



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring XO Communications SIP Trunking with Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise 6.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between XO Communications SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2, Avaya Session Border Controller for Enterprise (SBCE) 6.2 Q36 and various Avaya endpoints.

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

Table of Contents

1. INTRODUCTION.....	4
2. GENERAL TEST APPROACH AND TEST RESULTS	4
2.1. INTEROPERABILITY COMPLIANCE TESTING	4
2.2. TEST RESULTS	5
2.3. SUPPORT.....	5
3. REFERENCE CONFIGURATION	6
4. EQUIPMENT AND SOFTWARE VALIDATED.....	7
5. CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....	8
5.1. LICENSING AND CAPACITY	8
5.2. SYSTEM FEATURES.....	10
5.3. IP NODE NAMES.....	11
5.4. CODECS.....	11
5.5. IP NETWORK REGION	12
5.6. CONFIGURE IP INTERFACE FOR PROCR	13
5.7. SIGNALING GROUP	13
5.8. TRUNK GROUP	15
5.9. CALLING PARTY INFORMATION.....	18
5.10. OUTBOUND ROUTING	19
5.11. INCOMING CALL HANDLING TREATMENT	21
5.12. AVAYA AURA® COMMUNICATION MANAGER STATIONS	22
5.13. SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.....	22
6. CONFIGURE AVAYA AURA® SESSION MANAGER.....	23
6.1. AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION	24
6.2. SPECIFY SIP DOMAIN	26
6.3. ADD LOCATION	27
6.4. ADD SIP ENTITIES	28
6.4.1. <i>Configure Session Manager SIP Entity.....</i>	<i>29</i>
6.4.2. <i>Configure Communication Manager SIP Entity</i>	<i>30</i>
6.4.3. <i>Configure Avaya Session Border Controller for Enterprise SIP Entity.....</i>	<i>32</i>
6.5. ADD ENTITY LINKS	32
6.6. CONFIGURE TIME RANGES	34
6.7. ADD ROUTING POLICIES.....	34
6.8. ADD DIAL PATTERNS	36
7. CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	40
7.1. LOG IN AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	40
7.2. GLOBAL PROFILES.....	41
7.2.1. <i>Configure Server Interworking Profile - Avaya site.....</i>	<i>41</i>
7.2.2. <i>Configure Server Interworking Profile – XO Communications site.....</i>	<i>42</i>
7.2.3. <i>Configure URI Groups.....</i>	<i>43</i>
7.2.4. <i>Configure Routing – Avaya site</i>	<i>43</i>
7.2.5. <i>Configure Routing – XO Communications site</i>	<i>45</i>
7.2.6. <i>Configure Server – Session Manager.....</i>	<i>46</i>
7.2.7. <i>Configure Server – XO Communications.....</i>	<i>48</i>
7.2.8. <i>Configure Topology Hiding – Avaya site</i>	<i>49</i>
7.2.9. <i>Configure Topology Hiding – XO Communications site.....</i>	<i>51</i>
7.3. DOMAIN POLICIES	51
7.3.1. <i>Create Application Rules</i>	<i>52</i>

7.3.2. Create Border Rules.....	54
7.3.3. Create Media Rules.....	56
7.3.4. Create Security Rules.....	57
7.3.5. Create Signaling Rules.....	59
7.3.6. Create Time of Day Rules	60
7.3.7. Create Endpoint Policy Groups	62
7.3.8. Create Session Policy.....	63
7.4. DEVICE SPECIFIC SETTINGS.....	65
7.4.1. Manage Network Settings.....	65
7.4.2. Create Media Interfaces.....	66
7.4.3. Create Signaling Interfaces.....	67
7.4.4. Configuration of Server Flows.....	68
7.4.4.1 Create End Point Flows – Session Manager.....	68
7.4.4.2 Create End Point Flows - XO Communications.....	69
7.4.5. Create Session Flows	69
8. XO COMMUNICATIONS SIP TRUNKING CONFIGURATION	70
9. VERIFICATION STEPS.....	71
10. CONCLUSION.....	71
11. REFERENCES.....	72

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between XO Communications SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 6.2, Avaya Aura® Communication Manager 6.2, Avaya Session Border Controller for Enterprise (SBCE) 6.2 Q36 and various Avaya endpoints.

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to XO Communications SIP Trunking via the public Internet and exercise the features and functionality listed in **Section 2.1**. The simulated enterprise site was comprised of Communication Manager, Session Manager and the Avaya SBCE with various types of Avaya phones.

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 including 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 including 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 using H323 and SIP protocols (Soft client).

Avaya one-X® Communicator can place calls from the local computer or control a separate physical phone. Both of these modes were tested.

- Various call types including: local, long distance, international, outbound/inbound toll-free, operator, operator-assisted call (0 + 10-digits), local directory assistance (411) and emergency call (911).
- G.711MU and G.729A codecs.
- DTMF transmission using RFC 2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, internal call forwarding, transfer, and conference.
- Off-net call transfer, conference, off-net call forwarding, forwarding to Avaya Aura® Messaging and enterprise mobility (extension to cellular).
- T.38 Fax with G.729 voice setup.

Items not supported or not tested included the following:

- Media Shuffling on Communication Manager was turned off at XO's request so that the Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the enterprise endpoints providing media resources.

2.2. Test Results

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

- **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 ASBCE (**Section 7.3.3**). Media Anomaly Detection basically measures the jitter in the audio flow and is too sensitive in implementation of this feature.

2.3. Support

For technical support on the XO Communications system, please use the support link at <http://www.xo.com>, or call the customer support number at 800-421-3872

Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

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

For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked out and replaced with fictitious IP addresses throughout the document.

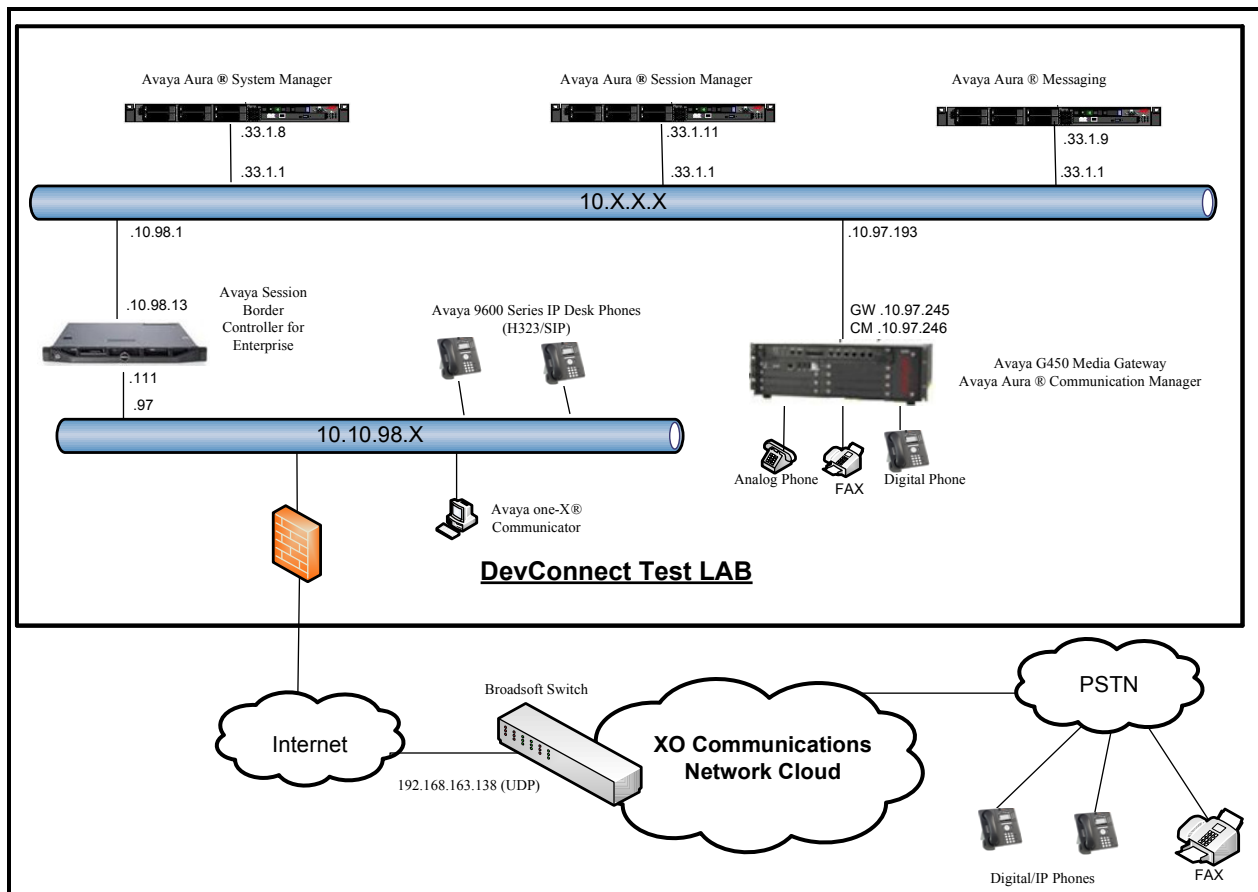


Figure 1: Avaya IP Telephony Network and XO Communications SIP Trunking

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	Release/Version
Avaya S8300 Server	Avaya Aura® Communication Manager R6.2-02.0.823.0 SP3
Avaya G450 Media Gateway MM711 Analog MM712 Digital	HW01 FW001 HW31 FW087 HW05 FW009
Avaya S8800 Server	Avaya Aura® Session Manager R6.2.0.0.620103 – 6.2.1.621002
Avaya S8800 Server	Avaya Aura® System Manager R6.2.0 – SP1 – 6.2.0.0.15669 – 6.2.12.105
Avaya Dell R210 V2 Server	Avaya Session Border Controller for Enterprise R6.2.0 Q36
Avaya S8800 Server	Avaya Aura® Messaging 6.2 SP2
Avaya 9640 Series IP Telephones (H.323)	Avaya one-X® Deskphone Edition S3.110b
Avaya 96xx IP Phone (SIP)	6.0.3-120511
Avaya Digital Telephones (1408D)	N/A
Avaya Symphony 2000 Analog Telephone	N/A
Avaya one-X® Communicator	3.2.3.15 64595
XO Communications SIP Trunking Solution Components	
Equipment/Software	Release/Version
Broadsoft Softswitch	Rel_18.sp1_1.890
Media Gateway SONUS GSX9000	V07.03.01 F009

Table 1: Equipment and Software Tested

The specific configuration above was 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 XO Communications SIP Trunking. It is assumed the general installation of Communication Manager, Avaya 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.

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 SIP trunks are available and 100 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	50
	Maximum Concurrently Registered IP Stations:	2400	2
	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	0
	Maximum Video Capable IP Softphones:	2400	2
	Maximum Administered SIP Trunks:	4000	100
	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	0
	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.)			

On **Page 3**, verify that **ARS** is set to **y**.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List? n	Audible Message Waiting? y		
Access Security Gateway (ASG)? n	Authorization Codes? n		
Analog Trunk Incoming Call ID? n	CAS Branch? n		
A/D Grp/Sys List Dialing Start at 01? n	CAS Main? n		
Answer Supervision by Call Classifier? n	Change COR by FAC? n		
ARS? y	Computer Telephony Adjunct		
Links? n			
ARS/AAR Partitioning? y	Cvg Of Calls Redirected		
Off-net? y			
ARS/AAR Dialing without FAC? y	DCS (Basic)? y		
ASAI Link Core Capabilities? y	DCS Call Coverage? y		
ASAI Link Plus Capabilities? y	DCS with Rerouting? y		
Async. Transfer Mode (ATM) PNC? n			
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y		
ATM WAN Spare Processor? n	DS1 MSP? y		
ATMS? y	DS1 Echo Cancellation? y		
Attendant Vectoring? y			

On **Page 5**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

display system-parameters customer-options		Page	5 of 11
OPTIONAL FEATURES			
MSP? n	Multinational Locations? n	Station and Trunk	
Multiple Level Precedence & Preemption? n	Multiple Locations? n	Station as Virtual Extension? n	
Personal Station Access (PSA)? y	PNC Duplication? n	System Management Data Transfer? n	
Port Network Support? n	Posted Messages? n	Tenant Partitioning? n	
Uniform Dialing Plan? y	Private Networking? y	Terminal Trans. Init. (TTI)? y	
Processor and System MSP? n	Processor Ethernet? y	Time of Day Routing? n	
		TN2501 VAL Maximum Capacity? y	
		Usage Allocation Enhancements? y	
		Wideband Switching? n	
		Wireless? n	
	Remote Office? n		
	Restrict Call Forward Off Net? y		
	Secondary Data Module? y		

5.2. System Features

Use the **change system-parameters features** command to set the **Trunk-to-Trunk Transfer** field to **all** for allowing inbound calls from the PSTN to be transferred to another PSTN endpoint. If for security reasons, incoming calls should not be allowed to be transferred back to the PSTN then leave the field set to **none**.

```
change system-parameters features                                     Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. This text string is entered in the two fields highlighted below. The compliance test used the value of **anonymous** for both.

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

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

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

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

      SCCAN PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and Session Manager (**InteropSM**). These node names will be needed for defining the service provider signaling group in **Section 5.7**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
InteropSM	10.33.1.11	
default	0.0.0.0	
procr	10.10.97.246	
procr6	::	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to use for calls between the enterprise and the service provider. For the compliance test, ip-codec-set 1 was used for this purpose. XO Communications SIP Trunking supports the **G.711MU** and **G.729A** codecs. Default values can be used for all other fields.

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

On **Page 2**, to enable T.38 fax, set the **Fax Mode** to **t.38-standard**. Otherwise, set the Fax Mode to **off**.

change ip-codec-set 1		Page 2 of 2
IP Codec Set		
Allow Direct-IP Multimedia? n		
FAX	Mode	Redundancy
FAX	t.38-standard	0
Modem	off	0
TDD/TTY	US	3
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 **1** was chosen for the service provider trunk. Use the **change ip-network-region 1** command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bwvdev7.com**. This name appears in the From header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Disable **IP-IP Direct Audio** (shuffling) not to allow audio traffic 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 **no**. Shuffling can be further restricted at the trunk level on the Signaling Group form (see **Section 5.7**).
- 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 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location:                Authoritative Domain: bwvdev7.com
      Name: procr
MEDIA PARAMETERS                                Intra-region IP-IP Direct Audio: no
      Codec Set: 1                                Inter-region IP-IP Direct Audio: no
      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
```

