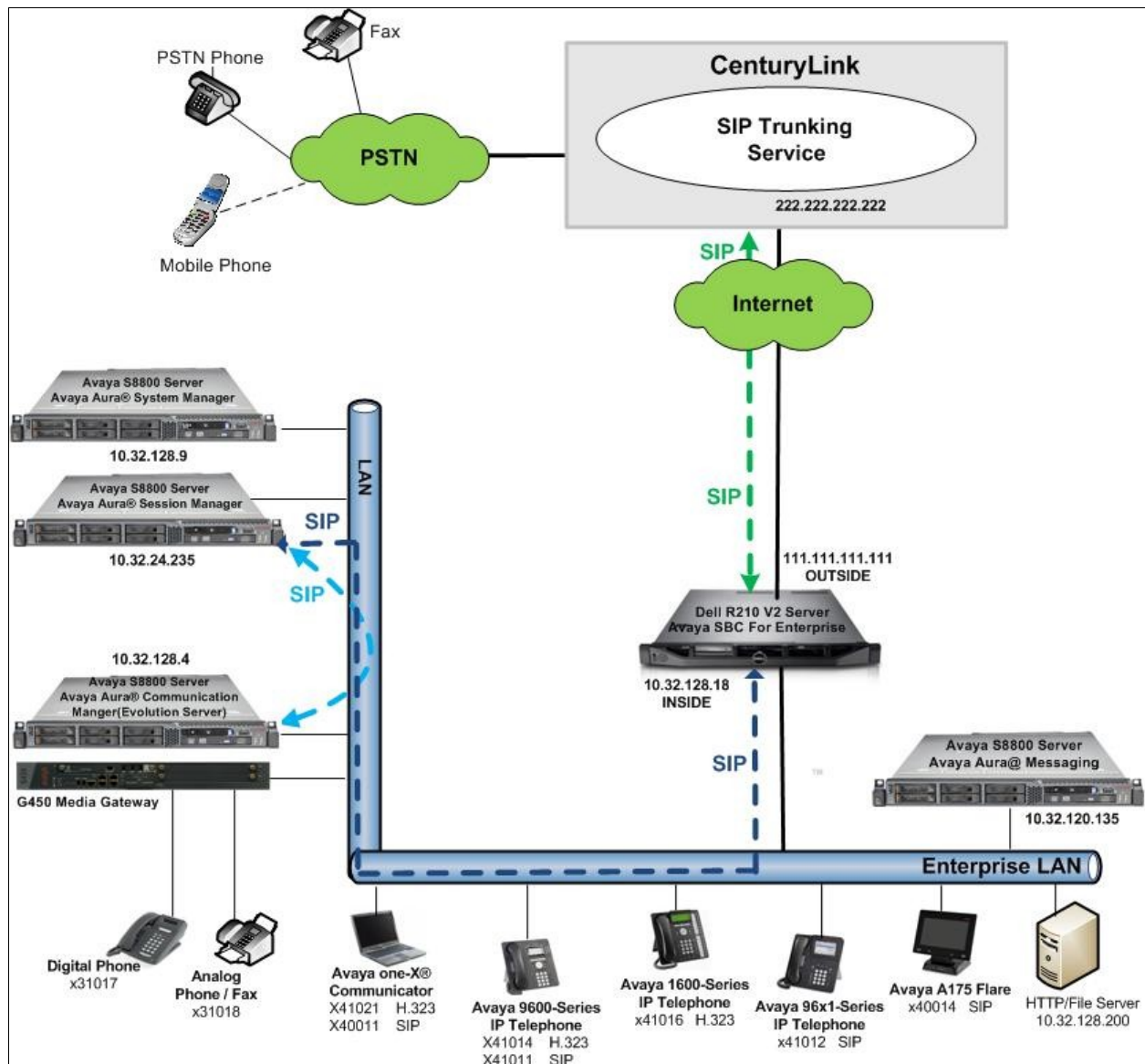


Figure 1: Avaya SIP Enterprise Solution with CenturyLink SIP Trunking

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

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

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

The administration of Avaya Aura® Messaging and Communication Manager extensions are standard for the enterprise. Since the configuration tasks for Avaya Aura® Messaging and enterprise endpoints are not directly related to the inter-operation with CenturyLink SIP Trunking service, they are not included in these Application Notes.

4. Equipment and Software Validated

| Avaya IP Telephony Solution Components | |
|--|--|
| Equipment/Software | Release/Version |
| Avaya Aura® Communication Manager running on Avaya S8800 Server | 6.0.1 (R016x.00.1.510.1-19303) |
| Avaya G450 Media Gateway <ul style="list-style-type: none"> – ICC – ANA – DCP | 31.20.0 HW01 FW001 HW33 FW091 HW07 FW009 |
| Avaya Aura® Session Manager running on Avaya S8800 Server | 6.1.5.0.615006 |
| Avaya Aura® System Manager running on Avaya S8800 Server | 6.1.0 Build 6.1.0.0.7345-6.1.5.502 Software Update Revision No: 6.1.9.1.1634 |
| Avaya 96x0 Series IP Telephone (H.323) | Avaya one-X® Deskphone Edition 3.1.1 |
| Avaya 96x0 Series IP Telephone (SIP) | Avaya one-X® Deskphone SIP Edition 2.6.6 |
| Avaya 96x1 Series IP Telephone (SIP) | Avaya one-X® Deskphone SIP Release 6.0 Service Pack 3 |
| Avaya 1600 Series IP Telephone (H.323) | Avaya one-X Deskphone Value Edition 1.2.2 |
| Avaya A175 Flare™ Desktop Video Device (SIP telephone function) | SIP Version 1.1.0 (SIP_A175_1_1_0_012004) |
| Avaya one-X Communicator (H.323 & SIP) | 6.1.3.09-SP3-Patch3-35953 |
| Avaya 8410D Digital Telephone | n/a |
| Avaya 6210 Analog Telephone | n/a |
| Fax device | Ventafax Home Version 6.1.59.144 |
| Avaya Session Border Controller for Enterprise running on Dell 210 V2 Server | 4.0.5.Q09 |
| Avaya Aura® Messaging running on Avaya S8800 Server | 6.1-11.0 |
| CenturyLink SIP Trunking Components | |
| Equipment/Software | Release/Version |
| Acme Packet 4250 SBC | SC6.1.0 MR-5 GA (Built 704) |
| BroadSoft BroadWorks | 17 sp2 |
| Sonus GSX | B07.02.07 F004 |
| Sonus NBX | B07.02.07 F004 |

The specific hardware and software listed in the table above were used for the compliance testing. Note that 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 BroadWorks SIP Trunk. 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.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. Note that the public IP addresses and PSTN routable phone numbers shown throughout these Application Notes have been edited so that the actual public 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 4000 licenses are available and 244 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: | | 4000 | 0 |
| Maximum Concurrently Registered IP Stations: | | 2400 | 3 |
| Maximum Administered Remote Office Trunks: | | 4000 | 0 |
| Maximum Concurrently Registered Remote Office Stations: | | 2400 | 0 |
| Maximum Concurrently Registered IP eCons: | | 68 | 0 |
| Max Concur Registered Unauthenticated H.323 Stations: | | 100 | 0 |
| Maximum Video Capable Stations: | | 2400 | 4 |
| Maximum Video Capable IP Softphones: | | 2400 | 2 |
| Maximum Administered SIP Trunks: | | 4000 | 244 |
| Maximum Administered Ad-hoc Video Conferencing Ports: | | 4000 | 0 |
| Maximum Number of DS1 Boards with Echo Cancellation: | | 80 | 0 |
| Maximum TN2501 VAL Boards: | | 10 | 0 |
| Maximum Media Gateway VAL Sources: | | 50 | 1 |
| Maximum TN2602 Boards with 80 VoIP Channels: | | 128 | 0 |
| Maximum TN2602 Boards with 320 VoIP Channels: | | 128 | 0 |
| Maximum Number of Expanded Meet-me Conference Ports: | | 300 | 0 |
| (NOTE: You must logoff & login to effect the permission changes.) | | | |

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? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? y
      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 values of **AV-Restricted** for restricted calls and **AV-Unavailable** for unavailable calls.

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

      CPN/ANI/ICLID PARAMETERS
      CPN/ANI/ICLID Replacement for Restricted Calls: AV-Restricted
      CPN/ANI/ICLID Replacement for Unavailable Calls: AV-Unavailable

      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:
      International Access Code:

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Avaya S8800 Server running Communication Manager (*procr*) and for Session Manager (*sessionMgr*). These node names will be needed for defining the service provider signaling group in **Section 5.6**.

| | | |
|----------------------|---------------------|---------------|
| change node-names ip | | Page 1 of 2 |
| | | IP NODE NAMES |
| Name | IP Address | |
| default | 0.0.0.0 | |
| procr | 10.32.128.4 | |
| procr6 | :: | |
| sessionMgr | 10.32.24.235 | |

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. CenturyLink officially supports G.711MU only. Thus, this codec was included in this set. Enter **G.711MU** in the **Audio Codec** column of the table. Default values can be used for all other fields.

| | | |
|-----------------------|----------------------------|-----------------------|
| change ip-codec-set 2 | | Page 1 of 2 |
| | | IP Codec Set |
| Codec Set: 2 | | |
| Audio Codec | Silence Suppression | Frames Per Pkt |
| 1: G.711MU | n | 2 |
| 2: | | |
| 3: | | |

On **Page 2**, set the **Fax Mode** to *off*. This setting was used for G.711MU pass-through fax testing.

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

5.5. 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. Use the **change ip-network-region 2** command to configure region 2 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **avaya.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 to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. 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**.
- Default values can be used for all other fields.

```
change ip-network-region 2                                     Page 1 of 20

                                IP NETWORK REGION

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

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

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

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and the 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 5 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 the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of *tcp* (Transport Layer Security). For ease of troubleshooting during testing, the compliance test was conducted with the **Transport Method** set to *tcp*. The transport method specified here is used between the Communication Manager and Session Manager.
- 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 and for TCP the well-known port value is 5060). This is necessary for Session Manager to distinguish this trunk from the trunk used for other enterprise SIP traffic. The compliance test was conducted with the **Near-end Listen Port** and **Far-end Listen Port** set to **5068**.
- Set the **Peer Detection Enabled** field to *y*. The **Peer-Server** field will initially be set to *Others* and cannot be changed via administration. Later, the **Peer-Server** field will automatically change to *SM* once Communication Manager detects its peer as a Session Manager.
- Set the **Near-end Node Name** to *procr*. This node name maps to the IP address of the Avaya S8800 Server running Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to *sessionMgr*. 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 5.5**.
- 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 allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint. Depending on the number of media resources available in the Avaya Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set the **Alternate Route Timer** to **15**. This defines the number of seconds the Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Default values may be used for all other fields.

Note that the **Initial IP-IP Direct Media** setting must be consistent with the setting in the signaling group used for general internal SIP traffic; otherwise unintended side effects could occur. The default setting is not to enable this feature.

```
add signaling-group 5
                                SIGNALING GROUP

Group Number: 5                Group Type: sip
IMS Enabled? n                Transport Method: tcp
    Q-SIP? n                                SIP Enabled LSP? n
    IP Video? n                        Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: SM

Near-end Node Name: procr      Far-end Node Name: sessionMgr
Near-end Listen Port: 5068     Far-end Listen Port: 5068
                                Far-end Network Region: 2
                                Far-end Secondary Node Name:

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate
    DTMF over IP: rtp-payload    Bypass If IP Threshold Exceeded? n
                                RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3    Direct IP-IP Audio Connections? y
                                IP Audio Hairpinning? n
    Enable Layer 3 Test? y        Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n    Alternate Route Timer(sec): 15
```

5.7. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group created in **Section 5.6**. For the compliance test, trunk group 5 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 created in **Section 5.6**.
- 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 5 | | Page 1 of 21 | |
| TRUNK GROUP | | | |
| Group Number: 5 | Group Type: sip | CDR Reports: y | |
| Group Name: A-SP-Trunk | COR: 1 | TN: 1 | TAC: 1005 |
| Direction: two-way | Outgoing Display? n | Night Service: | |
| Dial Access? n | Night Service: | | |
| Queue Length: 0 | | | |
| Service Type: public-ntwrk | Auth Code? n | | |
| | Member Assignment Method: auto | | |
| | Signaling Group: 5 | | |
| | Number of Members: 10 | | |

On **Page 2**, set the **Redirect On OPTIM Failure** timer to the same amount of time as the **Alternate Route Timer** on the signaling group form in **Section 5.6**. Note that the **Redirect On OPTIM Failure** timer is defined in milliseconds. 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 3 | | Page 2 of 21 | |
| Group Type: sip | | | |
| TRUNK PARAMETERS | | | |
| Unicode Name: auto | | | |
| Redirect On OPTIM Failure: 15000 | | | |
| SCCAN? n | Digital Loss Group: 18 | | |
| Preferred Minimum Session Refresh Interval(sec): 600 | | | |

On **Page 3**, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to *private* and the **Numbering Format** field in the route pattern was set to *unk-unk* (see **Section 5.9**)

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to *y*. This will allow the CPN displayed on enterprise 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 an enterprise user requests CPN block on a particular call routed out this trunk. Default values were used for all other fields.

| | | |
|----------------------------------|----------------|----------------------|
| add trunk-group 3 | | Page 3 of 21 |
| TRUNK FEATURES | | |
| ACA Assignment? n | Measured: none | Maintenance Tests? y |
| Numbering Format: private | | |
| UI Treatment: service-provider | | |
| Replace Restricted Numbers? y | | |
| Replace Unavailable Numbers? y | | |
| Modify Tandem Calling Number: no | | |
| Show ANSWERED BY on Display? y | | |
| DSN Term? n | | |

On **Page 4**, set the **Network Call Redirection** field to **n** (default setting). Setting the **Network Call Redirection** flag to **n** enables use of the SIP INVITE message for call transfer (instead of REFER which is not supported by CenturyLink).

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 needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Support Request History** field to **n**. This parameter determines whether the SIP History-Info header will be included in the call-redirection INVITE from the enterprise. Call-redirection of inbound call from PSTN back to PSTN failed in the compliance test when the call re-direction INVITE contains the History-Info header.

Set the **Telephone Event Payload Type** to **101**, the value preferred by CenturyLink.

Set **Always Use re-INVITE for Display Updates** to **y**. This setting causes CM to use re-INVITE instead of UPDATE for phone display updates.

| | |
|---|---------------------|
| add trunk-group 3 | Page 4 of 21 |
| PROTOCOL VARIATIONS | |
| Mark Users as Phone? | n |
| Prepend '+' to Calling Number? | n |
| Send Transferring Party Information? | n |
| Network Call Redirection? | n |
| Send Diversion Header? | y |
| Support Request History? | n |
| Telephone Event Payload Type: | 101 |
| Convert 180 to 183 for Early Media? | n |
| Always Use re-INVITE for Display Updates? | y |
| Identity for Calling Party Display: | P-Asserted-Identity |

5.8. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since private numbering was selected to define the format of this number (**Section 5.7**), use the **change private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

The screen below shows a subset of the DID numbers assigned for testing. The 3 DID numbers were mapped to the 3 enterprise extensions 41011, 41014, and 41016. These same 10-digit numbers were used for the outbound calling party information on the service provider trunk when calls were originated from these 3 extensions.

| | | | | | |
|----------------------------|----------|-------------|----------------|-----------|------------------------|
| change private-numbering 0 | | | | | Page 1 of 2 |
| NUMBERING - PRIVATE FORMAT | | | | | |
| Ext Len | Ext Code | Trk Grp (s) | Private Prefix | Total Len | |
| 5 | 3 | | | 5 | Total Administered: 10 |
| 5 | 4 | | | 5 | Maximum Entries: 540 |
| 5 | 41011 | 3 | 5857741111 | 10 | |
| 5 | 41014 | 3 | 5857741112 | 10 | |
| 5 | 41016 | 3 | 5857741113 | 10 | |

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private numbering entry can be applied for all extensions. In the example below, all stations with a 5-digit extension beginning with 4 will send the calling party number as the **Private Prefix** plus the extension number.

| | | | | | |
|----------------------------|----------|-------------|----------------|-----------|------------------------|
| change private-numbering 0 | | | | | Page 1 of 2 |
| NUMBERING - PRIVATE FORMAT | | | | | |
| Ext Len | Ext Code | Trk Grp (s) | Private Prefix | Total Len | |
| 5 | 3 | | | 5 | Total Administered: 10 |
| 5 | 4 | 3 | 58577 | 10 | Maximum Entries: 540 |

5.9. 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 with little elaboration. 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: 3 | | |
| Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type | Dialed String | Total Length | Call Type |
| 0 | 1 | fac | 9 | 1 | fac | | | |
| 00 | 3 | fac | * | 2 | fac | | | |
| 01 | 3 | fac | # | 2 | fac | | | |
| 1 | 3 | dac | | | | | | |
| 2 | 5 | ext | | | | | | |
| 3 | 5 | ext | | | | | | |
| 4 | 5 | ext | | | | | | |
| 44 | 5 | ext | | | | | | |
| 5 | 5 | ext | | | | | | |
| 50 | 4 | ext | | | | | | |
| 6 | 5 | ext | | | | | | |
| 7 | 5 | ext | | | | | | |
| 732 | 10 | udp | | | | | | |
| 777 | 7 | udp | | | | | | |
| 8 | 1 | fac | | | | | | |

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

| | | | |
|--|--|------------------|--|
| change feature-access-codes | | Page 1 of 10 | |
| FEATURE ACCESS CODE (FAC) | | | |
| Abbreviated Dialing List1 Access Code: | | | |
| Abbreviated Dialing List2 Access Code: | | | |
| Abbreviated Dialing List3 Access Code: | | | |
| Abbreviated Dial - Prgm Group List Access Code: | | | |
| Announcement Access Code: 001 | | | |
| Answer Back Access Code: | | | |
| Attendant Access Code: | | | |
| Auto Alternate Routing (AAR) Access Code: 8 | | | |
| Auto Route Selection (ARS) - Access Code 1: 9 | | Access Code 2: | |
| Automatic Callback Activation: | | Deactivation: | |
| Call Forwarding Activation Busy/DA: *2 All: *1 | | Deactivation: #1 | |
| Call Forwarding Enhanced Status: Act: | | Deactivation: | |
| Call Park Access Code: | | | |
| Call Pickup Access Code: | | | |
| CAS Remote Hold/Answer Hold-Unhold Access Code: | | | |
| CDR Account Code Access Code: | | | |
| Change COR Access Code: | | | |

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit 9. 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 **55** which contains the SIP trunk to the service provider (as defined next).

| | | | | | | | |
|--------------------------|--------|-------|-----|---------|------|-----------------|------|
| change ars analysis 0 | | | | | | Page 1 of 2 | |
| ARS DIGIT ANALYSIS TABLE | | | | | | | |
| Location: all | | | | | | Percent Full: 2 | |
| | Dialed | Total | | Route | Call | Node | ANI |
| | String | Min | Max | Pattern | Type | Num | Reqd |
| 0 | | 1 | 1 | 55 | op | | n |
| 0 | | 11 | 11 | 55 | op | | n |
| 00 | | 2 | 2 | 55 | op | | n |
| 011 | | 10 | 18 | 55 | intl | | n |
| 1800 | | 11 | 11 | 55 | fnpa | | n |
| 1877 | | 11 | 11 | 55 | fnpa | | n |
| 1908 | | 11 | 11 | 55 | fnpa | | n |
| 411 | | 3 | 3 | 55 | svcl | | 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 55 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 5 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 one will prefix any FNPA 10-digit number with a 1 and leave numbers of any other length unchanged. This will ensure 1 + 10 digits are sent to the service provider for long distance North American Numbering Plan (NANP) numbers. All HNPA 10 digit numbers are left unchanged.
- **Numbering Format:** Set this field to **unk-unk** since private Numbering Format should be used for this route (see **Section 5.7**).
- **LAR:** *next*

| | | | | | | | | | | | | | | | | | | |
|-------------------------|-----|-----|-----|-----|------|-----|----------|------|--|--|---|------------------------|---------|-------------------------------|--|------|-----------|-----|
| change route-pattern 55 | | | | | | | | | | | | Page | | 1 of | | 3 | | |
| Pattern Number: 55 | | | | | | | | | | | | Pattern Name: SP Route | | | | | | |
| 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: | 5 | 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 | | | | unk-unk | next | | | | | |
| 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. Configure Avaya Aura® Session Manager

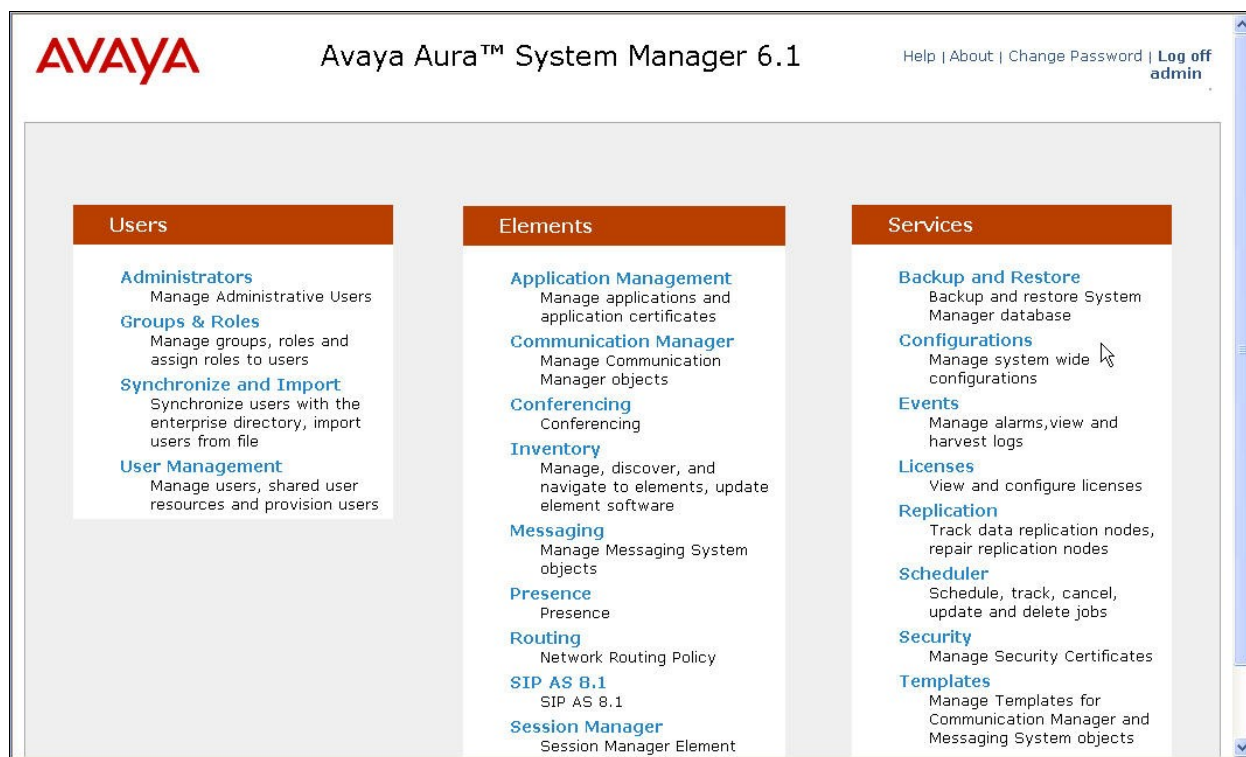
This section provides the procedures for configuring Session Manager. The procedures include the following items:

- Specify SIP domain
- Add Logical/physical Location that can be occupied by SIP Entities
- Add Adaptation module to perform dial plan manipulation
- Add SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager
- Add Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Add Routing Policies, which define route destinations and control call routing between the SIP Entities
- Add Dial Patterns, which specify dialed digits and govern to which SIP Entity a call is routed
- Add/View Session Manager, corresponding to the Session Manager to be managed by System Manager.

It may not be necessary to create all the items above when configuring for 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. 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. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



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

The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

The screenshot displays the Avaya Aura™ System Manager 6.1 web interface. The top header includes the Avaya logo, the product name, and user links for Help, About, Change Password, and Log off admin. A breadcrumb trail shows the path: Home / Elements / Routing - Introduction to Network Routing Policy. On the left, a navigation tree is expanded to 'Routing', showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Introduction to Network Routing Policy' and contains the following text:

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"
- Step 6: Create "Time Ranges"

6.2. Specify SIP Domain

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

Domain Management

CommitCancel

1 Item | RefreshFilter: Enable