5.6. Configure IP Interface for procr

Use the **change ip-interface procr** command to change the Processor Ethernet (procr) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the procr for SIP Trunk signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones. Ensure **Enable Interface** is **y** and **Network Region** is **1**

change ip-interface procr	
IP INTERFACES	
Type: PROCR	Target socket load: 4800
Enable Interface? y	Allow H.323 Endpoints? y
Network Region: 1	Allow H.248 Gateways? y
	Gatekeeper Priority: 5
IPv4 PARAMETERS	
Node Name: procr	IP Address: 10.10.97.246
Subnet Mask: /26	

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. The signaling groups are used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group **10** was used for outbound calls and signaling group **11** was used for inbound calls and were 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 Session Manager.
- Set the **Transport Method** to the value of **tcp** (Transport Layer Security). The transport method specified here is used between Communication Manager and Session Manager.
- Set the **Peer Detection Enabled** field to **y**. The **Peer-Server** field will initially be set to **Others** and cannot be changed via administration. 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 Communication Manager as defined in **Section 5.3**.
- Set the **Far-end Node Name** to **InteropSM**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid used port for TCP as **5060**.
- 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 **bwvdev7.com** of the enterprise domain for signaling group **10** and blank value for signaling group **11**.
- Set **Direct IP-IP Audio Connections** to **n**. This setting will disable media shuffling on the SIP trunk so that Communication Manager will not redirect media traffic directly between the SIP trunk and the enterprise endpoint. Note that Avaya Media Gateway will remain in the media path of all calls between the SIP trunk and the endpoint.
- 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 **6**. This defines the number of seconds the Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

```

add signaling-group 10                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 10                Group Type: sip
IMS Enabled? n                Transport Method: tcp
    Q-SIP? 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: InteropSM
Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                     Far-end Network Region: 1
                                     Far-end Secondary Node Name:
Far-end Domain: bwvdev7.com

Incoming Dialog Loopbacks: eliminate                Bypass If IP Threshold Exceeded? n
                DTMF over IP: rtp-payload                RFC 3389 Comfort Noise? n
                Session Establishment Timer(min): 3                Direct IP-IP Audio Connections? n
                Enable Layer 3 Test? y                IP Audio Hairpinning? n
                H.323 Station Outgoing Direct Media? n                Initial IP-IP Direct Media? n
                                     Alternate Route Timer(sec): 6

```

```

add signaling-group 11
                                     SIGNALING GROUP
                                     Page 1 of 2

Group Number: 11                    Group Type: sip
IMS Enabled? n                      Transport Method: tcp
    Q-SIP? 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: InteropSM
Near-end Listen Port: 5060           Far-end Listen Port: 5060
                                     Far-end Network Region: 1
                                     Far-end Secondary Node Name:

Far-end Domain:

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload           RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3  Direct IP-IP Audio Connections? n
    Enable Layer 3 Test? y           IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n Initial IP-IP Direct Media? n
                                     Alternate Route Timer(sec): 6

```

5.8. Trunk Group

Use the **add trunk-group** command to create trunk groups for the signaling groups created in **Section 5.7**. For the compliance test, trunk group **10** was used for outbound calls and trunk group **11** was used for inbound calls and were 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. (i.e. ***010, *011**).
- Set **Direction** to **outgoing** for trunk group **10** and **incoming** for trunk group **11**.
- Set the **Service Type** field to **public-ntwrk**.
- Set **Member Assignment Method** to **auto**.
- Set the **Signaling Group** to the signaling group configured in **Section 5.7**. Trunk group **10** was associated to signaling group **10** and trunk group **11** was associated to signaling group **11**.
- 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 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 10	Group Type: sip	CDR Reports: y	
Group Name: XO	COR: 1	TN: 1	TAC: *010
Direction: outgoing	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 10	
		Number of Members: 50	

add trunk-group 11		Page 1 of 21	
TRUNK GROUP			
Group Number: 11	Group Type: sip	CDR Reports: y	
Group Name: XO	COR: 1	TN: 1	TAC: *011
Direction: incoming	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 11	
		Number of Members: 50	

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 5.10**).

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

Page 3 of 21

```

add trunk-group 10
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
  
```

Page 3 of 21

```

add trunk-group 11
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**, the **Network Call Redirection** field can be set to **n** (default setting) or **y**. Set the **Network Call Redirection** flag to **y** to enable use of the SIP REFER message for call transfer as verified in the compliance test.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **n**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

Set the **Telephone Event Payload Type** to **101**.

```
add trunk-group 10
```

Page 4 of 21

PROTOCOL VARIATIONS

```
        Mark Users as Phone? n
        Prepend '+' to Calling Number? n
        Send Transferring Party Information? n
        Network Call Redirection? y
        Send Diversion Header? y
        Support Request History? n
        Telephone Event Payload Type: 101