| Name | Type | Default | Notes |
|-------------|------|--------------------------|-------------------|
| * avaya.com | sip | <input type="checkbox"/> | Enterprise Domain |

* Input Required

CommitCancel

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:

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

In the **Location Pattern** section (see 2nd screen below), click **Add** and enter the following values:

- **IP Address Pattern:** An IP address pattern used to identify the Location.
- **Notes:** Add a brief description (optional).

Displayed below are the top and bottom halves of the screen for addition of the **Location 1** Location, which includes all equipment on the enterprise network including Communication Manager and the Session Manager itself. Click **Commit** to save.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing **Home**

Home / Elements / Routing / Locations- Location Details

Location Details [Help ?](#)

General

* **Name:**

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

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

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

Minimum Multimedia Bandwidth: Kbit/Sec

* **Default Audio Bandwidth:**

Location Pattern

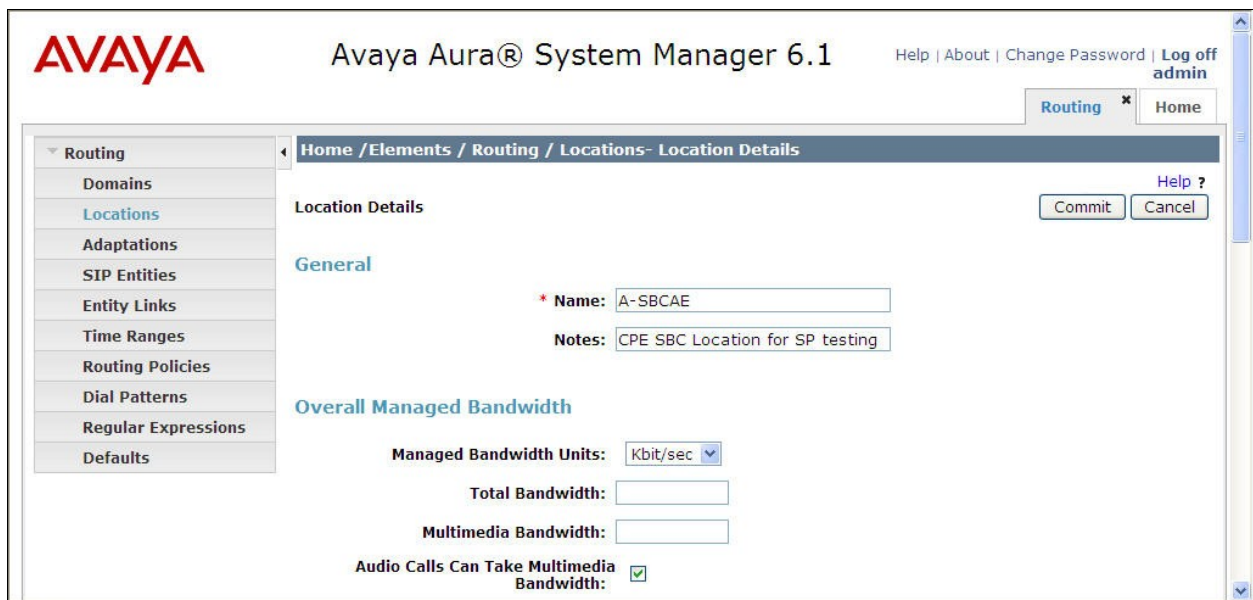
4 Items [Refresh](#) [Filter: Enable](#)

| <input type="checkbox"/> | IP Address Pattern | Notes |
|--------------------------|--------------------|--------------------------------|
| <input type="checkbox"/> | * 10.32.120.* | AAM and other CPE devices |
| <input type="checkbox"/> | * 192.168.49.* | CPE endpoints |
| <input type="checkbox"/> | * 10.32.24.235 | SM 6.1 (devcon-asm) |
| <input type="checkbox"/> | * 10.32.128.* | CM 6.0.1 and other CPE devices |

Select : All, None

Note that call bandwidth management parameters should be set per customer requirement.

Repeat the preceding procedure to create a separate Location for Avaya SBCE. Displayed below are the top and bottom halves of the screen for addition of the **A-SBCAE** Location, which specifies the specific inside IP address for the SBC. Click **Commit** to save.



AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

[Routing](#) * [Home](#)

[Home / Elements / Routing / Locations- Location Details](#)

Location Details [Help ?](#)

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

General

* **Name:** A-SBCAE

Notes: CPE SBC Location for SP testing

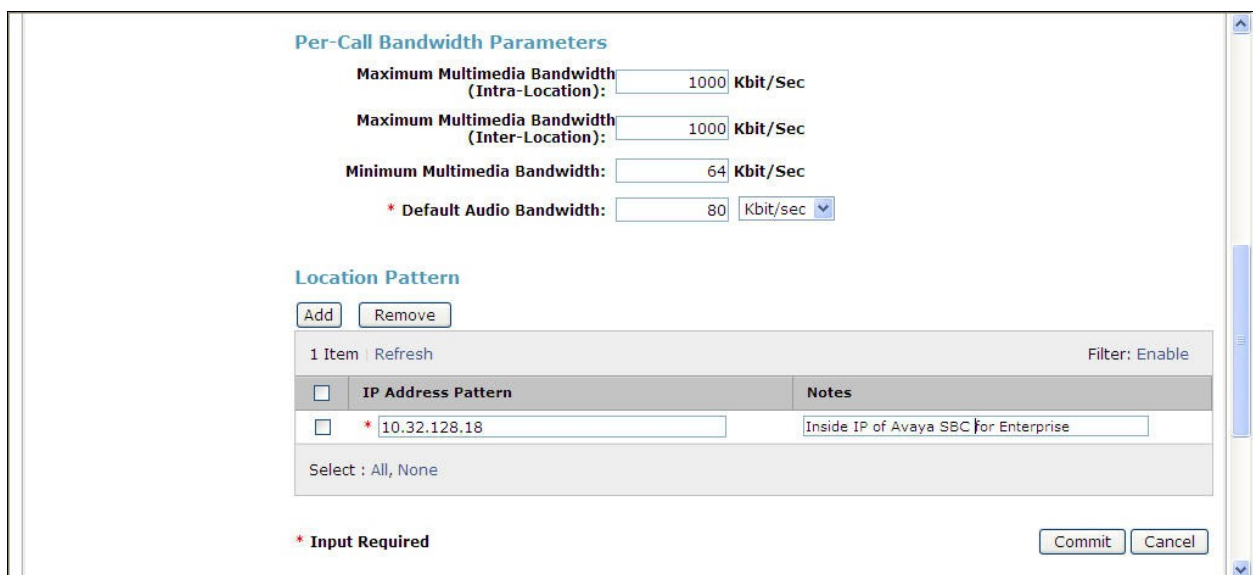
Overall Managed Bandwidth

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

Location Pattern

[Add](#) [Remove](#)

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

| <input type="checkbox"/> | IP Address Pattern | Notes |
|--------------------------|--------------------|---------------------------------------|
| <input type="checkbox"/> | * 10.32.128.18 | Inside IP of Avaya SBC for Enterprise |

Select : All, None

* **Input Required** [Commit](#) [Cancel](#)

6.4. Add Adaptation Module

Session Manager can be configured with Adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic Adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other Adaptation modules are built on this generic module, and can modify other headers to permit interoperability with third party SIP products.

For interoperability with CenturyLink BroadWorks SIP Trunk, only one Adaptation is needed. This adaptation is applied to the Communication Manager SIP entity to:

1. Replace the domain in the Request URI with the enterprise domain as expected by Communication Manager.
2. Map inbound DID numbers from CenturyLink to local Communication Manager extensions.

To create the Adaptation that will be applied to the Communication Manager SIP entity, navigate to **Routing → Adaptations** 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:

- **Adaptation Name:** Enter a descriptive name for the Adaptation.
- **Module Name:** Enter ***DigitConversionAdapter***
- **Module parameter:** Enter ***odstd=avaya.com***. This is the OverrideDestinationDomain parameter. This parameter replaces the domain in the Request URI with the given value for the destination domain.

This Adaptation uses the ***DigitConversionAdapter*** and specifies the ***odstd=avaya.com*** parameter to adapt the outbound destination domain to the domain expected by Communication Manager. More specifically, this configuration enables the destination domain to be overwritten with ***avaya.com*** for calls that egress to a SIP entity using this Adaptation. For example, for inbound PSTN calls from CenturyLink to the enterprise, the Request-URI sent to Communication Manager will contain ***avaya.com*** as expected by Communication Manager.

The screenshot shows the 'Adaptation Details' configuration page. The left navigation pane has 'Routing' expanded, and 'Adaptations' is selected. The main content area is titled 'Home / Elements / Routing / Adaptations - Adaptation Details'. Below the title bar, there's a 'General' section. The fields are as follows:

- Adaptation name:** CTL CM-ES
- Module name:** DigitConversionAdapter (selected from a dropdown)
- Module parameter:** odstd=avaya.com
- Egress URI Parameters:** (empty field)
- Notes:** Change RURI to CPE domain for in

At the top right of the main area, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

To map inbound DID numbers from CenturyLink to Communication Manager extensions, scroll down to the **Digit Conversion for Outgoing Calls from SM** section. Create an entry for each DID to be mapped. Click **Add** and enter the following values for each mapping. Use default values for all remaining fields:

- **Matching Pattern:** Enter a digit string used to match the inbound DID number.
- **Min:** Enter a minimum dialed number length used in the match criteria.
- **Max:** Enter a maximum dialed number length used in the match criteria.
- **Delete Digits** Enter the number of digits to delete from the beginning of the received number.
- **Insert Digits:** Enter the number of digits to insert at the beginning of the received number.
- **Address to modify:** Select **both**.

Click **Commit** to save.

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

| | Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Notes |
|--------------------------|------------------|------|------|---------------|---------------|---------------|-------------------|-------|
| <input type="checkbox"/> | * 5857741111 | * 10 | * 10 | | * 10 | 41011 | both | |
| <input type="checkbox"/> | * 5857741112 | * 10 | * 10 | | * 10 | 41014 | both | |
| <input type="checkbox"/> | * 5857741113 | * 10 | * 10 | | * 10 | 40016 | both | |

Digit Conversion for Outgoing Calls from SM

Add Remove

5 Items Refresh Filter: Enable

| | Matching Pattern | Min | Max | Phone Context | Delete Digits | Insert Digits | Address to modify | Notes |
|--------------------------|------------------|------|------|---------------|---------------|---------------|-------------------|-------|
| <input type="checkbox"/> | * 5857741111 | * 10 | * 10 | | * 10 | 41011 | both | |
| <input type="checkbox"/> | * 5857741112 | * 10 | * 10 | | * 10 | 41014 | both | |
| <input type="checkbox"/> | * 5857741113 | * 10 | * 10 | | * 10 | 40016 | both | |

In the example shown above, if a user on the PSTN dials 585-774-1112, Session Manager will convert the number to 41014 before sending out the SIP INVITE to Communication Manager. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, the Communication Manager private-numbering was configured with an entry to convert 41014 to 5857741112 before sending the call on the trunk group to Session Manager (as shown in **Section 5.8**).

During the compliance test, the digit conversions (or number mappings) in Session Manager Adaptation were varied to route inbound calls to various destinations (including voice messaging pilot number, Communication Manager Vector Directory Numbers, etc.) for different test cases.

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 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:** Select **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 created in **Section 6.4** 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 SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

The screenshot shows the 'SIP Entity Details' form in the 'Routing' section. The left navigation pane lists various configuration areas, with 'SIP Entities' selected. The main area is titled 'SIP Entity Details' and has a 'General' tab. The form contains the following fields:

- Name:** devcon-asm
- FQDN or IP Address:** 10.32.24.235
- Type:** Session Manager (dropdown menu)
- Notes:** SM 6.1 for SP testing
- Location:** Location 1 (dropdown menu)
- Outbound Proxy:** (empty dropdown menu)
- Time Zone:** America/New_York (dropdown menu)
- Credential name:** (empty text field)

Below the 'General' tab is the 'SIP Link Monitoring' section, which includes a dropdown menu set to 'Use Session Manager Configuration'. At the top right of the form are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

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 the **Session Manager** SIP Entity.

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

- **Port:** Port number on which the 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.

The compliance test used 2 **Port** entries:

- **5060** with **TCP** for connecting to Avaya SBCE
- **5068** with **TCP** for connecting to Communication Manager

In addition, port 5060 with TCP was also used by a separate SIP Link between Session Manager and Communication Manager for Avaya SIP telephones and SIP soft clients. This SIP Link was part of the standard configuration on Session Manager and was not directly relevant to the interoperability with CenturyLink BroadWorks SIP Trunk.

Port

Add Remove

6 Items Refresh Filter: Enable

| <input type="checkbox"/> | Port | Protocol | Default Domain | Notes |
|--------------------------|------|----------|----------------|-------|
| <input type="checkbox"/> | 5060 | TCP | avaya.com | |
| <input type="checkbox"/> | 5060 | UDP | avaya.com | |
| <input type="checkbox"/> | 5061 | TLS | avaya.com | |
| <input type="checkbox"/> | 5062 | TCP | avaya.com | |
| <input type="checkbox"/> | 5066 | TCP | avaya.com | |
| <input type="checkbox"/> | 5068 | TCP | avaya.com | |

Select : All, None

* Input Required

Commit Cancel

The following screen shows the addition of Communication Manager SIP Entity. In order for Session Manager to send SIP service provider traffic on a separate entity link to Communication Manager, it is necessary to create a separate SIP Entity for Communication Manager in addition to the one created at Session Manager installation for use with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of the Communication Manager. For the **Adaptation** field, select the Adaptation module previously defined for domain and digit manipulation in **Section 6.4**.

The screenshot shows a web-based configuration interface for SIP Entities. On the left is a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / SIP Entities- SIP Entity Details'. Below this is a 'SIP Entity Details' section with a 'General' tab. The form contains the following fields: 'Name' (sp5-cm), 'FQDN or IP Address' (10.32.128.4), 'Type' (CM), 'Notes' (CM 6.0.1 w/ trunk grp 5), 'Adaptation' (CTL CM-ES), 'Location' (Location 1), 'Time Zone' (America/New_York), 'Override Port & Transport with DNS SRV' (unchecked), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), 'Call Detail Recording' (none), and 'SIP Link Monitoring' (Use Session Manager Configuration). 'Commit' and 'Cancel' buttons are in the top right.

| Field | Value |
|--|-----------------------------------|
| Name | sp5-cm |
| FQDN or IP Address | 10.32.128.4 |
| Type | CM |
| Notes | CM 6.0.1 w/ trunk grp 5 |
| Adaptation | CTL CM-ES |
| Location | Location 1 |
| Time Zone | America/New_York |
| Override Port & Transport with DNS SRV | <input type="checkbox"/> |
| SIP Timer B/F (in seconds) | 4 |
| Credential name | |
| Call Detail Recording | none |
| SIP Link Monitoring | Use Session Manager Configuration |

The following screen shows the addition of the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the SBC's inside network interface (see **Figure 1**).

The screenshot shows a web-based configuration interface for SIP Entities. On the left is a navigation menu with the following items: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area has a breadcrumb trail: Home / Elements / Routing / SIP Entities- SIP Entity Details. Below the breadcrumb is a 'SIP Entity Details' section with a 'Help ?' link and 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields: * Name: A-SBCAE; * FQDN or IP Address: 10.32.128.18; Type: Other (dropdown); Notes: CPE Avaya SBC for Enterprise; Adaptation: (dropdown); Location: A-SBCAE (dropdown); Time Zone: America/New_York (dropdown); Override Port & Transport with DNS SRV: (checkbox, unchecked); * SIP Timer B/F (in seconds): 4; Credential name: (text field); Call Detail Recording: none (dropdown). Below the 'General' section is the 'SIP Link Monitoring' section with the field: SIP Link Monitoring: Use Session Manager Configuration (dropdown).

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the 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 Session Manager SIP Entity.
- **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 the Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **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 5.6**.
- **Trusted:** Check this box. *Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.5** will be denied.*

Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and Avaya SBCE. It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS. For the compliance test, TCP was used to aid in troubleshooting since the signaling traffic would not be encrypted. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.6**.

Entity Link to Communication Manager:

| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy |
|---------------|--------------|----------|--------|--------------|--------|-------------------|
| * sp5-cm-link | * devcon-asm | TCP | * 5068 | * sp5-cm | * 5068 | Trusted |

Entity Link to Avaya SBCE:

| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy |
|---------------|--------------|----------|--------|--------------|--------|-------------------|
| * A-SBCE-link | * devcon-asm | TCP | * 5060 | * A-SBCE | * 5060 | Trusted |

Note that a separate Entity Link existed between Communication Manager and Session Manager (not shown) for carrying SIP traffic between Session Manager and Communication Manager that is not necessarily related to calls to and from the service provider, such as traffic related to SIP Telephones registered to Session Manager, or traffic related to Avaya Aura® Messaging, which has SIP integration to Session Manager.

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 following screen 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**. 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 Manager:

Routing Policy Details

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

| Name | FQDN or IP Address | Type | Notes |
|--------|--------------------|------|-------------------------|
| sp5-cm | 10.32.128.4 | CM | CM 6.0.1 w/ trunk grp 5 |

Time of Day

1 Item | Refresh Filter: Enable

| <input type="checkbox"/> | Ranking 1 ▲ | Name 2 ▲ | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start Time | End Time | Notes |
|--------------------------|-------------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| <input type="checkbox"/> | 0 | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00 | 23:59 | Time Range 24/7 |

Select : All, None

Routing Policy for Avaya SBCE:

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

CommitCancelHelp ?

General

* Name:

A-SBCAE-route

Disabled:

☐

Notes:

Outbound to A-SBCAE for SP test

SIP Entity as Destination

Select

| Name | FQDN or IP Address | Type | Notes |
|---------|--------------------|-------|------------------------------|
| A-SBCAE | 10.32.128.18 | Other | CPE Avaya SBC for Enterprise |

Time of Day

AddRemoveView Gaps/Overlaps

1 Item | RefreshFilter: Enable

| <input type="checkbox"/> | Ranking 1 ▲ | Name 2 ▲ | Mon | Tue | Wed | Thu | Fri | Sat | Sun | Start Time | End Time | Notes |
|--------------------------|-------------|----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|------------|----------|-----------------|
| <input type="checkbox"/> | 0 | 24/7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 00:00 | 23:59 | Time Range 24/7 |

Select : All, None

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 Routing 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 SIP 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, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise. Other dial patterns (e.g., 411 directory assistance call, etc.) were similarly defined.

The first example shows that 11-digit dialed numbers that begin with **1** and have a destination SIP Domain of **avaya.com** (to be converted to the domain as required by the service provider at Avaya SBCE) uses Routing Policy **A-SBCAE-route** as defined in **Section 6.7**.

Note that the above Dial Pattern configuration did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised (e.g., use Pattern 1908, 1732, etc. with 11 digits) per customer business policies.

Also note that **-ALL-** was selected for Originating Location. This selection was to accommodate certain off-net call forward scenarios where the inbound call was re-directed outbound back to the PSTN. For straight outbound calls, like 411 local directory call, the enterprise Location **Location 1** could have been selected.

The second example shows that inbound 10-digit numbers that start with **585774** uses Routing Policy **sp5-cm-route** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by CenturyLink. Location **A-SBCAE** was selected as the originating location to indicate these calls come via Avaya SBCE.

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 585774

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: avaya.com

Notes: Frontier inbound DID numbers

Originating Locations and Routing Policies

Add Remove

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"/> | A-SBCAE | CPE SBC Location for SP testing | sp5-cm-route | 0 | <input type="checkbox"/> | sp5-cm | Inbound SP DID to sp5-cm |

Select : All, None

6.9. Add/View Session Manager

The creation of a Session Manager element 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 **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

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

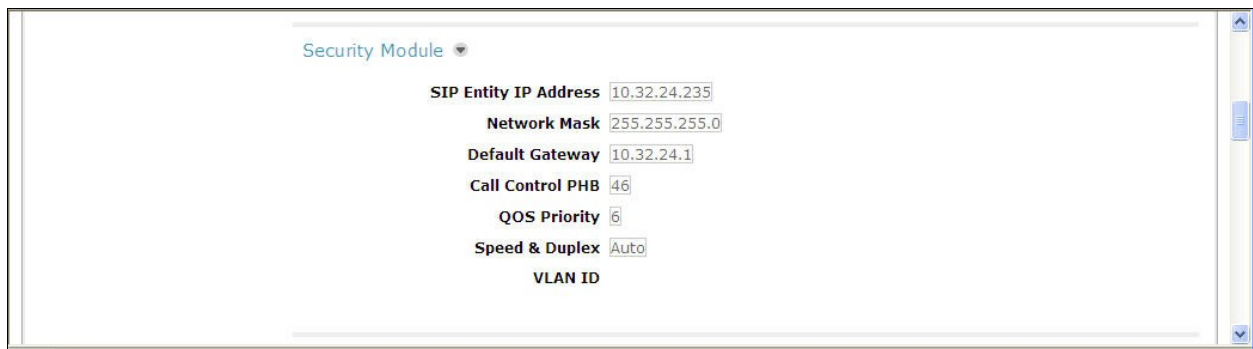
The screen below shows the Session Manager values used for the compliance test.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows the navigation path: 'Home / Elements / Session Manager / Session Manager Administration - Session Manager Administration'. The left sidebar contains a navigation menu with options like 'Session Manager', 'Dashboard', 'Session Manager Administration', 'Communication Profile Editor', 'Network Configuration', 'Device and Location Configuration', 'Application Configuration', 'System Status', and 'System Tools'. The main content area is titled 'View Session Manager' and includes a 'Return' button. Below this, there are tabs for 'General', 'Security Module', 'NIC Bonding', 'Monitoring', 'CDR', 'Personal Profile Manager (PPM)', and 'Connection Settings'. The 'General' tab is active, showing the following configuration fields: 'SIP Entity Name' (devcon-asm), 'Description' (empty), 'Management Access Point Host Name/IP' (10.32.24.233), and 'Direct Routing to Endpoints' (Enable).

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of the 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.



The screenshot displays a configuration window titled "Security Module" with a dropdown arrow. Below the title, several configuration fields are listed, each with a text input box containing a value:

- SIP Entity IP Address:** 10.32.24.235
- Network Mask:** 255.255.255.0
- Default Gateway:** 10.32.24.1
- Call Control PHB:** 46
- QOS Priority:** 6
- Speed & Duplex:** Auto
- VLAN ID:** (empty field)

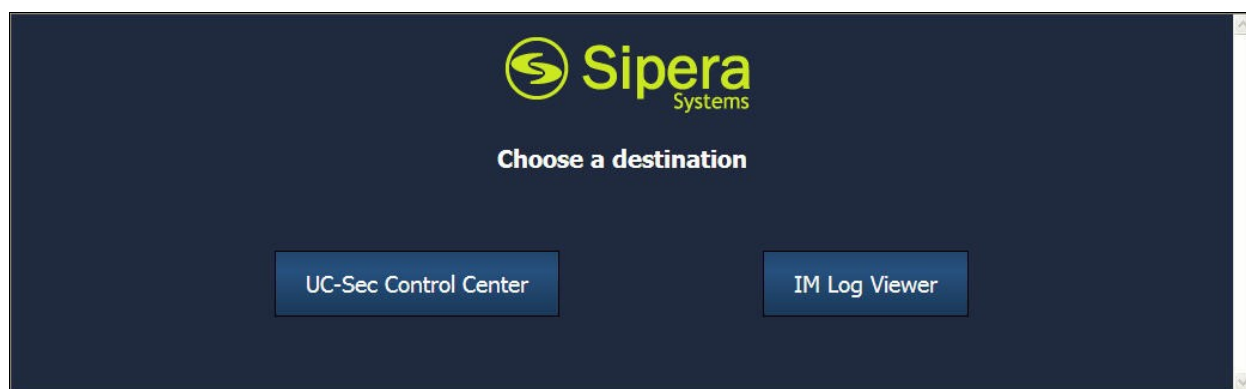
7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, an Avaya SBCE is used as the edge device between the Avaya CPE and CenturyLink SIP Trunking service.

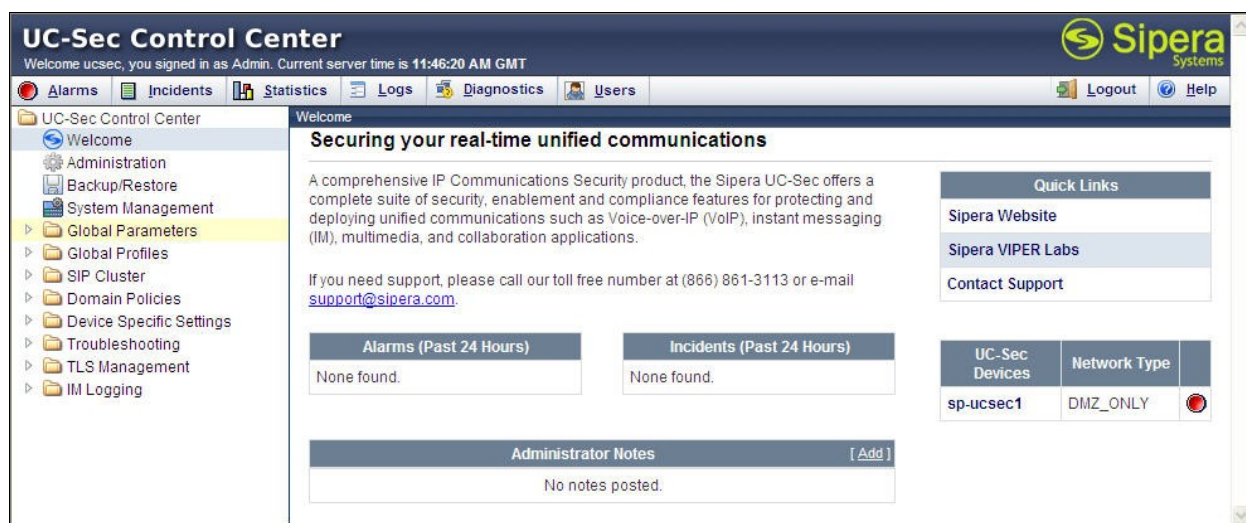
These Application Notes assume that the installation of the SBC and the assignment of a management IP Address have already been completed.

7.1. Access Management Interface

Use a WEB browser to access the web management interface by entering URL `https://<ip-addr>`, where `<ip-addr>` is the management LAN IP address assigned during installation. Select **UC-Sec Control Center** on the displayed web page, and log in using proper login credentials (not shown).



Once logged in, a Welcome screen will be presented. The following image illustrates the menu items available on the left-side of the UC-Sec Control Center screen.

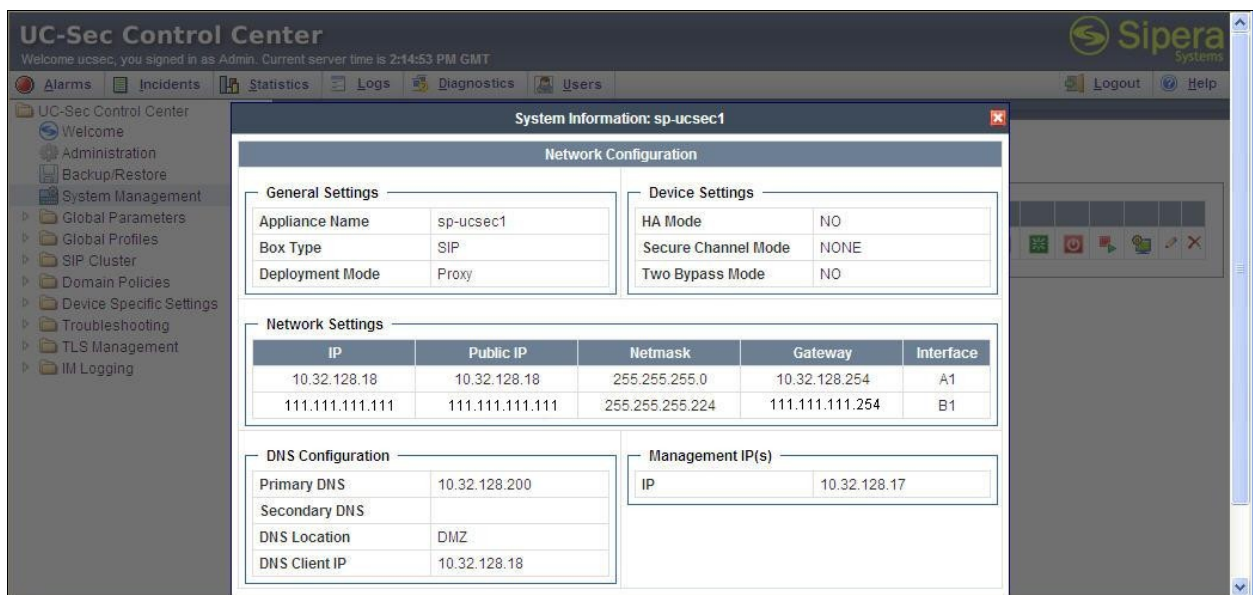


7.2. System Status

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 **sp-ucsec1** is shown. Device **Status** “Commissioned” should be displayed as shown below.



To view the network information of this device assigned during installation, click the **View Config** icon button (the third icon from the right). A **Network Configuration** window is displayed as shown below. Note that the A1 and B1 interface IP addresses correspond to the inside and outside interface IP's for the Avaya SBCE as shown in **Figure 1**.



7.3. Global Profiles – Server Interworking

Server interworking is defined for each server connected to Avaya SBCE. For the compliance test, the CenturyLink network-edge SBC serves as the Trunk Server and the Session Manager serves as the Call Server.

Navigate to **Global Profiles → Server Interworking** from the left-side menu to configure Server Interworking profiles.

7.3.1. Server Interworking: Avaya-SM

Click the **Add Profile** button (not shown) to add a new profile or select an existing Server Interworking profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate **Profile Name** such as *Avaya-SM* shown below. Click **Next**.



The screenshot shows a window titled "Interworking Profile" with a close button in the top right corner. Inside the window, there is a text input field labeled "Profile Name" which contains the text "Avaya-SM". Below the input field is a button labeled "Next".