        Convert 180 to 183 for Early Media? n
        Always Use re-INVITE for Display Updates? n
        Identity for Calling Party Display: P-Asserted-Identity
        Block Sending Calling Party Location in INVITE? n
        Enable Q-SIP? n
```

5.9. 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 5.8**), 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.

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 4-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
4	4	10	972941	10

Total Administered: 21
Maximum Entries: 540

5.10. Outbound Routing

In these Application Notes, the Automatic Route Selection (ARS) feature is used to route outbound calls via the SIP trunk to the service provider. In the sample configuration, the single digit **9** is used as the ARS access code. Enterprise callers will dial **9** to reach an “outside line”. This common configuration is illustrated below. Use the **change dialplan analysis** command to define a **Dialed String** beginning with **9** of **Length 1** as a feature access code (**fac**).

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

Use the **change feature-access-codes** command to configure **9** as the **Auto Route Selection (ARS) – Access Code 2**.

change feature-access-codes			FEATURE ACCESS CODE (FAC)		Page	1 of	11
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: *007							
Answer Back Access Code:							
Auto Alternate Routing (AAR) Access Code: *00							
Auto Route Selection (ARS) – Access Code 1:					Access Code 2: 9		
Automatic Callback Activation: *033					Deactivation: #033		
Call Forwarding Activation Busy/DA: *30			All: *031		Deactivation: #030		
Call Forwarding Enhanced Status:			Act:		Deactivation:		
Call Park Access Code: *040							
Call Pickup Access Code: *041							
CAS Remote Hold/Answer Hold-Unhold Access Code: *042							
CDR Account Code Access Code:							
Change COR Access Code:							
Change Coverage Access Code:							
Conditional Call Extend Activation:					Deactivation:		
Contact Closure Open Code: *080					Close Code: #080		

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 10** 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: 1	
	Dialed	Total		Route	Call	Node	ANI
	String	Min	Max	Pattern	Type	Num	Reqd
0		1	11	10	op		n
011		10	18	10	intl		n
1613		11	11	10	pubu		n
1877		11	11	10	pubu		n
411		3	3	10	svcl		n
911		3	3	10	svcl		n
9729		10	10	10	pubu		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 in route pattern **10** for 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 **10** 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.
- **Numbering Format:** Set this field to **unk-unk** since private Numbering Format should be used for this route (see **Section 5.8**).

change route-pattern 10													Page 1 of 3		
Pattern Number: 5 Pattern Name: XO															
SCCAN? n Secure SIP? n															
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC	
No			Mrk	Lmt	List	Del	Digits						QSIG		
													Intw		
1:	10	0											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	none	
2:	y	y	y	y	y	n	n	rest						none	
3:	y	y	y	y	y	n	n	rest						none	
4:	y	y	y	y	y	n	n	rest						none	
5:	y	y	y	y	y	n	n	rest						none	
6:	y	y	y	y	y	n	n	rest						none	

5.11. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Service Provider is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group **11**. As an example, use the **change inc-call-handling-trmt trunk-group 11** to convert incoming DID numbers **972941xxxx** to 4 digit extension xxxx by deleting **6** of the incoming digits.

change inc-call-handling-trmt trunk-group 11															Page 1 of 3		
INCOMING CALL HANDLING TREATMENT																	
Service/		Number			Number			Del Insert									
Feature		Len			Digits												
public-ntwrk		10			972941			6									

5.12. Avaya Aura® Communication Manager Stations

In the sample configuration, four digit station extensions were used with the format 4xxx. Use the **add station 4684** command to add an Avaya H.323 IP telephone

- Enter **Type: 9620, Name: Ext_4684, Security Code: 1234, Coverage Path 1: 1**
- Leave other values as default.

add station 4684		Page 1 of 5
STATION		
Extension: 4684	Lock Messages? n	BCC: 0
Type: 9620	Security Code: 1234	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: Ext_4684	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 4684	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	IP Video? n	
	Customizable Labels? Y	

5.13. Save Avaya Aura® Communication Manager Configuration Changes

Use the **save translation** command to save the configuration.

6. Configure Avaya Aura® Session Manager

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

- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Manager, SBCE and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which define route destinations and control call routing between the SIP Entities.
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call.

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

6.1. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL as <https://<ip-address>/SMGR>, where **<ip-address>** is the IP address of System Manager. At the **System Manager Log On** screen, enter appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

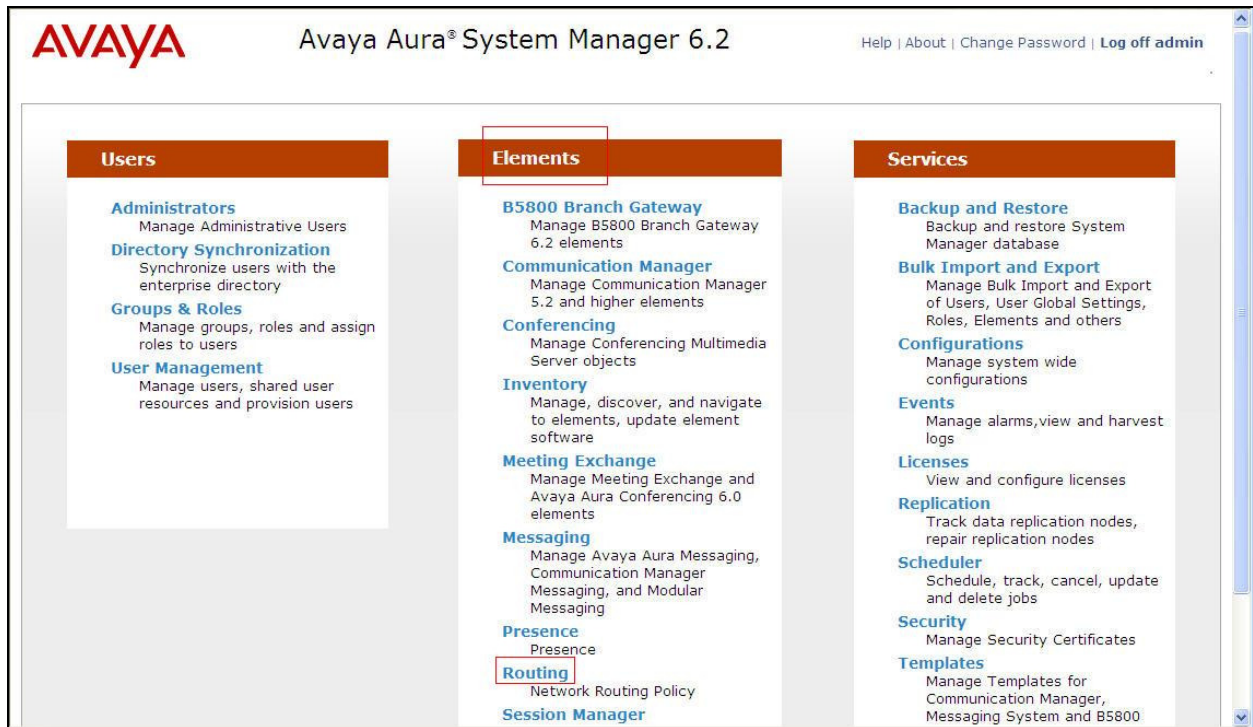


Figure 2 – System Manager Home Screen

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.

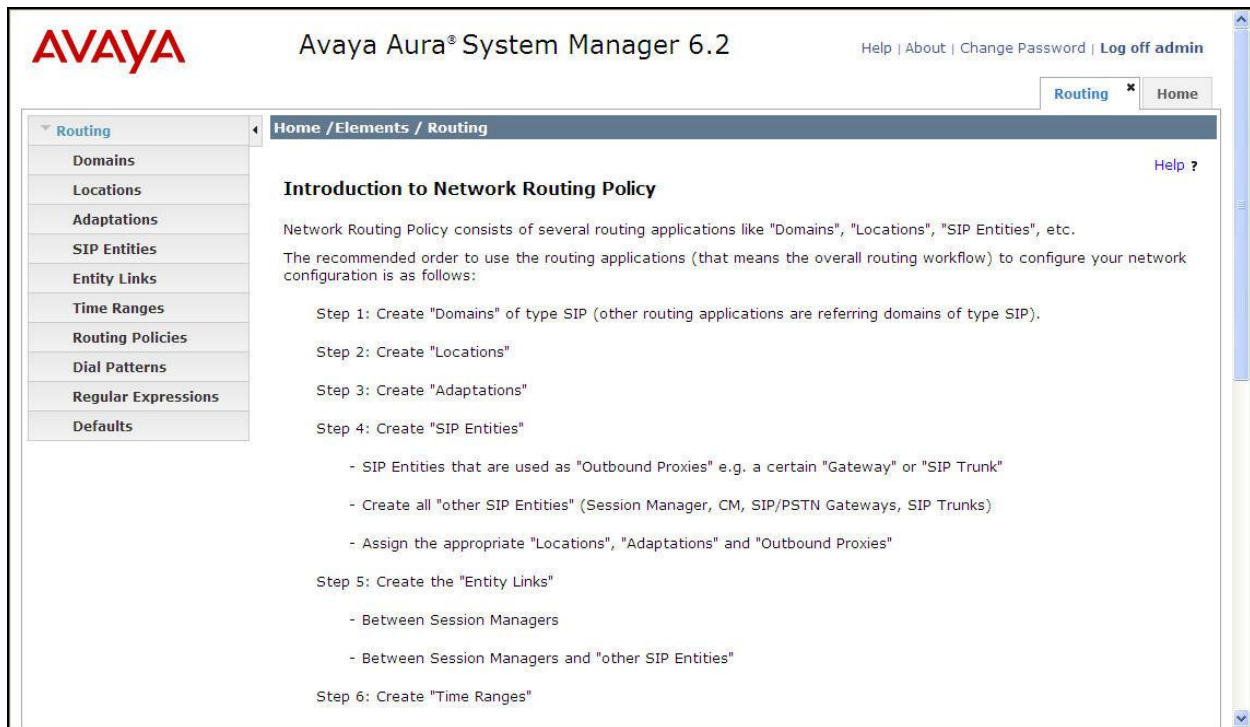


Figure 3 – Network Routing Policy

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 **bvwdev7.com**.

Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), 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** (not shown) to save.

The screen below shows the existing entry for the enterprise domain.

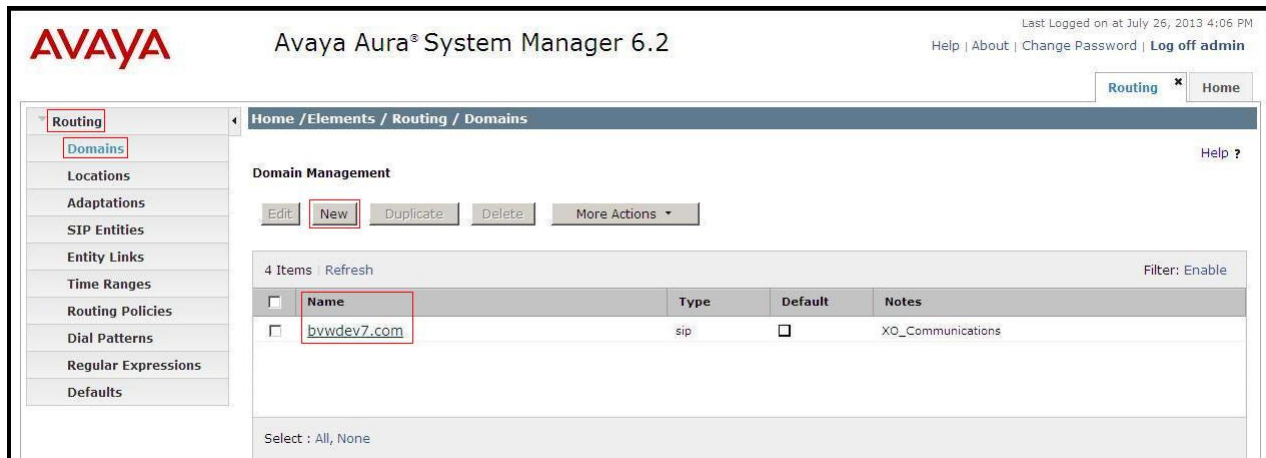


Figure 4 – Domain Management

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. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

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 new right pane that appears (shown below), fill in the following:

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

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

Click **Commit** to save.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at July 26, 2013 4:06 PM Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Locations

Location Details

General

* Name: Belleville

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 100000

Multimedia Bandwidth: 100000

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

Commit Cancel

Figure 5 – Location Configuration

In the **Location Pattern** section, click **Add** to enter IP Address patterns. The following patterns were used in testing:

- **IP Address Pattern:** 10.33.*, 10.10.97.*, 10.10.98.*

The screenshot shows the 'Location Pattern' configuration window. At the top, there are 'Add' and 'Remove' buttons. Below them, it says '3 Items' and 'Refresh'. A 'Filter: Enable' option is on the right. The main area is a table with two columns: 'IP Address Pattern' and 'Notes'. There are three rows, each with a checkbox in the first column and a text input field in the second column. The first row contains '10.33.*', the second '10.10.97.*', and the third '10.10.98.*'. At the bottom, there is a 'Select : All, None' dropdown and 'Commit' and 'Cancel' buttons. The 'Add' button and the 'Commit' button are highlighted with red boxes in the original image.

Figure 6 – IP Ranges Configuration

Click **Commit** to save.

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

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Manager and Avaya SBCE.

Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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 SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. Adaptation module was not used in this configuration.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Belleville**.
- **Time Zone:** Select the time zone for the Location above.