The following screens illustrate the **General** parameters used in the sample configuration for the Interworking Profile named “Avaya-SM”. Most parameters retain default values. In the sample configuration, **T.38 Support** was checked (this parameter could be unchecked since CenturyLink does not support T.38 fax; it was checked here since the profile was configured for shared use), and **Hold Support** was set for *RFC3264*.

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

Click **Next** (not shown) to advance to configure **Privacy** and **DTMF** general parameters, which can retain default values. The following screen shows the complete **General** tab used in the sample configuration for interworking profile named “Avaya-SM”

| | | Rename Profile | Clone Profile | Delete Profile |
|--|---------|----------------|---------------|----------------|
| Click here to add a description. | | | | |
| <div> <div>General</div> <div>Timers</div> <div>URI Manipulation</div> <div>Header Manipulation</div> <div>Advanced</div> </div> | | | | |
| General | | | | |
| Hold Support | RFC3264 | | | |
| 180 Handling | None | | | |
| 181 Handling | None | | | |
| 182 Handling | None | | | |
| 183 Handling | None | | | |
| Refer Handling | No | | | |
| 3xx Handling | No | | | |
| Diversion Header Support | No | | | |
| Delayed SDP Handling | No | | | |
| T.38 Support | Yes | | | |
| URI Scheme | SIP | | | |
| Via Header Format | RFC3261 | | | |
| Privacy | | | | |
| Privacy Enabled | No | | | |
| User Name | | | | |
| P-Asserted-Identity | No | | | |
| P-Preferred-Identity | No | | | |
| Privacy Header | | | | |
| DTMF | | | | |
| DTMF Support | None | | | |

The parameters in all other tabs may retain default settings.

7.3.2. Server Interworking: SP-CTL

A second Server Interworking profile named “SP-CTL” was similarly created. The following screens illustrate the **General** parameters used in the sample configuration for the “SP-CTL” Server Interworking profile. Most parameters retain default values. In the sample configuration, **T.38 Support** was set to *Yes* (this parameter could be unchecked since CenturyLink does not support T.38 fax; it was checked here since the profile was configured for shared use) and **Hold Support** was set for *RFC3264*.

| General | Timers | URI Manipulation | Header Manipulation | Advanced |
|--------------------------|---------|------------------|---------------------|----------|
| General | | | | |
| Hold Support | RFC3264 | | | |
| 180 Handling | None | | | |
| 181 Handling | None | | | |
| 182 Handling | None | | | |
| 183 Handling | None | | | |
| Refer Handling | No | | | |
| 3xx Handling | No | | | |
| Diversion Header Support | No | | | |
| Delayed SDP Handling | No | | | |
| T.38 Support | Yes | | | |
| URI Scheme | SIP | | | |
| Via Header Format | RFC3261 | | | |
| Privacy | | | | |
| Privacy Enabled | No | | | |
| User Name | | | | |
| P-Asserted-Identity | No | | | |
| P-Preferred-Identity | No | | | |
| Privacy Header | | | | |
| DTMF | | | | |
| DTMF Support | None | | | |
| Edit | | | | |

The parameters in all other tabs may retain default settings.

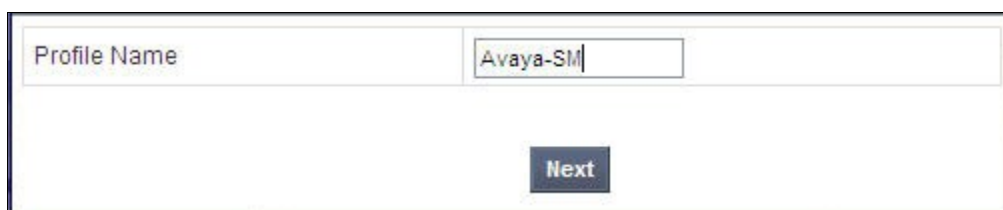
7.4. Global Profiles – Server Configuration

In the compliance test, the CenturyLink network-edge SBC is connected as the Trunk Server and the enterprise Session Manager is connected as the Call Server.

Navigate to **Global Profiles → Server Configuration** from the left-side menu to configure the 2 servers.

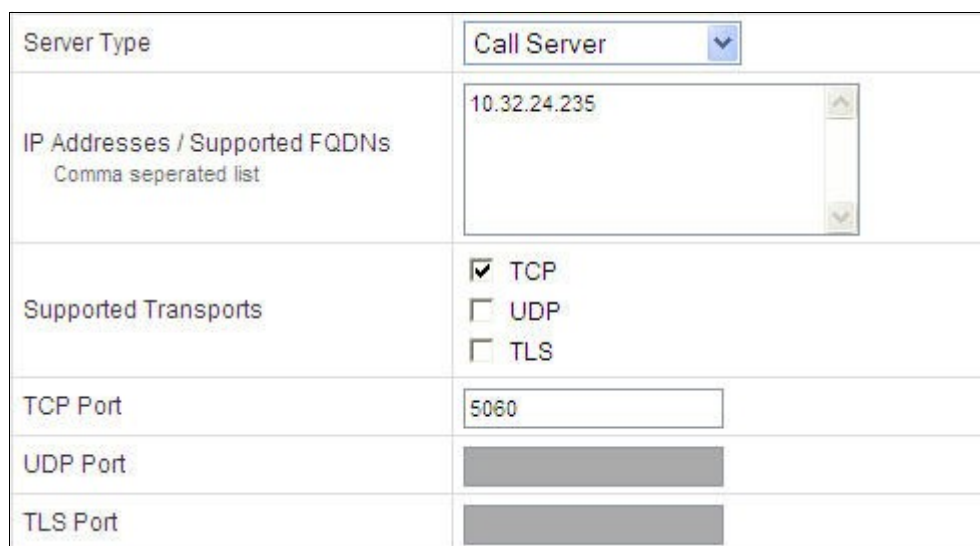
7.4.1. Server Configuration for Session Manager

Click the **Add Profile** button (not shown) to add a new profile, or select an existing profile to edit. If adding a profile, a screen such as the following is displayed. Enter an appropriate Profile Name such as *Avaya-SM* shown below. Click **Next**.



| | |
|--------------|----------|
| Profile Name | Avaya-SM |
| Next | |

The following screens illustrate the Server Configuration with Profile name “Avaya-SM”. Select **Call Server** from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the IP Address of the Session Manager SIP signaling interface should be entered. In the **Supported Transports** area, **TCP** is selected, and the **TCP Port** is set to **5060**. This configuration corresponds with the Session Manager Entity Link configuration for the Entity Link connecting to the SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish** (buttons not shown).



| | |
|--|---|
| Server Type | Call Server |
| IP Addresses / Supported FQDNs Comma separated list | 10.32.24.235 |
| Supported Transports | <input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS |
| TCP Port | 5060 |
| UDP Port | |
| TLS Port | |

Once configuration is completed, the **General** tab for the configured “Avaya-SM” Call Server will appear as shown below.

| | | | |
|---------|----------------|-----------|----------|
| General | Authentication | Heartbeat | Advanced |
|---------|----------------|-----------|----------|

| General | |
|----------------------|--------------|
| Server Type | Call Server |
| IP Addresses / FQDNs | 10.32.24.235 |
| Supported Transports | TCP |
| TCP Port | 5060 |

Edit

If adding the profile, click **Next** to accept default parameters for the **Authentication** tab, and advance to the **Heartbeat** area. If editing an existing profile, select the **Heartbeat** tab and click **Edit**.

The SBC can be configured to source “heartbeats” in the form of SIP OPTIONS. In the sample configuration, with one connected Session Manager, this configuration is optional.

If SBC-sourced OPTIONS messages are desired, check the **Enable Heartbeat** box. Select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS to this server. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC toward Session Manager. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.

| | |
|---------------------|-------------------------------------|
| Enable Heartbeat | <input checked="" type="checkbox"/> |
| Method | OPTIONS ▼ |
| Frequency | 60 seconds |
| From URI | ping@10.32.128.18 |
| To URI | ping@10.32.24.235 |
| TCP Probe | <input type="checkbox"/> |
| TCP Probe Frequency | seconds |

Finish

If SBC sourced OPTIONS is configured, the **Heartbeat** tab for the “Avaya-SM” server profile will appear as shown below.

| | | | |
|------------------|----------------|-------------------------------------|----------|
| General | Authentication | Heartbeat | Advanced |
| Heartbeat | | | |
| Enable Heartbeat | | <input checked="" type="checkbox"/> | |
| Method | | OPTIONS | |
| Frequency | | 60 seconds | |
| From URI | | ping@10.32.128.18 | |
| To URI | | ping@10.32.24.235 | |
| TCP Probe | | <input type="checkbox"/> | |
| Edit | | | |

If adding a profile, click **Next** to continue to the **Advanced** settings. If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select the **Interworking Profile** *Avaya-SM* created in **Section 7.3.1**. Click **Finish**.

| | |
|-------------------------------|---|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input type="checkbox"/> |
| Interworking Profile | Avaya-SM <input type="button" value="v"/> |
| Signaling Manipulation Script | None <input type="button" value="v"/> |
| TCP Connection Type | <input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING |
| Finish | |

Once configuration is completed, the **Advanced** tab for the call server “Avaya-SM” will appear as shown below.

| | | | | | | | | | | | | | |
|---|--------------------------|-----------|----------|-----------------------|--------------------------|-----------------|--------------------------|----------------------|----------|-------------------------------|------|---------------------|-------|
| General | Authentication | Heartbeat | Advanced | | | | | | | | | | |
| <div>Advanced</div> <table><tr><td>Enable DoS Protection</td><td><input type="checkbox"/></td></tr><tr><td>Enable Grooming</td><td><input type="checkbox"/></td></tr><tr><td>Interworking Profile</td><td>Avaya-SM</td></tr><tr><td>Signaling Manipulation Script</td><td>None</td></tr><tr><td>TCP Connection Type</td><td>SUBID</td></tr></table> <div>Edit</div> | | | | Enable DoS Protection | <input type="checkbox"/> | Enable Grooming | <input type="checkbox"/> | Interworking Profile | Avaya-SM | Signaling Manipulation Script | None | TCP Connection Type | SUBID |
| Enable DoS Protection | <input type="checkbox"/> | | | | | | | | | | | | |
| Enable Grooming | <input type="checkbox"/> | | | | | | | | | | | | |
| Interworking Profile | Avaya-SM | | | | | | | | | | | | |
| Signaling Manipulation Script | None | | | | | | | | | | | | |
| TCP Connection Type | SUBID | | | | | | | | | | | | |

7.4.2. Server Configuration for CenturyLink SIP Trunking

A second Server Configuration profile named “SP-CTL” was similarly created. The following screens illustrate the “SP-CTL” Server Configuration profile. In the “General” parameters, select **Trunk Server** from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the CenturyLink-provided SIP Trunking service network IP Address is entered. In the **Supported Transports** area, **UDP** is selected, and the **UDP Port** is set to **6003** as specified by CenturyLink.

| | |
|---|---|
| Server Type | Trunk Server |
| IP Addresses / Supported FQDNs <small>Comma seperated list</small> | 222.222.222.2222 |
| Supported Transports | <input type="checkbox"/> TCP <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TLS |
| TCP Port | |
| UDP Port | 6003 |
| TLS Port | |
| <input type="button" value="Finish"/> | |

If adding the profile, click **Next** to accept default parameters for the **Authentication** tab, and advance to the **Heartbeat** area. If editing an existing profile, select the **Heartbeat** tab and click edit.

The SBC can be configured to source “heartbeats” in the form of SIP OPTIONS towards CenturyLink. This configuration is optional. Independent of whether the SBC is configured to source SIP OPTIONS towards CenturyLink, CenturyLink will receive OPTIONS from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. When Session Manager sends SIP OPTIONS to the inside private IP Address of the SBC, the SBC will send SIP OPTIONS to CenturyLink. When CenturyLink responds, the SBC will pass the response to Session Manager.

If SBC-sourced OPTIONS is desired, select **OPTIONS** from the **Method** drop-down menu. Select the desired frequency that the SBC will source OPTIONS. The **From URI** and **To URI** may be filled in to configure easily identifiable URIs to appear in SIP OPTIONS sourced by the SBC. If adding a new profile, click **Next**. If editing an existing profile, click **Finish**.

Edit Server Configuration Profile - Heartbeat

| | |
|---------------------|-------------------------------------|
| Enable Heartbeat | <input checked="" type="checkbox"/> |
| Method | OPTIONS |
| Frequency | 60 seconds |
| From URI | ping@111.111.111.111 |
| To URI | ping@222.222.222.222 |
| TCP Probe | <input type="checkbox"/> |
| TCP Probe Frequency | seconds |

Finish

If the optional SBC sourced OPTIONS configuration is completed, the **Heartbeat** tab for the “SP-CTL” server profile will appear as shown below.

| | | | |
|------------------|----------------|-------------------------------------|----------|
| General | Authentication | Heartbeat | Advanced |
| Heartbeat | | | |
| Enable Heartbeat | | <input checked="" type="checkbox"/> | |
| Method | | OPTIONS | |
| Frequency | | 60 seconds | |
| From URI | | ping@111.111.111.111 | |
| To URI | | ping@222.222.222.222 | |
| TCP Probe | | <input type="checkbox"/> | |
| Edit | | | |

If adding a profile, click **Next** to continuing to the **Advanced** settings. If editing an existing profile, select the **Advanced** tab and **Edit**. In the resultant screen, select the **Interworking Profile** “SP-CTL” created in **Section 7.3.2**. Click **Finish**.

| | |
|---|---|
| Edit Server Configuration Profile - Advanced | |
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input type="checkbox"/> |
| Interworking Profile | SP-CTL <input type="button" value="v"/> |
| Signaling Manipulation Script | None <input type="button" value="v"/> |
| UDP Connection Type | <input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING |
| Finish | |

Once configuration is completed, the **Advanced** tab for “SP-CTL” will appear as shown below.

The screenshot shows a configuration interface with four tabs: General, Authentication, Heartbeat, and Advanced. The Advanced tab is selected and displays a table with the following settings:

| Advanced | |
|-------------------------------|--------------------------|
| Enable DoS Protection | <input type="checkbox"/> |
| Enable Grooming | <input type="checkbox"/> |
| Interworking Profile | SP-CTL |
| Signaling Manipulation Script | None |
| UDP Connection Type | SUBID |

Below the table is an **Edit** button.

7.5. Global Profiles – Routing

Routing information is required for routing to Session Manager on the internal side and CenturyLink network on the external side. The IP addresses and ports defined here will be used as the destination addresses for signaling. If no port is specified, default 5060 is used.

Navigate to **Global Profiles → Routing** from the left-side menu to configure Routing profiles.

7.5.1. Routing Configuration for Session Manager

Click the **Add Profile** button (not shown) to add a new profile, or select an existing routing profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as *To_SM* shown below. Click **Next**.

The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "To_SM". Below the input field is a **Next** button.

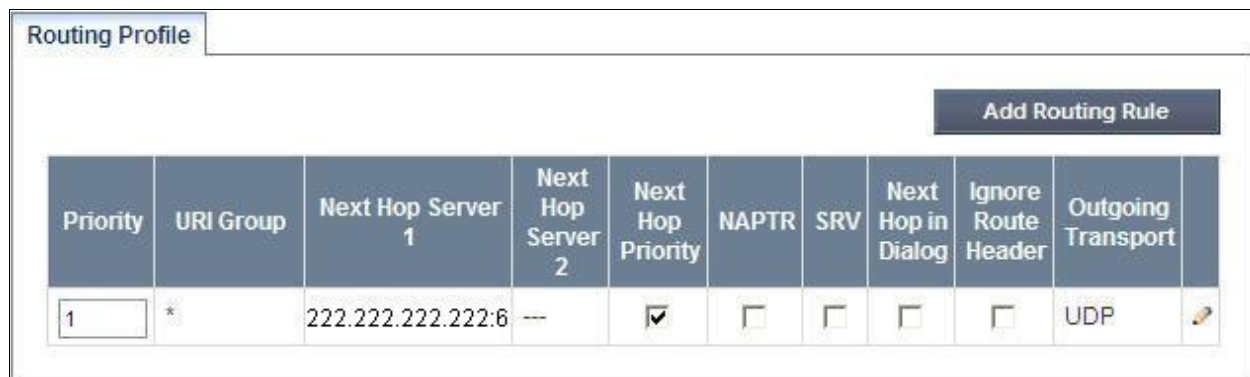
In the **Next Hop Routing** configuration, enter the IP Address of the Session Manager SIP signaling interface with port number (optional if port number is 5060) as **Next Hop Server 1**, as shown below. Check **Routing Priority based on Next Hop Server**. Choose **TCP** for **Outgoing Transport**.

Once configuration is completed, the **Routing Profile** for “To_SM” will appear as follows.

| Routing Profile | | | | | | | | | | |
|-----------------|-----------|-------------------|-------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------|------------------|
| | | | | | | | | | | Add Routing Rule |
| Priority | URI Group | Next Hop Server 1 | Next Hop Server 2 | Next Hop Priority | NAPTR | SRV | Next Hop in Dialog | Ignore Route Header | Outgoing Transport | |
| 1 | * | 10.32.24.235:5060 | -- | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | TCP | |

7.5.2. Routing Configuration for CenturyLink SIP Trunking

A Routing Profile named “To_SP1” for the trunk server was similarly configured as shown below (the partially displayed port number is 6003 in **Next Hop Server 1**, see [Section 7.4.2](#)).



The screenshot shows a web interface for configuring a Routing Profile. At the top, there is a tab labeled "Routing Profile" and a button labeled "Add Routing Rule". Below this is a table with the following columns: Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. The first row of the table contains the following values: Priority: 1, URI Group: *, Next Hop Server 1: 222.222.222.222:6, Next Hop Server 2: --, Next Hop Priority: ☒, NAPTR: ☐, SRV: ☐, Next Hop in Dialog: ☐, Ignore Route Header: ☐, and Outgoing Transport: UDP. There is a small edit icon (pencil) at the end of the first row.

| 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 | * | 222.222.222.222:6 | -- | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | UDP |

7.6. Global Profiles – Topology Hiding

Topology Hiding is a security feature which allows changing several parameters of the SIP packets, preventing private enterprise network information from being propagated to the un-trusted public network.

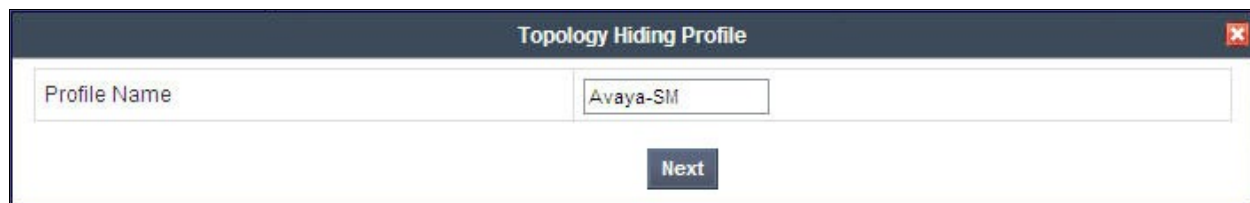
Topology Hiding can also be used as an interoperability tool to adapt the host portion in selected SIP headers to meet expectations by Session Manager and the SIP trunk service provider, allowing the call to be accepted in each case.

For the compliance test, only the minimum configuration required to achieve interoperability was performed.

Navigate to **Global Profiles → Topology Hiding** from the left-side menu for configuring Topology Hiding profiles.

7.6.1. Topology Hiding for Session Manager

Click the **Add Profile** button (not shown) to add a new profile, or select an existing topology hiding profile to edit. If adding a profile, a screen such as the following is displayed. Enter a **Profile Name** such as *Avaya-SM* shown below. Click **Next**.



The screenshot shows a web form titled "Topology Hiding Profile". It has a text input field labeled "Profile Name" with the value "Avaya-SM" entered. Below the input field is a button labeled "Next".

In the resultant screen, click the **Add Header** button to reveal additional headers.

| | | | | Add Header |
|--------------|-----------|----------------|-----------------|------------|
| Header | Criteria | Replace Action | Overwrite Value | |
| Request-Line | IP/Domain | Auto | | ✗ |

To ensure that the domain received by Session Manager from the SBC is the expected enterprise domain, select “Overwrite” as the **Replace Action** for the To, From, and Request-Line headers. Enter the enterprise domain in the **Overwrite Value** column as shown below. In the example below, the domain received by Session Manager is changed by the SBC to “avaya.com”. Click **Finish**.

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

Finish

After configuration is completed, the Topology Hiding for profile “Avaya-SM” will appear as follows.

| Topology Hiding | | | |
|-----------------|-----------|----------------|-----------------|
| Header | Criteria | Replace Action | Overwrite Value |
| Via | IP/Domain | Auto | --- |
| To | IP/Domain | Overwrite | avaya.com |
| Request-Line | IP/Domain | Overwrite | avaya.com |
| SDP | IP/Domain | Auto | --- |
| From | IP/Domain | Overwrite | avaya.com |
| Record-Route | IP/Domain | Auto | --- |

Edit

7.6.2. Topology Hiding for CenturyLink SIP Trunking

A Topology Hiding profile named “SP-CTL” for CenturyLink was similarly configured as shown below. Note that the domain in Request-Line, From and To headers will be replaced with the domain “bsoft.nc.labnet” required by CenturyLink.

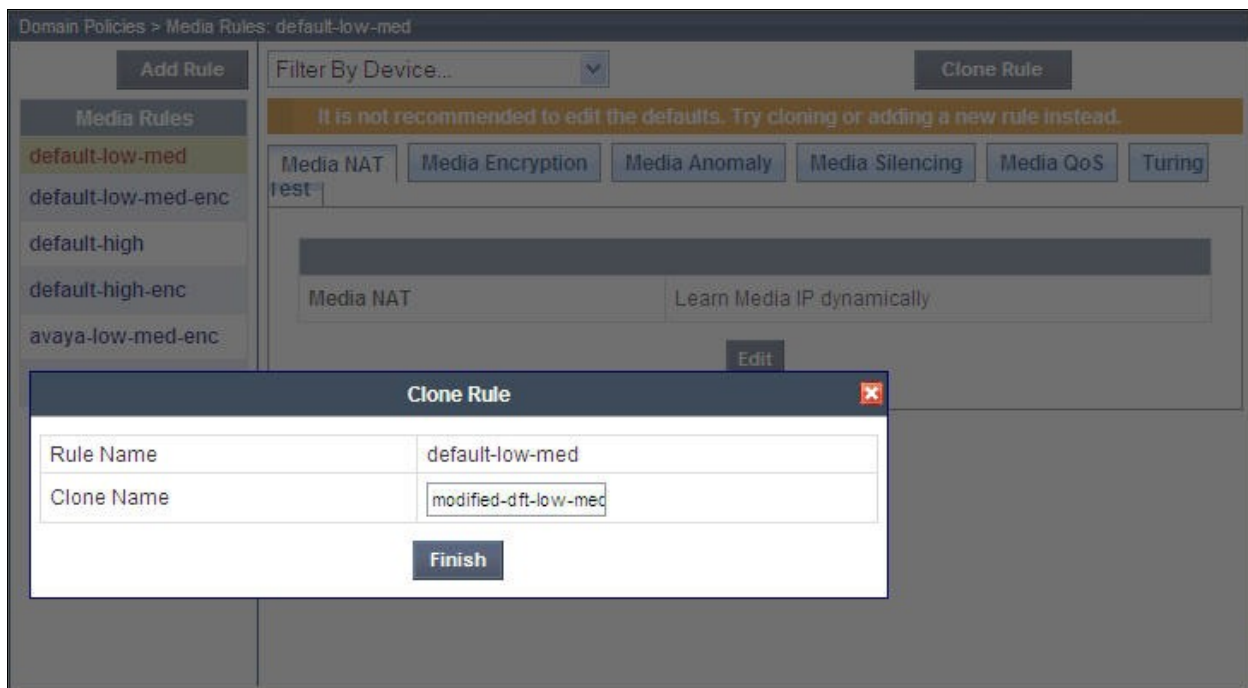
| Topology Hiding | | | |
|-----------------|-----------|----------------|-----------------|
| Header | Criteria | Replace Action | Overwrite Value |
| SDP | IP/Domain | Auto | --- |
| Request-Line | IP/Domain | Overwrite | bsoft.nc.labnet |
| From | IP/Domain | Overwrite | bsoft.nc.labnet |
| Via | IP/Domain | Auto | --- |
| Record-Route | IP/Domain | Auto | --- |
| To | IP/Domain | Overwrite | bsoft.nc.labnet |
| <div>Edit</div> | | | |

7.7. Domain Policies – Media Rules

Domain Policies allow configuring, managing and applying various sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise.

Navigate to **Domain Policies** → **Media Rules** from the left-side menu to configure Media Rules.

In the sample configuration, a single media rule was used. This media rule was cloned from the default rule “default-low-med” by selecting the default rule “default-low-med” then clicking the **Clone Rule** button in the upper right corner as shown below:



Enter a descriptive **Clone Name**, and then click **Finish**. The cloned media rule will be displayed in the **Media Rules** list on the left. Select this cloned rule from the list, then select **Media Anomaly** tab and click **Edit**. In the displayed Media Anomaly edit window, uncheck **Media Anomaly Detection** as shown below.



Click **Finish**. The rule named “modified-dft-low-med” is shown below with the Media Anomaly tab selected. This rule is sufficient for the compliance test. See the **Media Anomaly Detection** item of the observation list in **Section 2.2** on reason for turning off this feature.

7.8. Domain Policies – Signaling Rules

Signaling Rules define the actions to be taken (*Allow, Block, Block with Response*, etc.) on signaling request and response messages. They also allow the control of the Quality of Service of the signaling packets

The P-Location and P-Charging-Vector headers are sent in SIP messages from Session Manager to the service provider network. These headers should not be exposed external to the enterprise. For simplicity, these headers were simply removed (blocked) from both request and response messages originated from Session Manager.

Navigate to **Domain Policies → Signaling Rules** from the left-side menu to configure Signaling Rules.

Click the Add Rule button (not shown) to add a new signaling rule. In the Rule Name field, enter an appropriate name, such as **SM_SigRules**.

In the subsequent screen (not shown), click **Next** to accept defaults. In the Signaling QoS screen, click **Finish** (not shown).

After this configuration, the new “SM_SigRules” rule will appear as follows.

| General | Requests | Responses | Request Headers | Response Headers | Signaling QoS | | | | | | | | |
|--|-------------------------------------|-----------|-----------------|------------------|---------------|---------------|-------------------------------------|----------|-----|------------|---------|-----|----------------|
| <table border="1"> <tr> <td>Signaling QoS</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>QoS Type</td> <td>TOS</td> </tr> <tr> <td>Precedence</td> <td>Routine</td> </tr> <tr> <td>ToS</td> <td>Minimize Delay</td> </tr> </table> | | | | | | Signaling QoS | <input checked="" type="checkbox"/> | QoS Type | TOS | Precedence | Routine | ToS | Minimize Delay |
| Signaling QoS | <input checked="" type="checkbox"/> | | | | | | | | | | | | |
| QoS Type | TOS | | | | | | | | | | | | |
| Precedence | Routine | | | | | | | | | | | | |
| ToS | Minimize Delay | | | | | | | | | | | | |
| <input type="button" value="Edit"/> | | | | | | | | | | | | | |

Select the **Request Headers** tab, and select the **Add In Header Control** button. Check the **Proprietary Request Header?** checkbox. In the **Header Name** field, type “P-Location”. Select “INVITE” as the **Method Name**. In the Header Criteria, select **Forbidden**. Retain **Presence Action** “Remove header”. The intent is to remove the P-Location header which is inserted by Session Manager, but not needed by CenturyLink SIP Trunking service. This configuration is optional in that the P-Location header does not cause any user-perceivable problem if presented to CenturyLink.


Add Header Control
✕

| | | |