In this configuration, there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.4.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **InteropSM**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address** **10.33.1.11**. Select **Time Zone** as **America/Toronto**.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The left sidebar shows a navigation menu with 'Routing' selected, and 'SIP Entities' highlighted under the 'Routing' section. The main content area is titled 'Home / Elements / Routing / SIP Entities'. It features a 'SIP Entity Details' section with a 'General' tab. The configuration fields are as follows: 'Name' is 'InteropSM', 'FQDN or IP Address' is '10.33.1.11', 'Type' is 'Session Manager', 'Notes' is 'Interop Session Manager', 'Location' is 'Belleville', 'Outbound Proxy' is empty, 'Time Zone' is 'America/Toronto', and 'Credential name' is empty. At the bottom, there is a 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. The top right corner shows the user is logged in as 'admin' and the last login time is 'July 26, 2013 4:06 PM'.

Figure 7 – Session Manager SIP Entity

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 Session Manager listens for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

Defaults can be used for the remaining fields. Click **Commit** (not shown) to save.

The compliance test used port **5060** with **TCP** for connecting to Communication Manager and port **5060** with **UDP** for connecting to Avaya SBCE.

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 XO Communications SIP Trunking.

Other entries defined for other projects as shown in the screen were not used.

The screenshot shows the 'Port' configuration section of the Session Manager SIP Entity. It includes input fields for 'TCP Failover port' and 'TLS Failover port', and buttons for 'Add' and 'Remove'. Below these is a table with 5 items. The first two items are highlighted with red boxes. The first item has Port 5060, Protocol TCP, and Default Domain bvwdev7.com. The second item has Port 5060, Protocol UDP, and Default Domain bvwdev7.com. The 'Add' button is also highlighted with a red box.

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	bvwdev7.com	
<input type="checkbox"/>	5060	UDP	bvwdev7.com	

Figure 8 – Session Manager SIP Entity Port

6.4.2. Configure Communication Manager SIP Entity

The following screen shows the addition of the Communication Manager SIP Entity named **G450_CM62**. 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 during Session Manager installation. The original SIP entity is used with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of Communication Manager **10.10.97.246**. The **Location**

field is set to **Belleville** which is the Location that includes the subnet where Communication Manager resides. Note that **CM** was selected for **Type**. Select **Time Zone** as **America/Toronto**.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at July 26, 2013 4:06 PM Help | About | Change Password | Log off admin

Routing * Home

Routing Domains Locations Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions Defaults

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: G450_CM62

* FQDN or IP Address: 10.10.97.246

Type: CM

Notes: For CM6.2

Adaptation: (empty)

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

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

Credential name: (empty)

Call Detail Recording: none

Commit Cancel Help ?

Figure 9 – Communication Manager SIP Entity

6.4.3. Configure Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **SBCE62**. The **FQDN or IP Address** field is set to the IP address of the SBC's private network interface **10.10.98.13**. The **Location** field is set to **Belleville** which includes the subnet where the Avaya SBCE resides. Note that **Other** was selected for **Type**. Select **Time Zone** as **America/Toronto**.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields and values:

- Name:** SBCE62
- * FQDN or IP Address:** 10.10.98.13
- Type:** Other (selected from a dropdown)
- Notes:** (empty text field)
- Adaptation:** (empty dropdown)
- Location:** Belleville (selected from a dropdown)
- Time Zone:** America/Toronto (selected from a dropdown)
- Override Port & Transport with DNS SRV:** ☐
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (selected from a dropdown)
- CommProfile Type Preference:** (empty dropdown)

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

Figure 10 – Avaya SBCE SIP Entity

6.5. 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 Communication Manager for use only by service provider traffic and one to the 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). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **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 Entity Link, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**.
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.4**.

- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager Entity Link, this must match the Near-end Listen Port defined on the Communication Manager signaling group in **Section 5.7**.
- **Trusted:** Check this box. Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save.

The following screen illustrates the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.7**.

Avaya Aura® System Manager 6.2

Home / Elements / Routing / Entity Links

Entity Links

1 Item Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* InteropSM_G450_C	* InteropSM	TCP	* 5060	* G450_CM62	* 5060	Trusted	XO_Communication

Commit Cancel

Figure 11 – Communication Manager Entity Link

The following screen illustrates the Entity Links to SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4** and **7.2.6**.

Avaya Aura® System Manager 6.2

Home / Elements / Routing / Entity Links

Entity Links

1 Item Refresh

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* InteropSM_SBCE62	* InteropSM	UDP	* 5060	* SBCE62	* 5060	Trusted	XO_Communication

Figure 12 – Avaya SBCE Entity Link

6.6. Configure Time Ranges

Time Ranges is configured for time-based-routing. In order to add a Time Ranges, select **Routing → Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the 24/7 range since time-based routing was not the focus of these Application Notes.

Avaya Aura® System Manager 6.2

Home / Elements / Routing / Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions

1 Item Refresh

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
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

Figure 13 – Time Ranges

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. 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). In the new right pane that appears (shown below), 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 screen shows the **Routing Policy Details** for the policy named **To_G450_CM62** associated with incoming PSTN calls from XO Communications to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **G450_CM62**

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and user information: 'Last Logged on at July 26, 2013 4:06 PM' and 'Log off admin'. The left sidebar shows a menu with 'Routing' selected, and sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Routing Policies'. It features a 'Routing Policy Details' section with a 'General' tab. The 'Name' field is set to 'To_G450_CM62', 'Disabled' is unchecked, 'Retries' is 0, and 'Notes' is 'XO_Communications'. Below this is the 'SIP Entity as Destination' section with a 'Select' button. At the bottom, a table lists the selected SIP entity:

Name	FQDN or IP Address	Type	Notes
G450_CM62	10.10.97.246	CM	For CM6.2

Figure 14 – Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **To_XO_Communications** associated with outgoing calls from Communication Manager to the PSTN via XO Communications through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE62**.

Avaya Aura® System Manager 6.2

Last Logged on at July 26, 2013 4:06 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing * **Home**

Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* **Name:** To_XO_Communications

Disabled: ☐

* **Retries:** 0

Notes: XO_Communications

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SBCE62	10.10.98.13	Other	

Commit **Cancel** **Help ?**

Figure 15 – Routing to XO Communications

6.8. Add Dial Patterns

Dial Patterns are needed to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from Communication Manager to XO Communications through the Avaya SBCE and vice versa. Dial Patterns define which Route Policy will be selected as route destination 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). In the new right pane that appears (shown below), fill in the following:

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

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

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating

Location for use in the match criteria. Lastly, select the Routing Policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

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

Two examples of the Dial Patterns used for the compliance test are shown below, 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., 1877 Toll free call, 011 international call, etc.) were similarly defined.

The first example shows that outbound 11-digit dialed numbers that begin with **1** and have a destination SIP Domain of **bvwdev7.com** uses Routing Policy **To_XO_Communications** as defined in **Section 6.7**.

Figure 16 – Dial Pattern_1613

Note that the above Dial Pattern did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised (e.g., use Dial Pattern 1908, 1905, etc. with 11 digits) per customer business policies.

Also note that **-ALL-** was selected for **Originating Location Name**. This selection was chosen to accommodate certain off-net call forward scenarios where the inbound call was re-directed outbound back to the PSTN.

The second example shows that inbound 10-digit numbers that start with **9729** uses Routing Policy **To_G450_CM62** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by XO Communications.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at July 26, 2013 4:06 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Help ?
Commit Cancel

General

* Pattern: 9729

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev7.com

Notes: XO_Communications Inbound Calls

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"/>	Belleville		To_G450_CM62	0	<input type="checkbox"/>	G450_CM62	XO_Communications

Select : All, None

Figure 17 – Dial Pattern_9729

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top navigation bar includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.2', and user information 'Last Logged on at July 26, 2013 4:06 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. A secondary navigation bar shows 'Routing' and 'Home' tabs. On the left, a sidebar menu lists various configuration areas: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, **Dial Patterns** (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Dial Patterns' and features a 'Dial Patterns' section with buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below this is a table listing 54 items, with the first 8 visible. The table has columns for checkboxes, Pattern, Min, Max, Emergency Call, Emergency Type, Emergency Priority, SIP Domain, and Notes. The patterns listed are 0, 011, 1613, 1877, 411, 911, 9725, and 9729, all associated with the domain 'bvwddev7.com' and various communication notes. At the bottom of the table area, there is a 'Select' dropdown set to 'All, None' and a pagination control showing 'Page 1 of 4'.

	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	0	1	11	<input type="checkbox"/>			bvwddev7.com	XO_Communications Operator Outbound Calls
<input type="checkbox"/>	011	13	13	<input type="checkbox"/>			bvwddev7.com	XO_Communications International Outbound Calls
<input type="checkbox"/>	1613	11	11	<input type="checkbox"/>			bvwddev7.com	XO_Communications Outbound Calls
<input type="checkbox"/>	1877	11	11	<input type="checkbox"/>			bvwddev7.com	XO_Communications Toll Free Outbound Calls
<input type="checkbox"/>	411	3	3	<input type="checkbox"/>			bvwddev7.com	XO_Communications 411 Outbound Calls
<input type="checkbox"/>	911	3	3	<input type="checkbox"/>			bvwddev7.com	XO_Communications 911 Outbound Calls
<input type="checkbox"/>	9725	10	10	<input type="checkbox"/>			bvwddev7.com	XO_Communications Outbound Calls
<input type="checkbox"/>	9729	10	10	<input type="checkbox"/>			bvwddev7.com	XO_Communications Inbound Calls

Figure 18 – Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE necessary for interoperability with the Session Manager and XO Communications system.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the XO Communications system resides on the Public side of the network.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see **Section 11** of these Application Notes.

7.1. Log in Avaya Session Border Controller for Enterprise

Access the web interface by typing “<https://x.x.x.x/sbc/>” (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password**.



The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise'. On the right, there is a 'Log In' section with two input fields: 'Username:' containing 'ucsec' and 'Password:' containing a masked password. Below these fields is a 'Log In' button. To the right of the button, there is a disclaimer text block. At the bottom, there is a copyright notice: '© 2011 - 2013 Avaya Inc. All rights reserved.'

AVAYA

**Session Border Controller
for Enterprise**

Log In

Username:

Password:

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

Figure 19 - Avaya SBCE Login

7.2. Global Profiles

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

7.2.1. Configure Server Interworking Profile - Avaya site

Server Interworking profile allows administrator to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking → Add**

- Enter Profile name: **SM62**
- Check **Hold Support** as **RFC2543**.
- Check **Diversion Header Support** as **Yes**.
- Check **T.38 Support** as **Yes**.
- All other options on the **General** Tab can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs: all options can be left at default. Click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SM62**) was added.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded, showing the path: **Global Profiles → Server Interworking**. The main content area is titled "Interworking Profiles: SM62" and includes an "Add" button. Below this, a list of existing profiles is shown, with "SM62" highlighted. The configuration tabs are "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing the following configuration:

General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	Yes
Diversion Header Support	Yes
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	

Figure 20 - Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – XO Communications site

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking** → **Add**

- Enter Profile name: **XO_Communications**
- Check **Hold Support** as **RFC2543**.
- Check **Diversion Header Support** as **Yes**.
- Check **T.38 Support** as **Yes**.
- All other options on the **General** Tab can be left at default.

On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** Tabs: all options can be left at default. Click **Finish** (not shown).

The following screen shows that XO Communications server interworking profile (named: **XO_Communications**) was added.

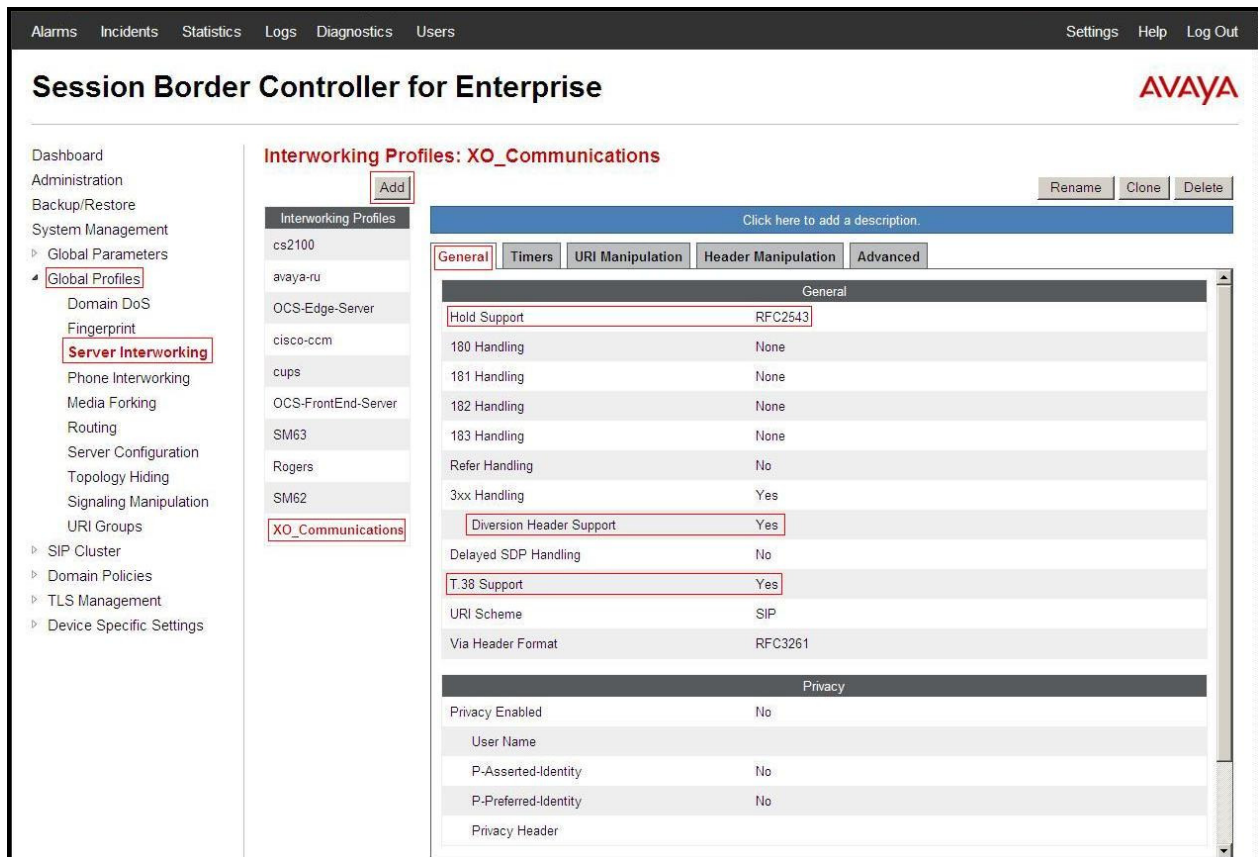


Figure 21 - Server Interworking – XO Communications site

7.2.3. Configure URI Groups

The URI Group feature allows administrator to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group.

The following URI Group configuration is used for this specific testing in DevConnect Lab environment. The URI-Group named **XO_Communications** was used to match the “From” and “To” headers in a SIP call dialog received from both Enterprise and XO Communications service. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see **Section 7.2.4, 7.2.5**), Server Flow (see **Section 7.4.4**), and Session Flow (see **section 7.4.5**) to route incoming and outgoing calls to the right destinations. In production environment, there is not a requirement to define this URI.

From the menu on the left-hand side, select **Global Profiles** → **URI Groups**. Select **Add**.

- Enter Group Name: **XO_Communications**.
- Edit the URI Type: **Regular Expression** (not shown).
- Add URI: **. *10\10\33\11** (Session Manager IP address), **. *10\10\98\111** (Avaya SBCE public interface IP address), **. *10\10\98\13** (Avaya SBCE internal interface IP address), **. *192\168\163\138** (XO Communications Broadsoft Switch IP address), **. *anonymous\invalid** (Anonymous URI), **. *bvwddev7\com** (Enterprise domain).
- Click **Finish** (not shown).

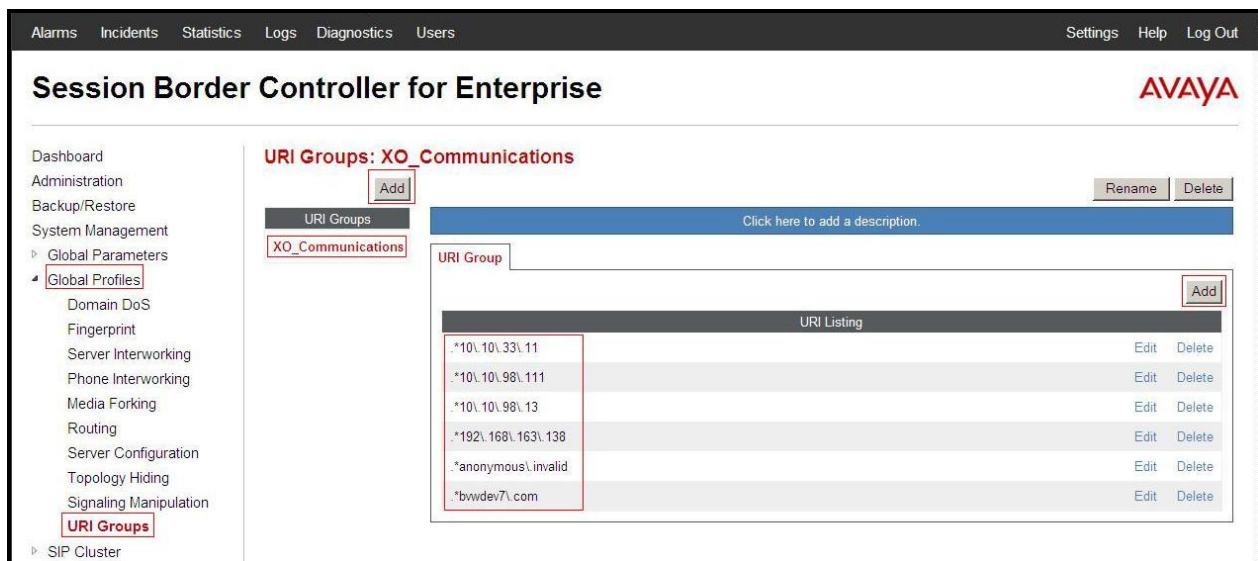


Figure 22 - URI Group

7.2.4. Configure Routing – Avaya site

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

From the menu on the left-hand side, select **Global Profiles → Routing → Add**
Enter Profile Name: **XO_To_SM62**.