|-----------------------------|---|---|
| Proprietary Request Header? | <input checked="" type="checkbox"/> | |
| Header Name | <input type="text" value="P-Location"/> | |
| Method Name | INVITE ▼ | |
| Header Criteria | <input checked="" type="radio"/> Forbidden <input type="radio"/> Mandatory <input type="radio"/> Optional | |
| Presence Action | Remove header ▼ | <input type="button" value="426"/> <input type="button" value="Busy Here"/> |

Similarly, configure additional header control rules to

- Remove the P-Charging-Vector header in the outbound INVITE
- Remove the P-Charging-Vector header in the outbound UPDATE

Once complete, the **Request Headers** tab appears as follows.

| General | Requests | Responses | Request Headers | Response Headers | Signaling QoS | | | |
|---------|-------------------|-------------|-----------------------|------------------|------------------------|-----------|---|---|
| | | | Add In Header Control | | Add Out Header Control | | | |
| Row | Header Name | Method Name | Header Criteria | Action | Proprietary | Direction | | |
| 1 | P-Charging-Vector | INVITE | Forbidden | Remove Header | Yes | IN |  |  |
| 2 | P-Charging-Vector | UPDATE | Forbidden | Remove Header | Yes | IN |  |  |
| 3 | P-Location | INVITE | Forbidden | Remove Header | Yes | IN |  |  |

Select the **Response Headers** tab and repeat the above configuration steps to

- Remove the P-Charging-Vector header in the 200 OK response to INVITE
- Remove the P-Charging-Vector header in the 200 OK response to UPDATE
- Remove the P-Location header in the 200 OK response to INVITE

Once configuration is complete, the **Response Headers** tab for the “SM_SigRules” signaling rule will appear as follows.

| General | Requests | Responses | Request Headers | Response Headers | Signaling QoS | | | | |
|-----------------------|-------------------|---------------|-----------------|------------------------|---------------|-------------|-----------|---|---|
| Add In Header Control | | | | Add Out Header Control | | | | | |
| Row | Header Name | Response Code | Method Name | Header Criteria | Action | Proprietary | Direction | | |
| 1 | P-Charging-Vector | 200 | INVITE | Forbidden | Remove Header | Yes | IN |  |  |
| 2 | P-Charging-Vector | 200 | UPDATE | Forbidden | Remove Header | Yes | IN |  |  |
| 3 | P-Location | 200 | INVITE | Forbidden | Remove Header | Yes | IN |  |  |

7.9. Domain Policies – End Point Policy Groups

End Point Policy Groups are associations of different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the SBC.

Navigate to **Domain Policies → End Point Policy Groups** from the left-side menu as to configure End Point Policy Groups.

Select the **Add Group** button (not shown). Enter a name in the **Group Name** field, such as **SM** as shown below. Click **Next**.

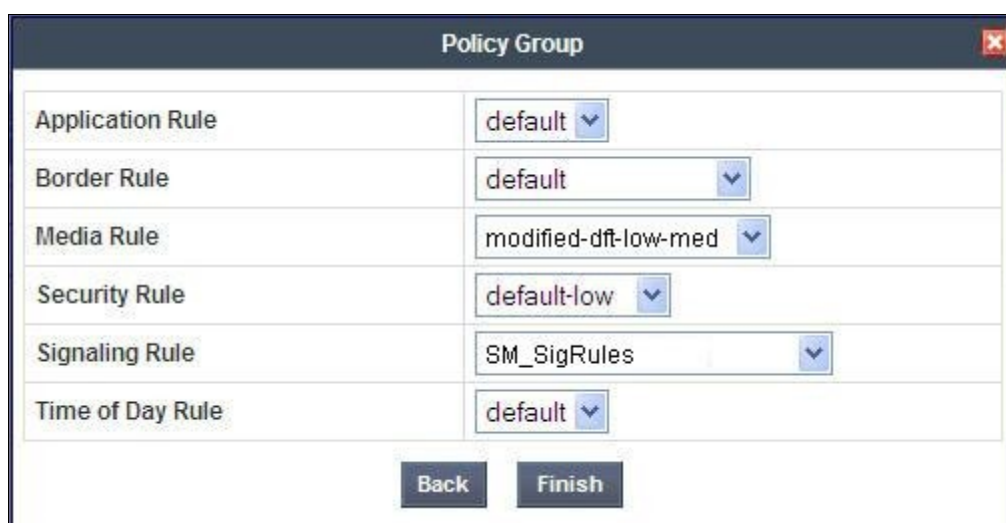


The screenshot shows a window titled "Policy Group" with a close button in the top right corner. Inside the window, there is a form with a label "Group Name" and a text input field containing the text "SM". Below the input field is a button labeled "Next".

In the sample configuration, defaults were selected for all fields, with the exception of

- **Media Rule**, which was set to the “modified-dft-low-med” media rule as defined in **Section 7.7**
- **Signaling Rule**, which was set to the “SM_SigRules” signaling rule as defined in **Section 7.8**

Click **Finish**.



The screenshot shows the "Policy Group" configuration window with several dropdown menus. The "Application Rule" is set to "default", "Border Rule" is set to "default", "Media Rule" is set to "modified-dft-low-med", "Security Rule" is set to "default-low", "Signaling Rule" is set to "SM_SigRules", and "Time of Day Rule" is set to "default". At the bottom of the window, there are two buttons: "Back" and "Finish".

Once configuration is completed, the “SM” End Point Policy Group will appear as follows.

Domain Policies > End Point Policy Groups: SM

Filter By Device... [v] [Rename Group] [Delete Group]

Click here to add a description.

Hover over a row to see its description.

Policy Group

[View Summary] [Add Policy Set]

| Order | Application | Border | Media | Security | Signaling | Time of Day | |
|-------|-------------|---------|----------------------|-------------|-------------|-------------|--------------|
| 1 | default | default | modified-dft-low-med | default-low | SM_SigRules | default | [edit] [add] |

Repeat the above configuration steps to create a 2nd End Point Policy Group named “General-SP” for the network side as shown below.

Note that this End Point Policy Group uses the same Media Rule (“modified-dft-low-med”) for disabling Media Anomaly Detection and the default Signaling Rule since no header manipulations are required for messages to and from the outside interface of the SBC.

Domain Policies > End Point Policy Groups: General-SP

Filter By Device... [v] [Rename Group] [Delete Group]

Click here to add a description.

Hover over a row to see its description.

Policy Group

[View Summary] [Add Policy Set]

| Order | Application | Border | Media | Security | Signaling | Time of Day | |
|-------|-------------|---------|----------------------|-------------|-----------|-------------|--------------|
| 1 | default | default | modified-dft-low-med | default-low | default | default | [edit] [add] |

7.10. Device Specific Settings – Network Management

The network information should have been previously specified during installation of Avaya SBCE.

Navigate to **Device Specific Setting → Network Management** from the left-side menu.

Under **UC-Sec Devices**, select the device being managed, which was named “sp-ucsec1” in the sample configuration (not shown). The **Network Configuration** tab is shown below. Observe the **IP Address**, **Netmask**, **Gateway**, and **Interface** information previously assigned. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for the external side of the Avaya SBCE.

Network Configuration

Interface Configuration

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

A1 Netmask

255.255.255.0

A2 Netmask

B1 Netmask

255.255.255.224

B2 Netmask

Add IP

Changes will not take effect until the interface is updated.

Save Changes

Clear Changes

| IP Address | Public IP | Gateway | Interface | |
|-----------------|-----------|-----------------|-----------|---|
| 10.32.128.18 | | 10.32.128.254 | A1 | ✖ |
| 111.111.111.111 | | 111.111.111.254 | B1 | ✖ |

Select the **Interface Configuration** tab. The **Administrative Status** can be toggled between **Enabled** and **Disabled** in this screen. The following screen was captured after the interfaces had already been enabled. To enable the interface if it is disabled, click the **Toggle State** button.

| Network Configuration | | Interface Configuration |
|-----------------------|-----------------------|-------------------------|
| Name | Administrative Status | |
| A1 | Enabled | <div>Toggle State</div> |
| A2 | Disabled | <div>Toggle State</div> |
| B1 | Enabled | <div>Toggle State</div> |
| B2 | Disabled | <div>Toggle State</div> |

When the IP addresses and masks are assigned to the interfaces, these are then configured as signaling and media interfaces.

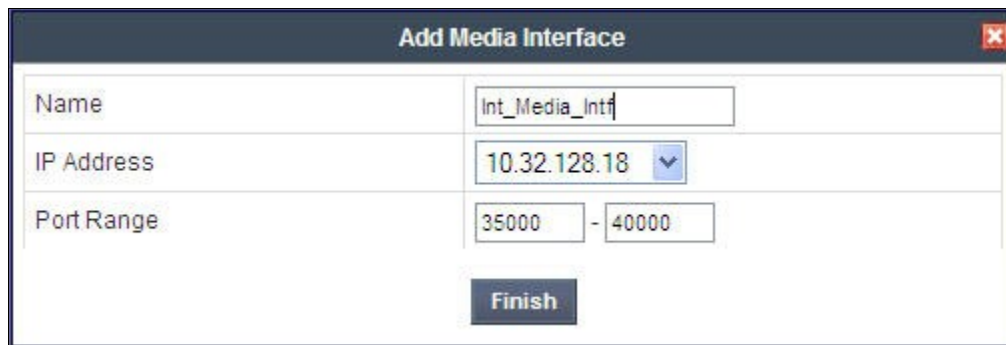
7.11. Device Specific Settings – Media Interface

Media Interfaces are created to adjust the port range assigned to media streams leaving the interfaces of the SBC. The compliance test used the port range 35000 to 40000 for both the private interface and the public interface.

Navigate to **Device Specific Setting → Media Interface** from the left-side menu to configure Media Interfaces, one for internal and one for external.

Under **UC-Sec Devices**, select the device being managed, which was named “sp-ucsec1” in the sample configuration (not shown). Select **Add Media Interface**.

Enter an appropriate **Name** for the Media Interface facing the enterprise and select the inside private IP Address from the **IP Address** drop-down menu. In the sample configuration, **Int_Media_Intf** is chosen as the name, and the inside IP Address of the SBC is **10.32.128.18**. For the **Port Range**, default values are shown. Click **Finish**.



The screenshot shows a web-based configuration window titled "Add Media Interface" with a close button (X) in the top right corner. The window contains three input fields: "Name" with the text "Int_Media_Intf", "IP Address" with a dropdown menu showing "10.32.128.18", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center of the form.

An external Media Interface facing the network was similarly created with name **Ext_Media_Intf** and the outside IP Address of the SBC **111.111.111.111** as shown below. Same **Port Range** setting was used as for the internal Media Interface.



The screenshot shows a web-based configuration window titled "Add Media Interface" with a close button (X) in the top right corner. The window contains three input fields: "Name" with the text "Ext_Media_Intf", "IP Address" with a dropdown menu showing "111.111.111.111", and "Port Range" with two input boxes containing "35000" and "40000" separated by a hyphen. A "Finish" button is located at the bottom center of the form.

The resultant Media Interface configuration used in the sample configuration is shown below.

Media Interface

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

Add Media Interface

| Name | Media IP | Port Range | | |
|----------------|-----------------|---------------|--|--|
| Int_Media_Intf | 10.32.128.18 | 35000 - 40000 | | |
| Ext_Media_Intf | 111.111.111.111 | 35000 - 40000 | | |

7.12. Device Specific Settings – Signaling Interface

Navigate to **Device Specific Setting** → **Signaling Interface** from the left-side menu to configure Signaling Interfaces, one for internal and one for external.

Under **UC-Sec Devices**, select the device being managed, which was named “sp-ucsec1” in the sample configuration (not shown). Select **Add Signaling Interface**.

In the **Add Signaling Interface** screen, enter an appropriate **Name** (e.g., *Int_Sig_Intf*) for the inside interface, and choose the private inside IP Address from the **IP Address** drop-down menu. Enter **5060** for **TCP Port** since TCP and port 5060 is used between Session Manager and the SBC in the sample configuration. Click **Finish**.

Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.

| | |
|--|--------------------------|
| Name | Int_Sig_Intf |
| IP Address | 10.32.128.18 |
| TCP Port <small>Leave blank to disable</small> | 5060 |
| UDP Port <small>Leave blank to disable</small> | |
| TLS Port <small>Leave blank to disable</small> | |
| Cluster TLS <small>Only for use with Cisco SIP Clusters</small> | <input type="checkbox"/> |
| Enable Stun <small>Requires a UDP Port</small> | <input type="checkbox"/> |

Finish

An external Signaling Interface facing the network was similarly created with name **Ext_Sig_Intf** and the outside IP Address of the SBC **111.111.111.111** as shown below. Note that **5060** was specified for **UDP Port** since UDP was used between the SBC and the CenturyLink network.

Only Cluster TLS is available because no TLS Server Profiles exist. There is no restriction on non-TLS profiles.





| | |
|--|--------------------------|