- **URI Group: XO_Communications.**
- **Next Hop Server 1: 10.33.1.11** (Session Manager IP address).
- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport: UDP** (not shown).
- Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various system management options, with 'Routing' highlighted under 'Global Profiles'. The main content area is titled 'Routing Profiles: XO_To_SM62' and features an 'Add' button. Below this, a table lists the configured routing profiles. The table has columns for Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. A single profile is listed with Priority 1, URI Group XO_Communications, and Next Hop Server 1 set to 10.33.1.11. The Next Hop Server 2 column is empty. Action buttons 'View' and 'Edit' are visible for the listed profile.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	XO_Communications	10.33.1.11		View Edit

Figure 23 - Routing to Avaya

7.2.5. Configure Routing – XO Communications site

The Routing Profile allows administrator to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles → Routing → Add**

Enter Profile Name: **SM62_To_XO**.

- **URI Group: XO_Communications.**
- **Next Hop Server 1: 192.168.163.138** (XO Communications Broadsoft Switch IP address. This IP Address provided by Customer).
- Check **Routing Priority based on Next Hop Server** (not shown).
- **Outgoing Transport as UDP** (not shown).
- Click **Finish** (not shown).

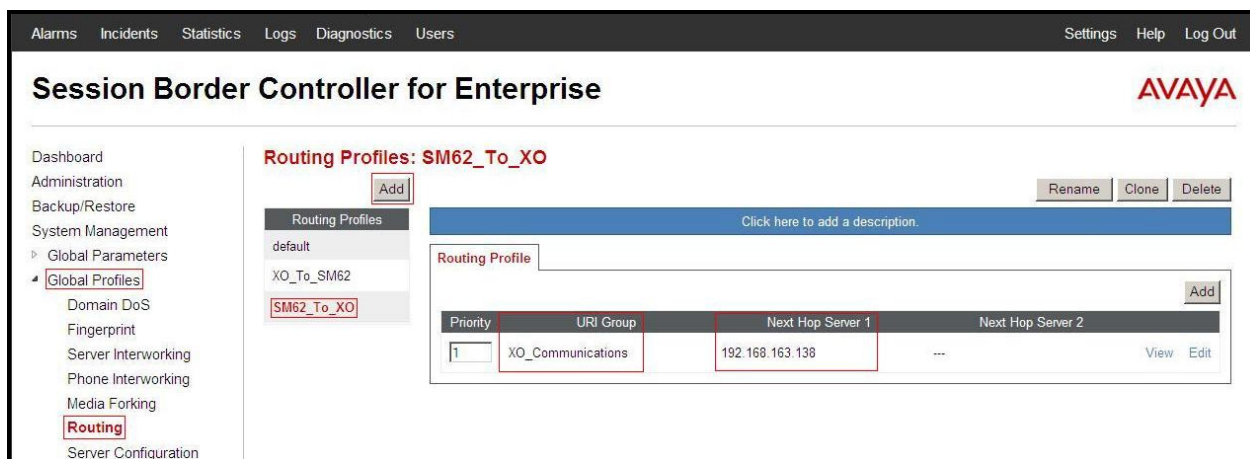


Figure 24 - Routing to XO Communications

7.2.6. Configure Server – Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow administrator to configure and manage various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** → **Add**.

Enter profile name: **SM62**.

On **General** tab enter the following:

- **Server Type:** Select **Call Server**
- **IP Address/FQDNs:** **10.33.1.11** (Session Manager IP Address)
- **Supported Transports:** **UDP**
- **UDP Port:** **5060**

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various system management options, with 'Global Profiles' expanded and 'Server Configuration' highlighted. The main content area is titled 'Server Configuration: SM62' and features an 'Add' button. Below this, there are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a table with the following configuration details:

Server Type	Call Server
IP Addresses / FQDNs	10.33.1.11
Supported Transports	UDP
UDP Port	5060

Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are visible at the top right of the configuration area.

Figure 25 - Session Manager General Server Configuration

On the **Advanced** tab:

- Select **SM62** for **Interworking Profile**.

Click **Finish** (not shown).

The screenshot shows the Avaya Session Manager Advanced Server Configuration interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "Server Configuration" highlighted. The main content area is titled "Server Configuration: SM62" and features an "Add" button. Below this, a "Server Profiles" list shows "SM62" selected. To the right, there are tabs for "General", "Authentication", "Heartbeat", and "Advanced", with "Advanced" currently active. The "Advanced" tab contains several configuration options: "Enable DoS Protection" (checkbox), "Enable Grooming" (checkbox), "Interworking Profile" (set to "SM62"), "Signaling Manipulation Script" (set to "None"), and "UDP Connection Type" (set to "SUBID"). An "Edit" button is located at the bottom right of the configuration area.

Figure 26 - Session Manager Advanced Server Configuration

7.2.7. Configure Server – XO Communications

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** → **Add**.

Enter profile name: **XO_Communications**

On **General** tab enter the following:

- **Server Type:** Select **Trunk Server**
- **IP Address:** **192.168.163.138** (XO Communications Broadsoft Switch IP Address)
- **Supported Transports:** **UDP**
- **UDP Port:** **5060**

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand navigation menu lists various system management options, with "Global Profiles" and "Server Configuration" highlighted. The main content area is titled "Server Configuration: XO_Communications" and features an "Add" button. Below this, a list of server profiles shows "SM62" and "XO_Communications". The "XO_Communications" profile is selected, and its configuration is shown in a table with tabs for General, Authentication, Heartbeat, and Advanced. The "General" tab is active, displaying the following configuration:

Parameter	Value
Server Type	Trunk Server
IP Addresses / FQDNs	192.168.163.138
Supported Transports	UDP
UDP Port	5060

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

Figure 27 - XO Communications General Server Configuration

On the **Advanced** tab enter the following:

- **Interworking Profile:** select **XO_Communications**

Click **Finish** (not shown).

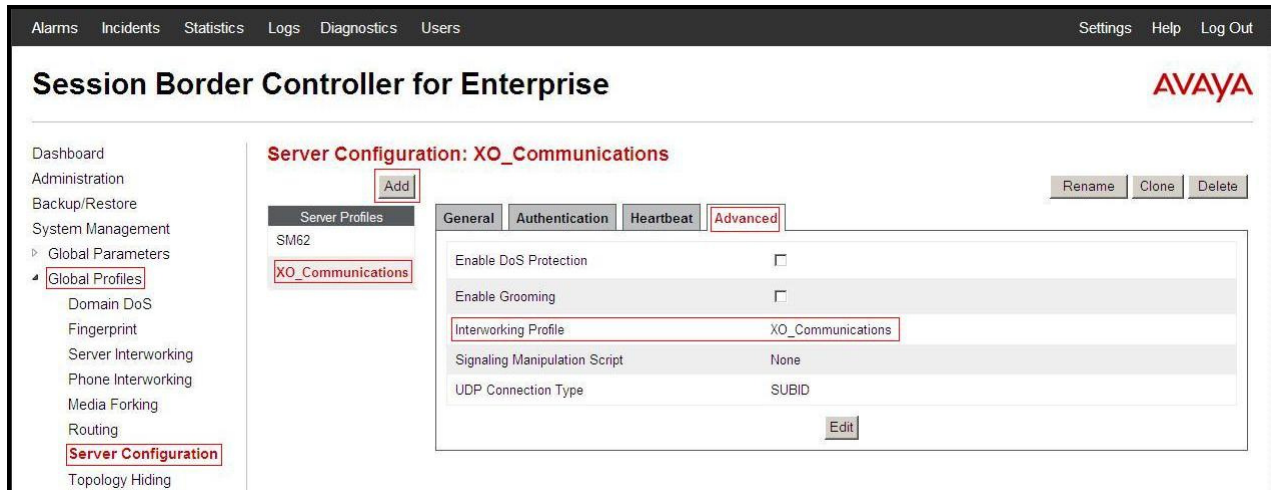


Figure 28 - XO Communications Advanced Server Configuration

7.2.8. Configure Topology Hiding – Avaya site

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

From the menu on the left-hand side, select **Global Profiles → Topology Hiding**.

Select **Add**, enter Profile Name: **XO_To_SM62**.

- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev7.com**
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev7.com**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev7.com**

Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), and Signaling Manipulation. The main content area is titled "Topology Hiding Profiles: XO_To_SM62" and features an "Add" button, a "Click here to add a description" link, and buttons for Rename, Clone, and Delete. Below this is a "Topology Hiding" table with columns for Header, Criteria, Replace Action, and Overwrite Value. The table contains three rows: "From", "Request-Line", and "To", all with "IP/Domain" as the criteria and "bwdev7.com" as the overwrite value. An "Edit" button is located at the bottom right of the table.

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	bwdev7.com
Request-Line	IP/Domain	Overwrite	bwdev7.com
To	IP/Domain	Overwrite	bwdev7.com

Figure 29 - Topology Hiding Session Manager

7.2.9. Configure Topology Hiding – XO Communications site

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **Add Profile**, enter Profile Name: **SM62_To_XO**.

- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **10.10.98.111**
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **192.168.163.138**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **192.168.163.138**

Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding, and Signaling Manipulation. The 'Global Profiles' section is expanded, and 'Topology Hiding' is selected. The main content area displays 'Topology Hiding Profiles: SM62_To_XO'. There is an 'Add' button and a list of profiles: 'default', 'cisco_th_profile', 'XO_To_SM62', and 'SM62_To_XO'. The 'SM62_To_XO' profile is selected, and its configuration is shown in a table. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The configuration for 'SM62_To_XO' is as follows:

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	10.10.98.111
Request-Line	IP/Domain	Overwrite	192.168.163.138
To	IP/Domain	Overwrite	192.168.163.138

Figure 30 - Topology Hiding XO Communications

7.3. Domain Policies

The Domain Policies feature allows administrator to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or administrator can create a custom domain policy.

7.3.1. Create Application Rules

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

From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Name: **SM62_XO_AppR**
 - Click Finish (not shown).

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left-hand navigation menu is expanded to 'Domain Policies', and 'Application Rules' is selected. The main content area displays the configuration for the 'SM62_XO_AppR' rule. At the top, there are buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below these is a blue bar with the text 'Click here to add a description.' The 'Application Rule' section contains a table with columns: 'Application Type', 'In', 'Out', 'Maximum Concurrent Sessions', and 'Maximum Sessions Per Endpoint'. The table has three rows: 'Voice' (In: checked, Out: checked, Max Concurrent: 200, Max Sessions: 5), 'Video' (In: unchecked, Out: unchecked), and 'IM' (In: unchecked, Out: unchecked). Below the table is a 'Miscellaneous' section with two rows: 'CDR Support' (None) and 'RTCP Keep-Alive' (No). An 'Edit' button is located at the bottom right of the configuration area.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