| Name | Ext_Sig_Intf |
| IP Address | 111.111.111.111▼ |
| TCP Port <small>Leave blank to disable</small> | |
| UDP Port <small>Leave blank to disable</small> | 5060 |
| TLS Port <small>Leave blank to disable</small> | |
| Cluster TLS <small>Only for use with Cisco SIP Clusters</small> | <input type="checkbox"/> |
| Enable Stun <small>Requires a UDP Port</small> | <input type="checkbox"/> |

Finish

The following screen shows the Signaling Interfaces defined for the sample configuration.

Signaling Interface

Add Signaling Interface

| Name | Signaling IP | TCP Port | UDP Port | TLS Port | TLS Profile | | |
|--------------|-----------------|----------|----------|----------|-------------|---|---|
| Int_Sig_Intf | 10.32.128.18 | 5060 | --- | --- | None |  |  |
| Ext_Sig_Intf | 111.111.111.111 | --- | 5060 | --- | None |  |  |

7.13. Device Specific Settings – End Point Server Flows

End Point Server Flows combine the previously defined profiles into an outgoing flow from the Call Server (Session Manager) to the Trunk Server (service provider network) and an incoming flow from the Trunk Server to the Call Server. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the service provider network and vice versa.

Select **Device Specific Setting → End Point Flows** from the left-side menu to configure End Point Flows.

Under **UC-Sec Devices**, select the device being managed, which was named “sp-ucsec1” in the sample configuration (not shown). Select the **Server Flows** tab. Select **Add Flow**.

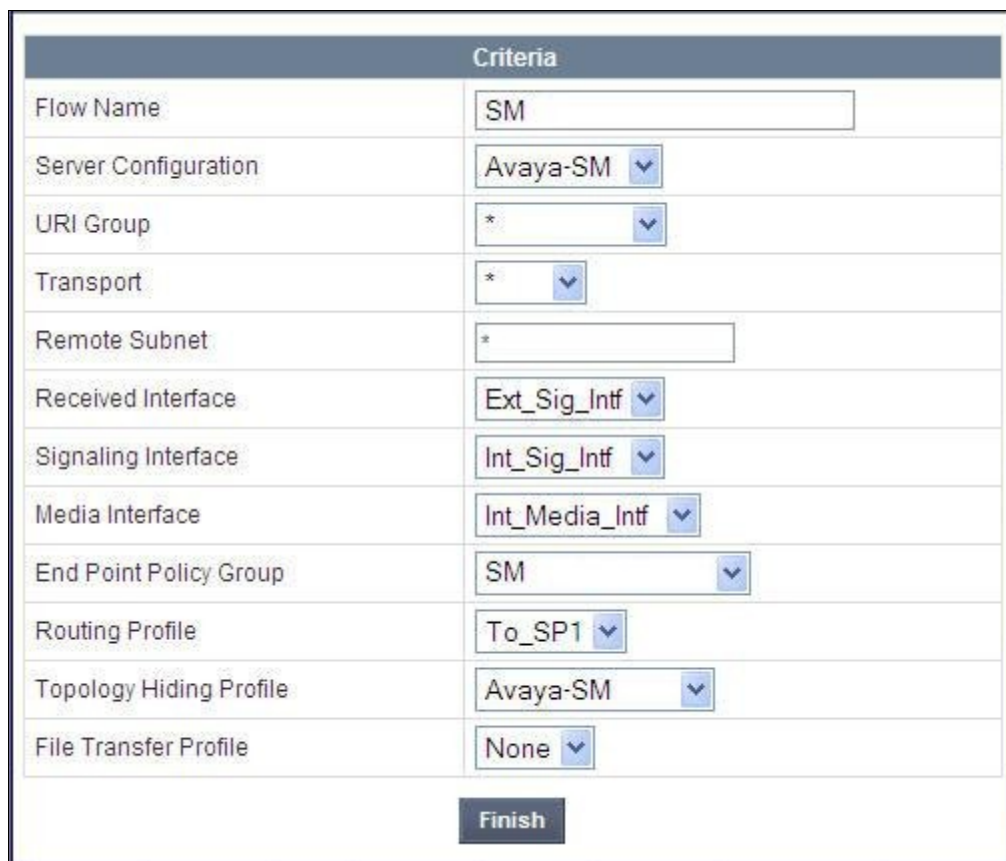


End Point Flows: Sipera-outside-1112

Subscriber Flows Server Flows

Add Flow

The following screen shows the flow named **SM** being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection which is the reverse route of the flow. Click **Finish**.



| Criteria | |
|-------------------------|----------------|
| Flow Name | SM |
| Server Configuration | Avaya-SM |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | Ext_Sig_Intf |
| Signaling Interface | Int_Sig_Intf |
| Media Interface | Int_Media_Intf |
| End Point Policy Group | SM |
| Routing Profile | To_SP1 |
| Topology Hiding Profile | Avaya-SM |
| File Transfer Profile | None |

Finish

Once again, select the **Server Flows** tab. Select **Add Flow**.

The following screen shows the flow named **CTL** being added to the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection which is the reverse route of the flow. Click **Finish**.

| Criteria | |
|-------------------------|----------------|
| Flow Name | CTL |
| Server Configuration | SP-CTL |
| URI Group | * |
| Transport | * |
| Remote Subnet | * |
| Received Interface | Int_Sig_Intf |
| Signaling Interface | Ext_Sig_Intf |
| Media Interface | Ext_Media_Intf |
| End Point Policy Group | General-SP |
| Routing Profile | To_SM |
| Topology Hiding Profile | SP-CTL |
| File Transfer Profile | None |
| Finish | |

The following screen summarizes the Server Flows configured in the sample configuration.

Subscriber Flows
Server Flows
Add Flow

Click here to add a row description.

Server Configuration: Avaya-SM

| Priority | Flow Name | URI Group | Transport | Remote Subnet | Received Interface | Signaling Interface | Media Interface | End Point Policy Group | Routing Profile | Topology Hiding Profile | File Transfer Profile | | | |
|----------|-----------|-----------|-----------|---------------|--------------------|---------------------|-----------------|------------------------|-----------------|-------------------------|-----------------------|--|--|--|
| 1 | SM | * | * | * | Ext_Sig_Intf | Int_Sig_Intf | Int_Media_Intf | SM | To_SP1 | Avaya-SM | None | | | |

Server Configuration: SP-CTL

| Priority | Flow Name | URI Group | Transport | Remote Subnet | Received Interface | Signaling Interface | Media Interface | End Point Policy Group | Routing Profile | Topology Hiding Profile | File Transfer Profile | | | |
|----------|-----------|-----------|-----------|---------------|--------------------|---------------------|-----------------|------------------------|-----------------|-------------------------|-----------------------|--|--|--|
| 1 | CTL | * | * | * | Int_Sig_Intf | Ext_Sig_Intf | Ext_Media_Intf | General-SP | To_SM | SP-CTL | None | | | |

8. CenturyLink BroadWorks SIP Trunk Configuration

To use CenturyLink BroadWorks SIP Trunk, a customer must request the service from CenturyLink using the established sales and provisioning processes.

During the signup process, CenturyLink will require that the customer provide the public IP address used to reach the SBC at the edge of the enterprise and information related to SIP configuration supported by the enterprise. CenturyLink will provide the IP address of the CenturyLink SIP proxy/SBC, transport protocol and listening port for the SIP connection to the enterprise, IP addresses of media sources, and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete the configurations of Communication Manager, Session Manager, and Avaya SBCE discussed in the previous sections.

The configuration between CenturyLink BroadWorks SIP Trunk and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the CenturyLink network.

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.

Verification Steps:

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active with 2-way audio path.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call remains active with 2-way audio path.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

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 group number> - Displays trunk group information.
- **status trunk** <trunk group number/channel number> - Displays signaling and media information for an active trunk channel.

2. Session Manager:

- **System State** – Navigate to **Home** → **Elements** → **Session Manager**, as shown below. Verify that for the Session Manager of interest, a green check mark is placed under **Tests Pass** and the **Service State** is **Accept New Service**.

The screenshot displays the Session Manager Dashboard. On the left is a navigation menu with options: Session Manager, Dashboard, Session Manager, Administration, Communication Profile Editor, Network Configuration, Device and Location Configuration, Application Configuration, System Status, and System Tools. The main content area is titled 'Session Manager Dashboard' and includes a breadcrumb trail 'Home / Elements / Session Manager- Session Manager'. Below the title is a description: 'This page provides the overall status and health summary of each administered Session Manager.' A section titled 'Session Manager Instances' contains two dropdown menus for 'Service State' and 'Shutdown System', and a timestamp 'As of 11:13 AM'. Below this is a table with 4 items, showing details for four Session Manager instances. The table columns are: Session Manager, Type, Alarms, Tests Pass, Security Module, Service State, Entity Monitoring, Active Call Count, Registrations, and Version. The first instance, BR110-SM, has 48/47/264 alarms, tests pass (green check), security module is Up, service state is Accept New Service, 3/5 entity monitoring, 0 active call count, 0 registrations, and version 6.1.5.0.615006. The second instance, BR110-SMH, has 14/13/13 alarms, tests fail (red X), security module is ---, service state is ---, 0 entity monitoring, 0 active call count, 0 registrations, and version ---. The third instance, Dev4 SM, has 62/10/420 alarms, tests fail (red X), security module is ---, service state is ---, 0 entity monitoring, 0 active call count, 0 registrations, and version ---. The fourth instance, devcon-asm, has 23/19/882 alarms, tests pass (green check), security module is Up, service state is Accept New Service, 3/14 entity monitoring, 0 active call count, 0 registrations, and version 6.1.5.0.615006. At the bottom of the table, there is a 'Select : All, None' option.

| Session Manager | Type | Alarms | Tests Pass | Security Module | Service State | Entity Monitoring | Active Call Count | Registrations | Version |
|----------------------------|------|-----------|------------|-----------------|--------------------|-------------------|-------------------|---------------|----------------|
| BR110-SM | Core | 48/47/264 | ✓ | Up | Accept New Service | 3/5 | 0 | 0 | 6.1.5.0.615006 |
| BR110-SMH | Core | 14/13/13 | ✗ | --- | --- | --- | --- | 0 | --- |
| Dev4 SM | Core | 62/10/420 | ✗ | --- | --- | --- | --- | --- | --- |
| devcon-asm | Core | 23/19/882 | ✓ | Up | Accept New Service | 3/14 | 0 | 0 | 6.1.5.0.615006 |

- **traceSM -x** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
 - **Call Routing Test** - The Call Routing Test verifies routing for a particular source and destination. To run the routing test, navigate to **Home → Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run tests.
3. Avaya SBC for Enterprise
- **OPTIONS** – Disable the SBC-sourced OPTIONS to the trunk server (see **Section 7.4.2**) and use a network sniffer like Wireshark to verify that the service provider network will receive OPTIONS forwarded by the SBC from the enterprise site as a result of the SIP Entity Monitoring configured for Session Manager. Reversely, when the service provider network responds to the OPTIONS from Session Manager, the SBC will pass the response to Session Manager.
 - **Incidents** – From the admin web interface of Avaya SBCE, open the Incidents report by clicking the **Incidents** menu button in the menu bar. Verify that no abnormal incidents are listed.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager R6.0.1, Avaya Aura® Session Manager R6.1 and Avaya Session Border Controller for Enterprise R4.0.5 to CenturyLink BroadWorks SIP Trunk. CenturyLink BroadWorks SIP Trunk is a SIP-based Voice over IP service for customers ranging from small businesses to large enterprises providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. References

The Avaya product documentation is available at <http://support.avaya.com> unless otherwise noted.

Avaya Aura® Session Manager/System Manager

- [1] *Administering Avaya Aura® Session Manager*, Document ID 03-603324, Issue 1.1, Release 6.1, October 2011
- [2] *Installing and Configuring Avaya Aura® Session Manager*, Doc ID 03-603473 Issue 2.2, April 2011
- [3] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Issue 4.1, March 2011
- [4] *Administering Avaya Aura® System Manager*, Document Number 03-603324, June 2010

Avaya Aura® Communication Manager

- [5] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Issue 6.0, Release 6.0, August 2010
- [6] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya Aura® Messaging

[7] *Administering Avaya Aura® Messaging 6.1*, CID: 151610, December 2011

[8] *Implementing Avaya Aura® Messaging 6.1*, CID: 150976, October 2011

Avaya Session Border Controller for Enterprise

Product documentation for UC-Sec can be obtained from Sipera using the link at <http://www.sipera.com>.

[9] *E-SBC IU Installation Guide, Release 4.0.5*, Part Number: 101-5225-405v1.00, Release Date: November 2011

[10] *E-SBC Administration Guide, Release 4.0.5*, Part Number: 010-5424-405v1.00, Release Date: November 2011

©2012 Avaya Inc. All Rights Reserved.

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

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