Figure 31 - Session Manager Application Rule

From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Name: **XO_AppR**
 - Click **Finish** (not shown).

Session Border Controller for Enterprise AVAYA

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Application Rules: XO_AppR

[Add](#) [Filter By Device...](#) [Rename](#) [Clone](#) [Delete](#)

Click here to add a description.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

[Edit](#)

Figure 32 - XO Communications Application Rule

7.3.2. Create Border Rules

Border Rules allow administrator to control NAT Traversal. The NAT Traversal feature allows administrator to determine whether or not call flow through the DMZ needs to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic.

From the menu on the left-hand side, select **Domain Policies** → **Border Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter Clone Name: **SM62_XO_BorderR**
 - Click **Finish** (not shown).

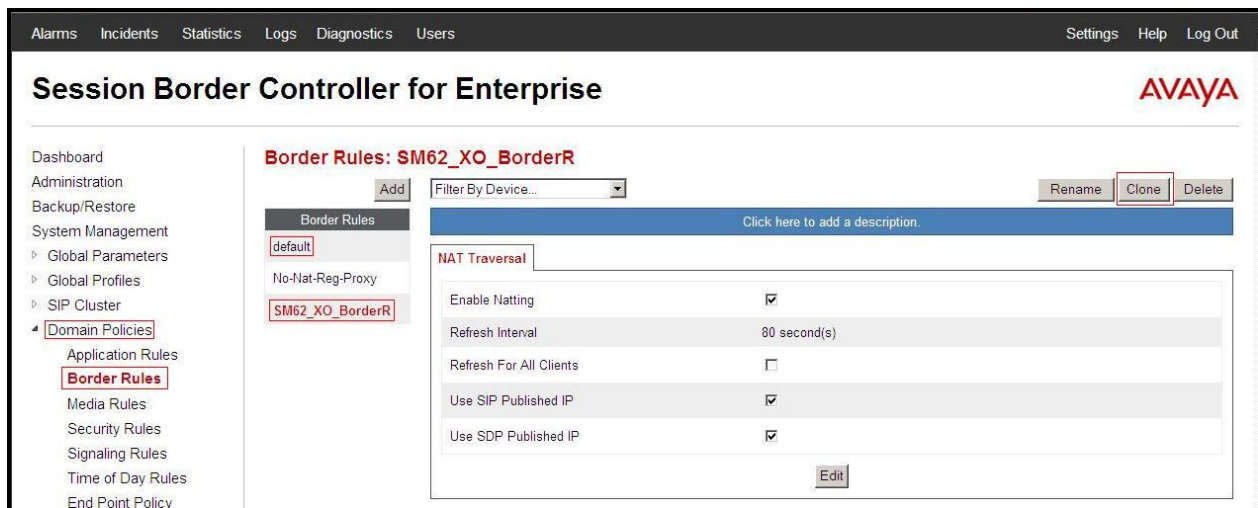


Figure 33 - Session Manager Border Rule

From the menu on the left-hand side, select **Domain Policies → Border Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter Clone Name: **XO_BorderR**
 - Click **Finish** (not shown).

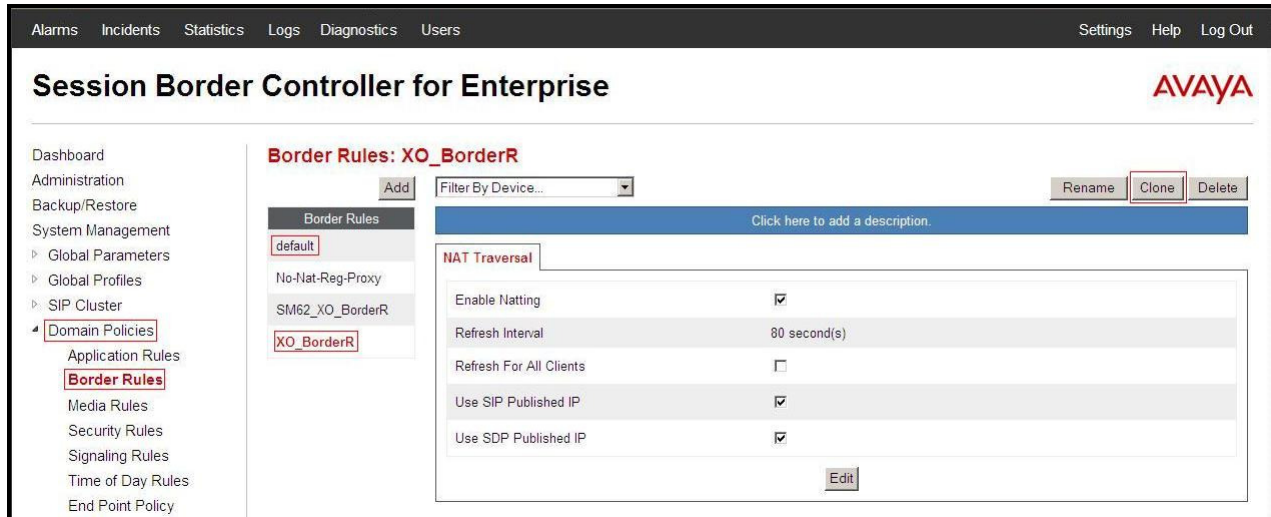


Figure 34 - XO Communications Border Rule

7.3.3. Create Media Rules

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

From the menu on the left-hand side, select **Domain Policies** → **Media Rules**.

- Select the **default-low-med** Rule.
- Select **Clone** button.
 - Enter Clone Name: **SM62_XO_MediaR**
 - Click **Finish** (not shown).



Figure 35 - Session Manager Media Rule

From **Media Anomaly** tab, uncheck **Media Anomaly Detection**

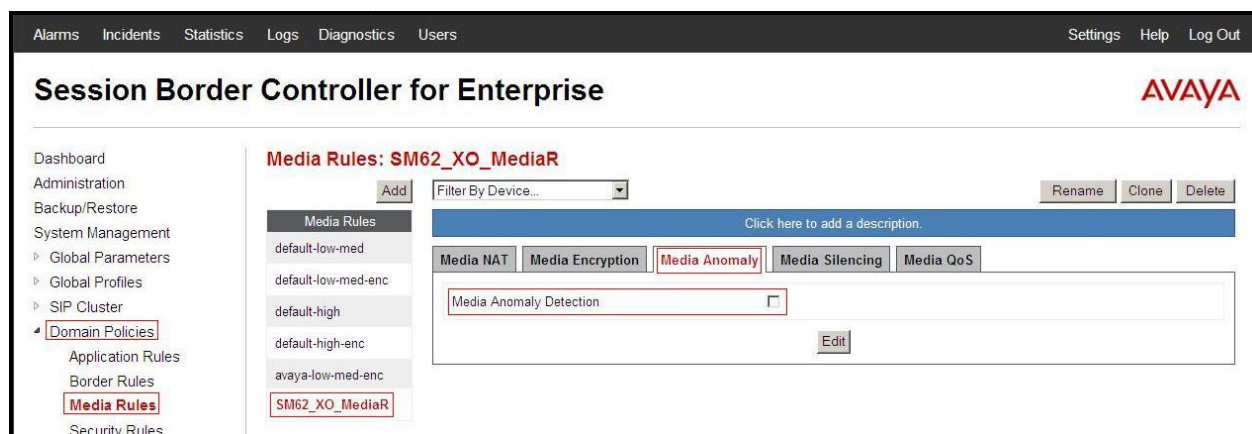


Figure 36 - Session Manager Media Rule – Media Anomaly Detection

From the menu on the left-hand side, select **Domain Policies** → **Media Rules**.

- Select the **default-low-med** Rule.
- Select **Clone** button.
 - Enter Clone Name: **XO_MediaR**
 - Click **Finish** (not shown).

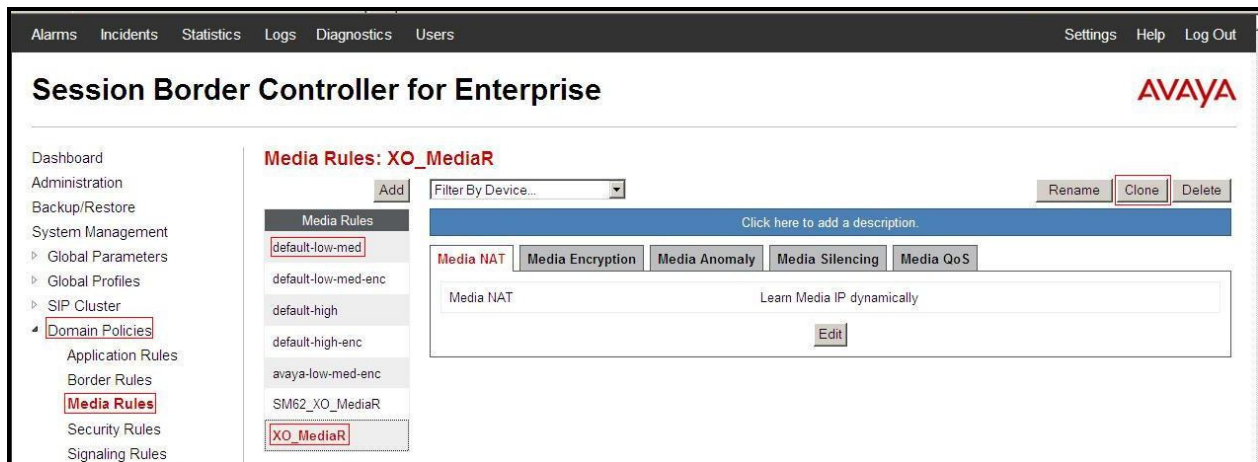


Figure 37 – XO Communications Media Rule

From **Media Anomaly** tab, uncheck **Media Anomaly Detection**

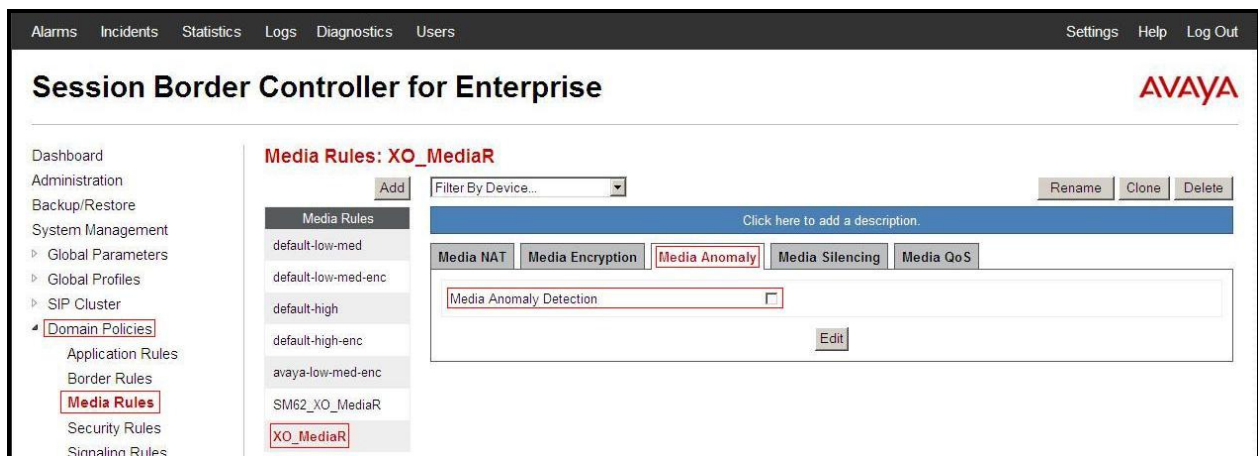


Figure 38 - XO Communications Media Rule - Media Anomaly Detection

7.3.4. Create Security Rules

Security Rules allow administrator to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows one to configure Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, administrator can also define

the security feature profile, so that the feature is applied in a specific manner to a specific situation.

From the menu on the left-hand side, select **Domain Policies** → **Security Rules**.

- Select the **default-med** Rule.
- Select **Clone** button.
 - Enter Clone Name: **SM62_XO_SecR**
 - Click **Finish** (not shown).

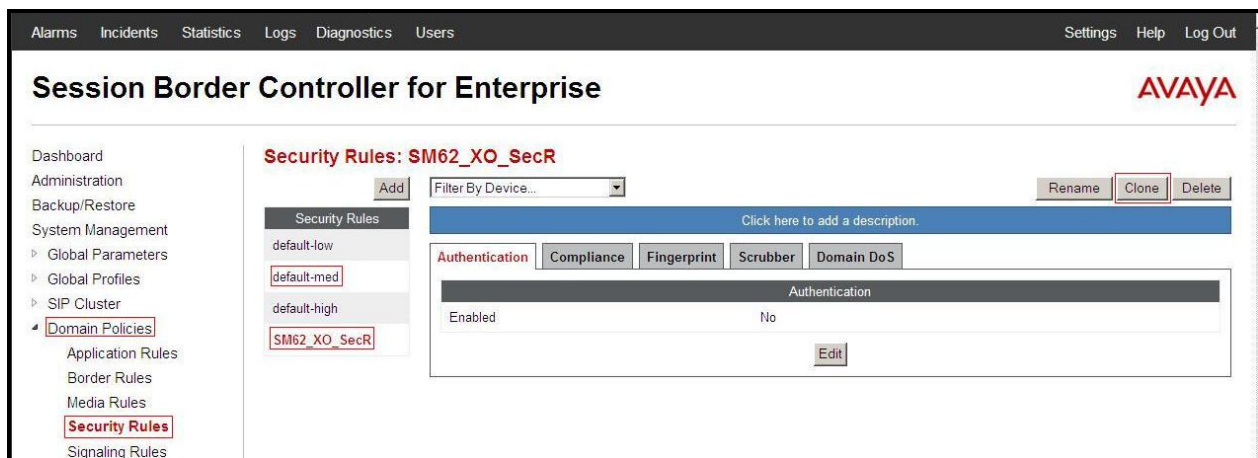


Figure 39 - Session Manager Security Rule

From the menu on the left-hand side, select **Domain Policies** → **Security Rules**.

- Select the **default-med** Rule.
- Select **Clone** button.
 - Enter Clone Name: **XO_SecR**
 - Click **Finish** (not shown).

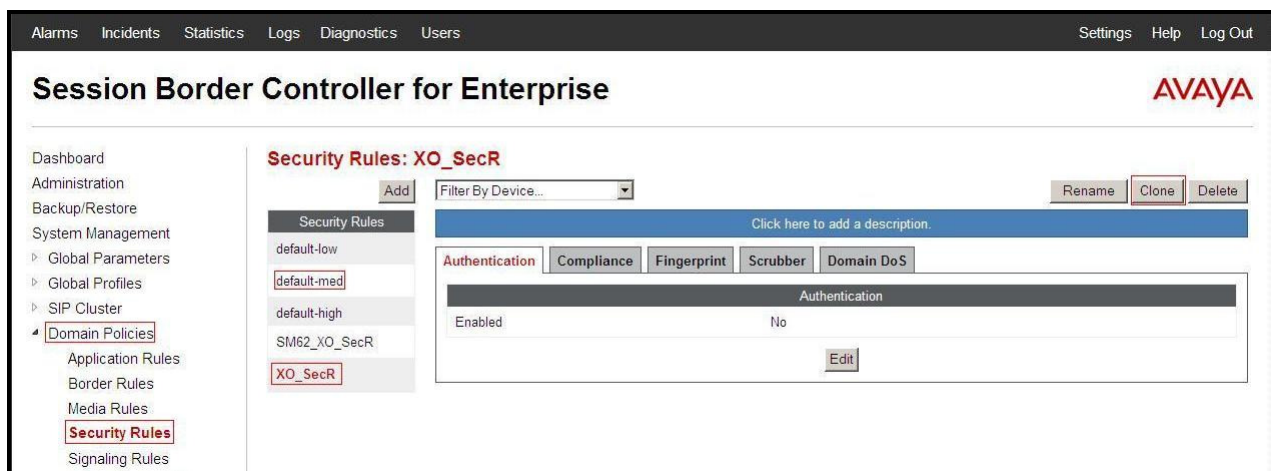


Figure 40 - XO Communications Security Rule

7.3.5. Create Signaling Rules

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

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter Clone Name: **SM62_XO_SigR**
 - Click **Finish** (not shown).

The screenshot shows the 'Session Border Controller for Enterprise' web interface. The left-hand navigation menu is expanded to 'Domain Policies', and 'Signaling Rules' is selected. The main content area displays the configuration for a rule named 'SM62_XO_SigR'. The rule is currently set to 'default'. The configuration is divided into three tabs: 'General', 'Requests', and 'Responses'. The 'General' tab is active, showing the 'Inbound' and 'Outbound' sections. The 'Inbound' section has a table with the following data:

Request Type	Action
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

The 'Outbound' section has a table with the following data:

Request Type	Action
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	

The 'Content-Type Policy' section has a table with the following data:

Policy Name	Action
Enable Content-Type Checks	<input checked="" type="checkbox"/>
Action	Allow
Multipart Action	Allow
Exception List	Exception List

The 'Edit' button is located at the bottom right of the configuration area.

Figure 41 - Session Manager Signaling Rule

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter Clone Name: **XO_SigR**
 - Click **Finish** (not shown).

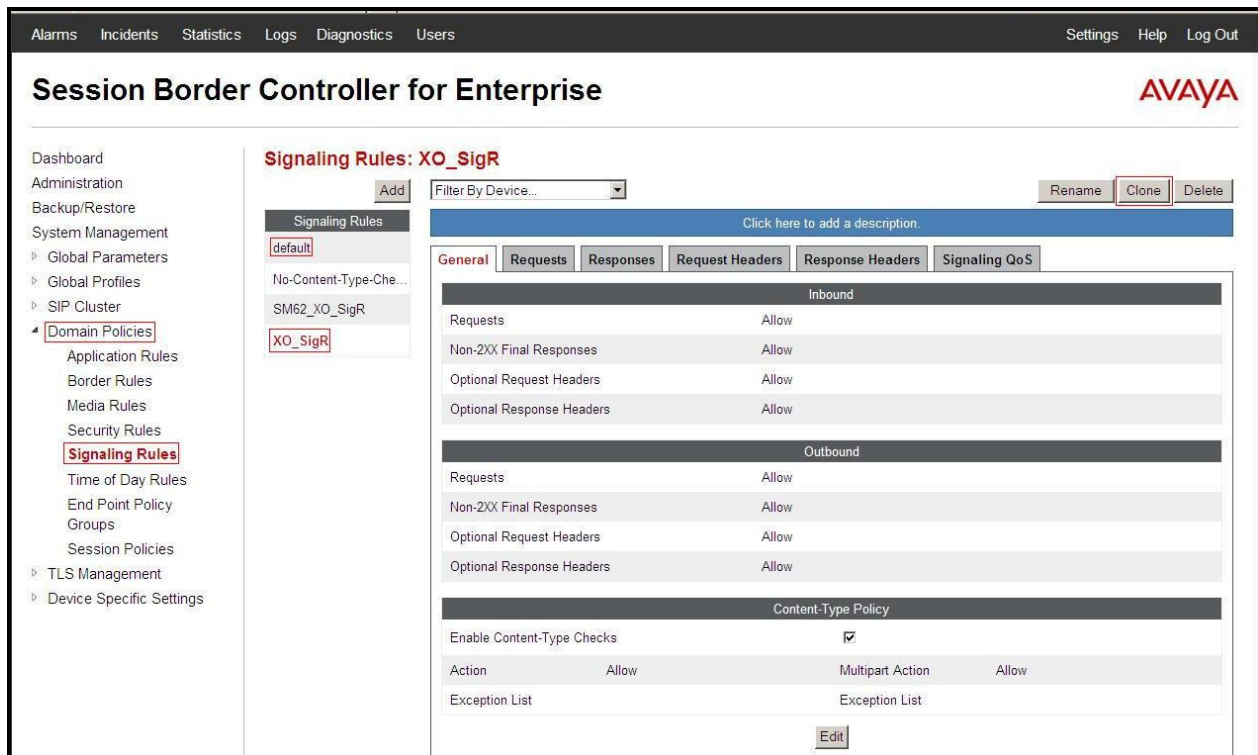


Figure 42 - XO Communications Signaling Rule

7.3.6. Create Time of Day Rules

A Time-of-day (ToD) Rule allows administrator to determine when the domain policy will be in effect. ToD Rules provide complete flexibility to fully accommodate the enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect.

From the menu on the left-hand side, select **Domain Policies** → **Time of Day Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter Clone Name: **SM62_XO_ToDR**
 - Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand menu is expanded to 'Domain Policies', and 'Time of Day Rules' is selected. The main content area displays the configuration for the 'SM62_XO_ToDR' rule. The 'Time of Day Rules' list on the left shows 'default' and 'SM62_XO_ToDR'. The 'Time of Day' configuration table shows the following details:

Date	
Start Date	02/19/2007
End Date	Never

Time	
Start Time	12:00 AM
End Time	11:59 PM

Recurrence	
This policy is applied every day.	

Buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' are visible at the top. An 'Edit' button is at the bottom right of the configuration area.

Figure 43 - Session Manager Time of Day Rule

From the menu on the left-hand side, select **Domain Policies** → **Time of Day Rules**.

- Select the **default** Rule.
- Select **Clone** button.
 - Enter Clone Name: **XO_ToDR**
 - Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand menu is expanded to 'Domain Policies', and 'Time of Day Rules' is selected. The main content area displays the configuration for the 'XO_ToDR' rule. The 'Time of Day Rules' list on the left shows 'default', 'SM62_XO_ToDR', and 'XO_ToDR'. The 'Time of Day' configuration table shows the following details:

Date	
Start Date	02/19/2007
End Date	Never

Time	
Start Time	12:00 AM
End Time	11:59 PM

Recurrence	
This policy is applied every day.	

Buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete' are visible at the top. An 'Edit' button is at the bottom right of the configuration area.

Figure 44 - XO Communications Time of Day Rule

7.3.7. Create Endpoint Policy Groups

The End-Point Policy Group feature allows administrator to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections. A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of UC-Sec security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SM62_XO_PolicyG**
 - **Application Rule: SM62_XO_AppR**
 - **Border Rule: SM62_XO_BorderR**
 - **Media Rule: SM62_XO_MediaR**
 - **Security Rule: SM62_XO_SecR**
 - **Signaling Rule: SM62_XO_SigR**
 - **Time of Day: SM62_XO_ToDR**
- Select **Finish** (not shown).

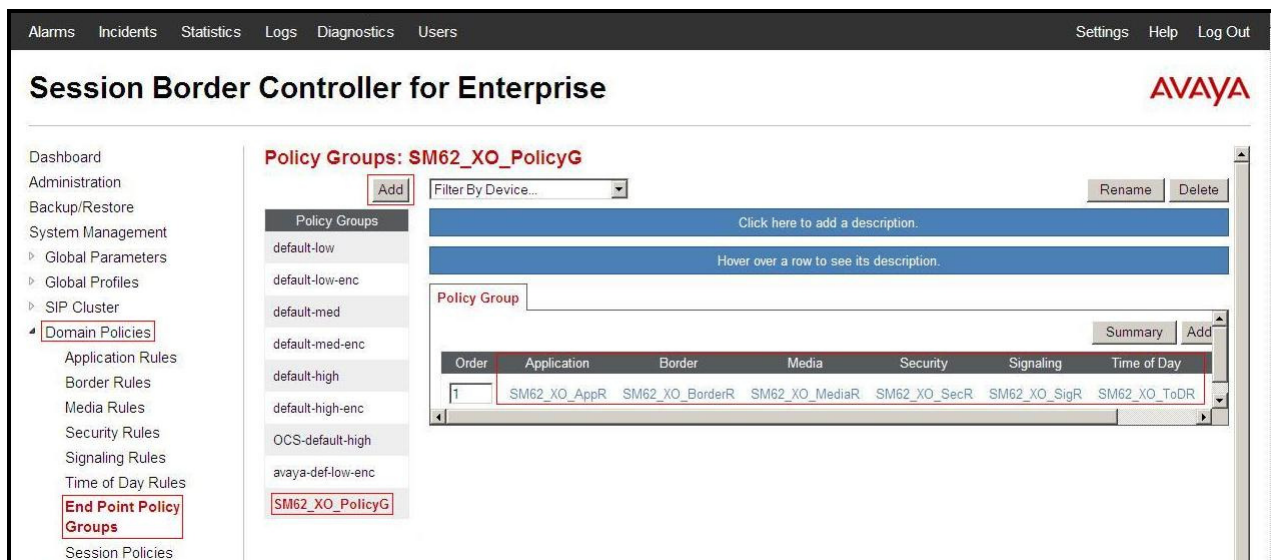


Figure 45 - Session Manager End Point Policy Group

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: XO_PolicyG**
 - **Application Rule: XO_AppR**
 - **Border Rule: XO_BorderR**
 - **Media Rule: XO_MediaR**
 - **Security Rule: XO_SecR**
 - **Signaling Rule: XO_SigR**
 - **Time of Day: XO_ToDR**
- Select **Finish** (not shown).

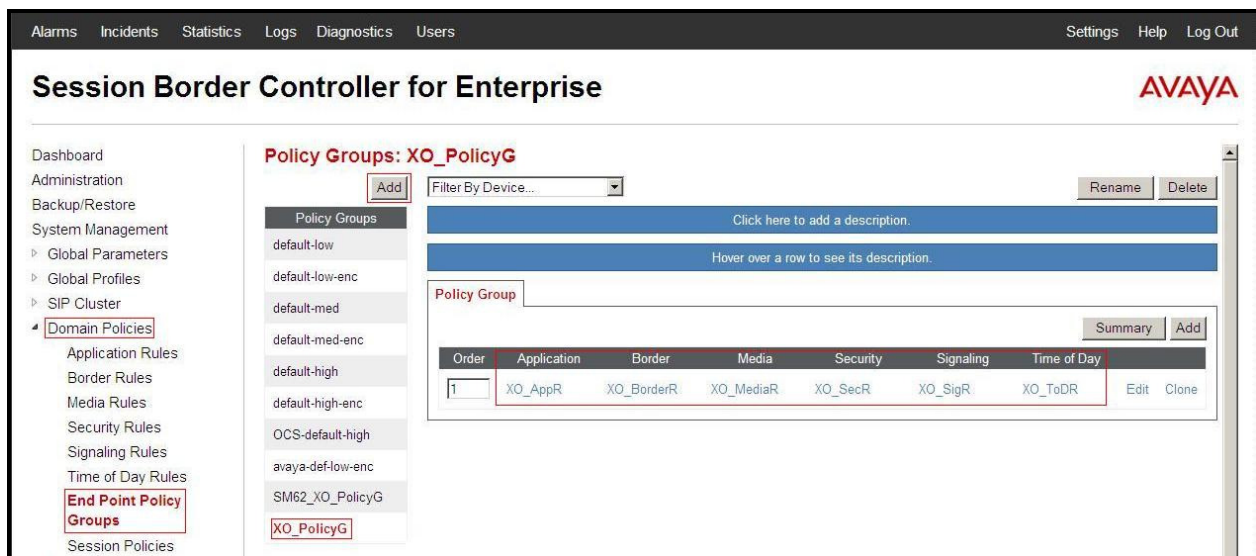


Figure 46 - XO Communications End Point Policy Group

7.3.8. Create Session Policy

Session Policies allow users to define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criterion will be handled by the Avaya SBCE product.

Select **Domain Policies** from the menu on the left-hand side.

- Select the **Session Policies**.
- Select **Add**.
- Enter Policy Name: **XO**
 - Check **Codec Prioritization**
 - Set **Preferred Codec #1: G729 (18)**
 - Set **Preferred Codec #2: PCMU (0)**
 - Set **Preferred Codec #3: Dynamic (101)**
- Select **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded to 'Domain Policies', which is highlighted. Under 'Domain Policies', 'Session Policies' is selected. The main content area shows the 'Session Policies: default' configuration. A red box highlights the 'XO' policy name in the list. The 'Add' button is also visible. The 'Codec Prioritization' tab is selected, showing the 'Audio Codec' section. The 'Codec Prioritization' checkbox is checked. The 'Allow Preferred Codecs Only' checkbox is unchecked. The 'Preferred Codec #1' is set to 'G729 (18)', 'Preferred Codec #2' is set to 'PCMU (0)', and 'Preferred Codec #3' is set to 'Dynamic (101)'. The 'Video Codec' section is also visible, with 'Codec Prioritization' unchecked. The 'Edit' button is at the bottom right of the configuration area.

Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Preferred Codec #1	G729 (18)
Preferred Codec #2	PCMU (0)
Preferred Codec #3	Dynamic (101)

Video Codec	
Codec Prioritization	<input type="checkbox"/>

Figure 47 - XO Communications Session Policy

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows administrator to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, administrator has the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows and Network Management.

7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
 - **IP Address** for Inside interface: **10.10.98.13**; **Gateway**: **10.10.98.1**
 - **IP Address** for Outside interface: **10.10.98.111**; **Gateway**: **10.10.98.97**
- Select the physical interface used in the Interface column:
 - **Inside Interface**: **A1**
 - **Outside Interface**: **B1**.

Figure 48 - Network Management

Select the **Interface Configuration** Tab.

- Toggle the State of the physical interfaces being used to **Enabled**.

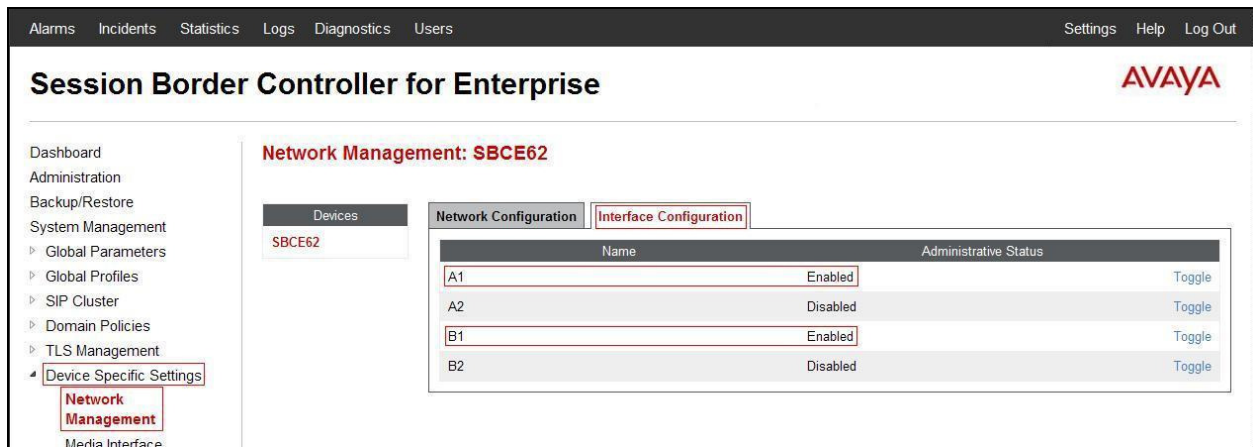


Figure 49 - Network Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya SBCE can be used for both inside and outside ports.

From the menu on the left-hand side, **Device Specific Settings** → **Media Interface**.

- Select **Add**.
 - **Name: InsideMedia**
 - **Media IP: 10.10.98.13** (Internal IP Address toward Session Manager).
 - **Port Range: 35000 - 40000**
 - Click **Finish** (not shown).
- Select **Add**.
 - **Name: OutsideMedia**
 - **Media IP: 10.10.98.111** (External IP Address toward XO Communications trunk).
 - **Port Range: 35000 - 40000**
 - Click **Finish** (not shown).

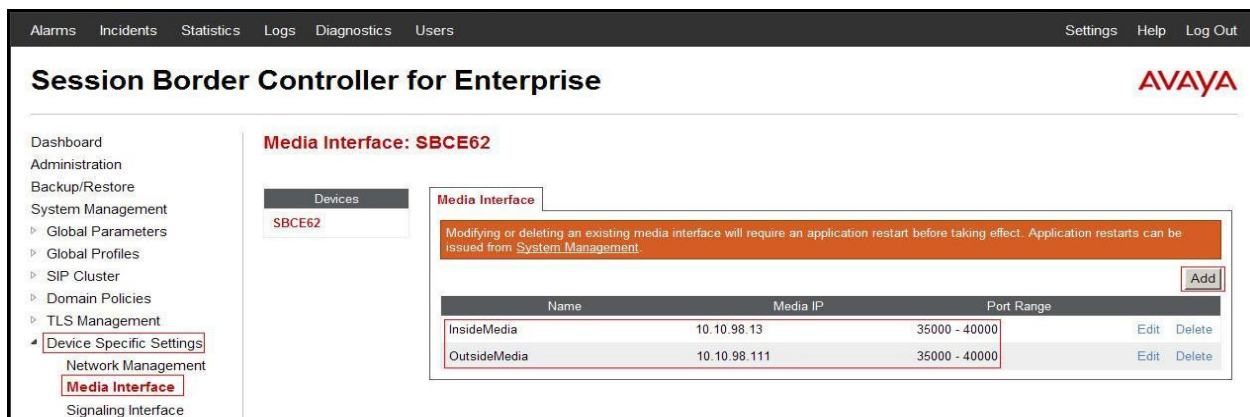


Figure 50 - Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**.

- Select **Add**.
 - **Name: InsideUDP**
 - **Media IP: 10.10.98.13** (Internal IP Address toward Session Manager).
 - **UDP Port: 5060**
 - Click **Finish** (not shown).

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**.

- Select **Add**.
 - **Name: OutsideUDP**
 - **Media IP: 10.10.98.111** (External IP Address toward XO Communications trunk).
 - **UDP Port: 5060**
 - Click **Finish** (not shown).

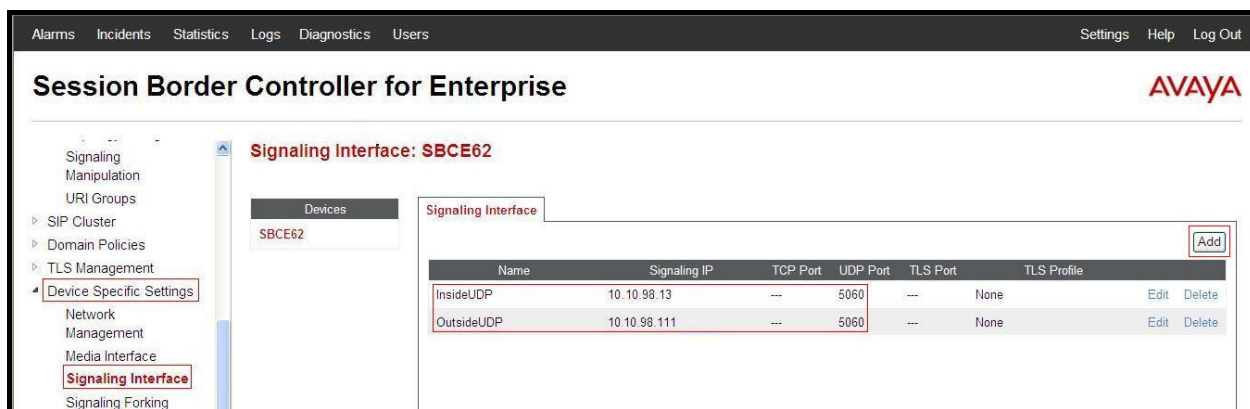


Figure 51 - Signaling Interface

7.4.4. Configuration of Server Flows

Server Flows allow administrator to categorize trunk-side signaling and apply a policy.

7.4.4.1 Create End Point Flows – Session Manager

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** Tab.
- Select **Add**, enter **Flow Name: To XO_Communications**
 - **Server Configuration: SM62**
 - **URI Group: XO_Communications**
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: OutsideUDP**
 - **Signaling Interface: InsideUDP**
 - **Media Interface: InsideMedia**
 - **End Point Policy Group: SM6_XO_PolicyG**
 - **Routing Profile: SM62_To_XO**
 - **Topology Hiding Profile: XO_To_SM62**
 - **File Transfer Profile: None**
 - Click **Finish** (not shown).

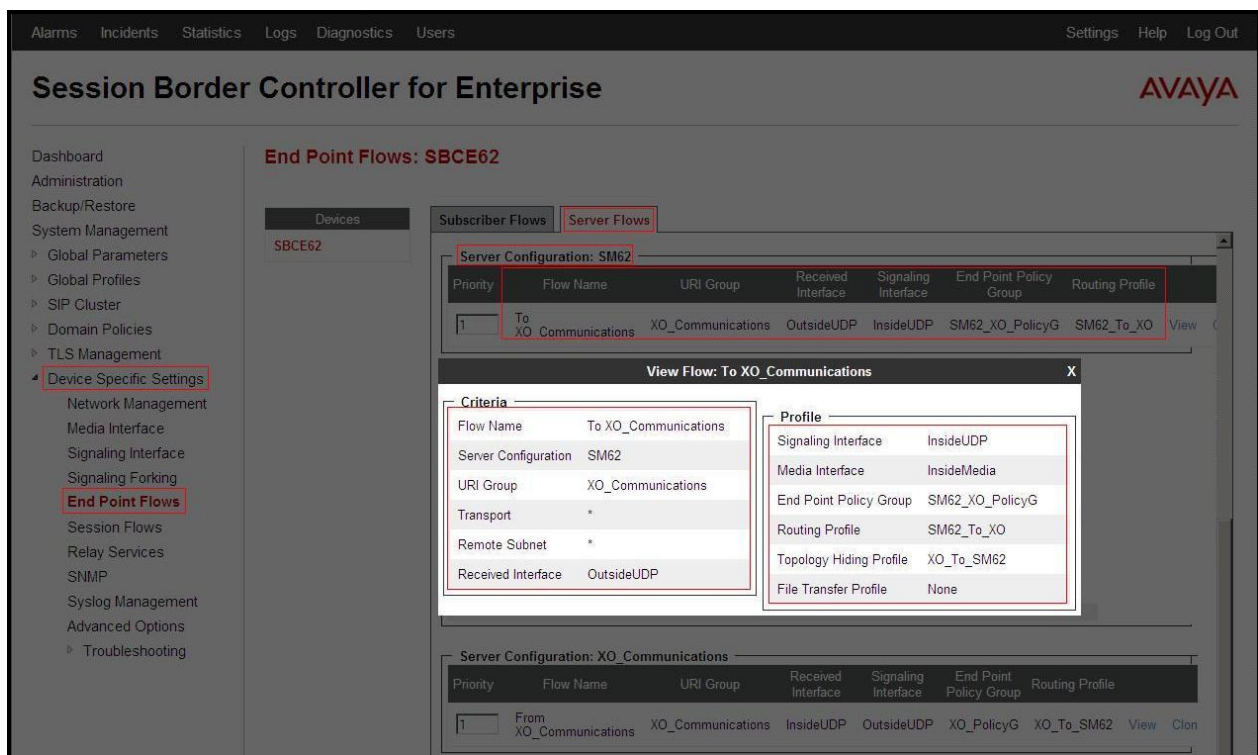


Figure 52 - End Point Flow to XO Communications

7.4.4.2 Create End Point Flows - XO Communications

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** Tab.
- Select **Add**, enter **Flow Name: From XO_Communications**
 - **Server Configuration: XO_Communications**
 - **URI Group: XO_Communications**
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: InsideUDP**
 - **Signaling Interface: OutsideUDP**
 - **Media Interface: OutsideMedia**
 - **End Point Policy Group: XO_PolicyG**
 - **Routing Profile: XO_To_SM62**
 - **Topology Hiding Profile: SM62_To_XO**
 - **File Transfer Profile: None**
 - Click **Finish** (not shown).

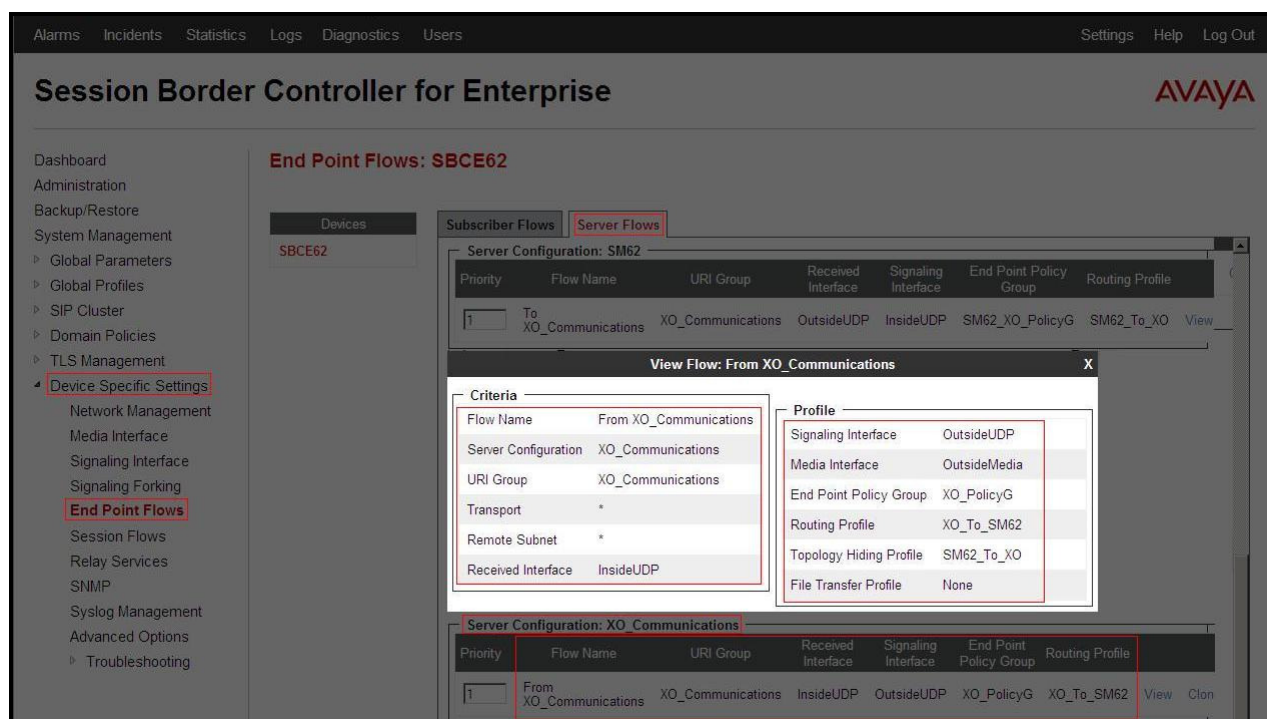


Figure 53 - End Point Flow from XO Communications

7.4.5. Create Session Flows

Session Flow determines the media (audio/video) sessions in order to apply the appropriate session policy.

- Select **Device Specific Settings** from the menu on the left-hand side.
- Select the **Session Flows**.

- Select **Add**.
- **Flow Name: XO**
 - **URI Group#1: XO_Communications**
 - **URI Group#2: XO_Communications**
 - **Session Policy: XO**
- Select **Finish** (not shown) .

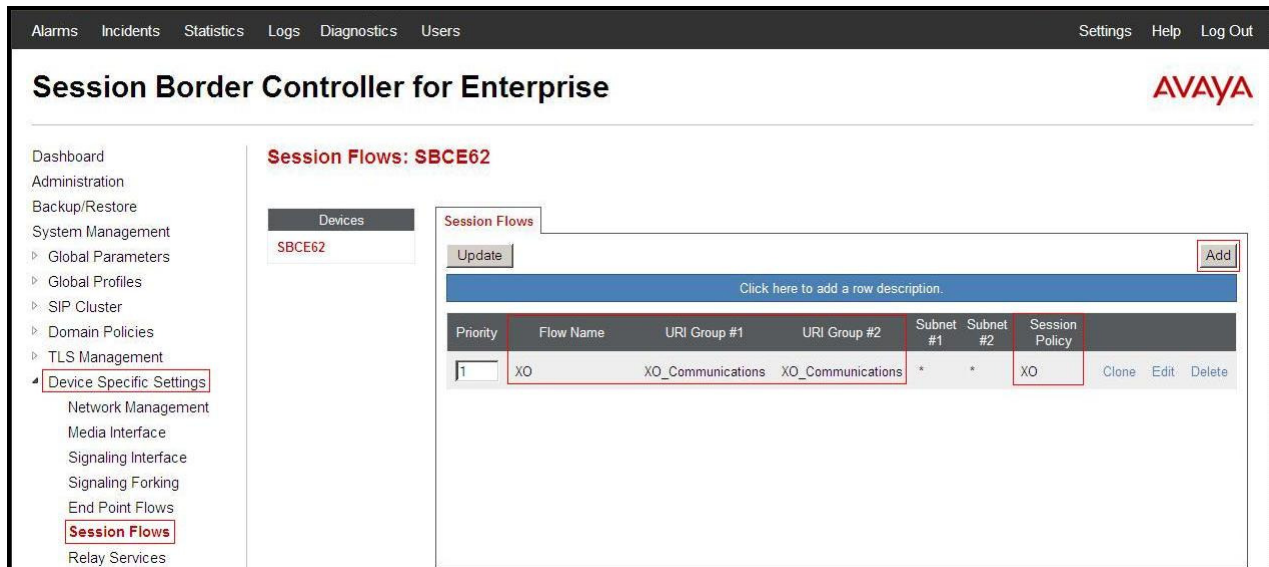


Figure 54 – Session Flows

8. XO Communications SIP Trunking Configuration

XO Communications is responsible for the network configuration of the XO Communications SIP Trunking service. XO Communications will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. XO Communications will provide the IP address of the XO Communications SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between XO Communications and the enterprise is a static configuration. There is no registration and authentication of the SIP trunk or enterprise users to the XO Communications network.

9. Verification Steps

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

Troubleshooting:

1. Enter the following commands using Communication Manager System Access Terminal (SAT) interface:
 - **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-group** <trunk-group number> - Displays trunk-group state information.
 - **status signaling-group** <signaling-group number> - Displays signaling-group state information.
2. Session Manager:
 - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.
 - **traceSM -x** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to XO Communications SIP Trunking. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workarounds.

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at:

<http://support.avaya.com/>

Avaya Aura® Session Manager/System Manager

- [1] *Administering Avaya Aura® Session Manager*, Document ID 03-603324, Release 6.2, July 2012
- [2] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Release 6.2, August 2012
- [3] *Administering Avaya Aura® System Manager*, Release 6.2, July 2012

Avaya Aura® Communication Manager

- [4] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509, Release 6.2, July 2012
- [5] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010

Avaya one-X® IP Phones

- [6] *Avaya one-X® Deskphone SIP for 9601 IP Telephone User Guide*, Document ID 16-603618, Issue 1, December 2010
- [7] *Avaya one-X® Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones*, Document ID 16-603596, Issue 1, May 2011
- [8] *Avaya one-X® Deskphone H.323 9608 and 9611G User Guide*, Document ID 16-603593, Issue 3, February 2012
- [9] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Document ID 16-601944, Release 2.6, June 2010
- [10] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Document ID 16-300698, Release 3.1, November 2009
- [11] *Administering Avaya one-X® Communicator*, October 2011
- [12] *Using Avaya one-X® Communicator Release 6.1*, October 2011

Avaya Aura® Messaging

- [13] *Administering Avaya Aura® Messaging 6.2, Issue 2.2, May 2013*
- [14] *Implementing Avaya Aura® Messaging 6.2, Issue 2, January 2013*

Avaya Session Border Controller for Enterprise

Product services for Avaya SBCE may be found at:

<http://www.sipera.com/products-services/esbc>

- [15] *Installing Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, June 2013*
- [16] *Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, March 2013*

IETF (Internet Engineering Task Force) SIP Standards Specifications

- [17] RFC 3261 *SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [18] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

©2013 Avaya Inc. All Rights Reserved.

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

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